

В.И. Кочергин

**АНГЛО-РУССКИЙ ТОЛКОВЫЙ
НАУЧНО-ТЕХНИЧЕСКИЙ СЛОВАРЬ
ПО СОВРЕМЕННОЙ КРИПТОЛОГИИ**

ИРИСС ГРУПП

Москва 2010

В.И. Кочергин

**АНГЛО-РУССКИЙ ТОЛКОВЫЙ
НАУЧНО-ТЕХНИЧЕСКИЙ СЛОВАРЬ
ПО СОВРЕМЕННОЙ КРИПТОЛОГИИ**

Томск – 2010

УДК 681.3 (038)
ББК 73 + 81.2 Англ-4
К 55

Кочергин В. И.

К 55 Англо-русский толковый научно-технический словарь по современной криптологии – М.: «ИРИС ГРУПП», 2010, -324 с.

Содержит 12 тыс. наиболее употребительных терминов по современной криптологии. В словарь также включены общенаучные термины. Словарь предназначен для специалистов, занимающихся вопросами перевода текстов по представленной тематике.

ISBN 978-5-452-0084-6

УДК 681.3 (038)
ББК 73 + 81.2 Англ-4
К 55

ISBN 978-5-452-0084-6

© Кочергин В.И., 2010
© Издательство ООО «ИРИС ГРУПП», 2010

ПРЕДИСЛОВИЕ

В последнее время выпускается большое количество русско-английских словарей по техническим дисциплинам в обычном и электронном вариантах. Однако толковых словарей, удовлетворяющих специалистов по современной криптологии, практически нет.

Современная криптология (**contemporary cryptology**) образует отдельное научное направление на стыке математики и информатики: это – математическая криптология.

Математическая криптология (**mathematical cryptology**) для шифрования сообщений использует сложные математические операции, такие как возведение очень больших чисел в чрезвычайно высокие степени по модулю произведения двух простых чисел и т.д..

Практическое применение математической криптологии стало неотъемлемой частью жизни современного общества – её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации в сотовой связи, на транспорте для защиты билетов от подделок, в банковских операциях и других.

Работы в этой области публикуются главным образом в научных журналах на английском языке, а для их понимания и правильного перевода требуются знания не только технических терминов современной криптологии, которые включают также термины по системному анализу, программированию, но знания общенаучных терминов.

Существующие словари по криптологии не содержат общенаучных терминов и не в состоянии в настоящее время удовлетворить специалистов в этой области науки. Это положение можно объяснить тем, что термины образуют самый подвижный лексический строй, а в бурно развивающихся отраслях науки и техники, к которым относятся представленные дисциплины, составляющие современную криптологию, постоянно требуется введение новых терминов и пояснений.

Восполнить этот пробел предназначен настоящий словарь.

В русском переводе термины в предлагаемом словаре разделяются следующими знаками: синонимы – запятой; более далекие значения – точной с запятой; разные значения – цифрами.

Специализированные толкования даются к английскому термину и отделяются знаком @, а общенаучные и общепринятые толкования отделяются знаком решетки (#). Все английские термины располагаются в словаре в алфавитном порядке и выделяются полужирным шрифтом. Также полужирным шрифтом выделяются номера различных специализированных толкований. При этом слова, одинаковые по написанию и произношению, например существительное и глагол, даются один раз. Слова, одинаковые по написанию, но имеющие иное произношение, представляются отдельно. При этом произношения даются в международной фонетической транскрипции. Неко-

торые звуки, например, ə, d, t, d в транскрипции могут быть даны курсивом ə, d, t, d для указания факультативности их произнесения.

АНГЛИЙСКИЙ АЛФАФИТ

A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	

ПРИНЯТЫЕ СОКРАЩЕНИЯ

<i>adj</i> (adjective)	имя прилагательное
<i>adv</i> (adverb)	наречие
<i>cj</i> (cojunction)	союз
<i>n</i> (noun)	имя существительное
<i>num</i> (numeral)	числительное
<i>pl</i> (plural)	множественное число
<i>predic</i> (predicative)	предикативное употребление
<i>pref</i> (prefix)	приставка
<i>pron</i> (pronoun)	местоимение
<i>prop</i> (proper name)	имя собственное
<i>prp</i> (preposition)	предлог
<i>refl</i> (reflexive)	употребляется с возвратным местоимением
<i>suf</i> (suffix)	окончание
<i>superl</i> (superlative degree)	превосходная степень
<i>v</i> (verb)	глагол

Основной список литературы, использованной при составлении словаря

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. История криптографии // Основы современной криптографии. – М.: Горячая линия – Телеком, 2002. – 175 с.
2. Бассар Ж. Современная криптология: Пер. с англ. – М.: Полимед, 1999.
3. Кочергин В.И. Англо-русский толковый научно-технический словарь по системному анализу, программированию, электронике и электроприводу: В 2-х т. Т. 1. – Томск, 2008. – 652 с.
5. Скляр Д.В. Криптография и наука // Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2004. – 288 с.
4. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003 – 400 С.

A*

able ['eɪbl] *n.* название шестнадцатеричной цифры А (числовое значение – 10); *adj.* знающий; способный, умелый. # **to be able** быть в состоянии.

about [ə'baʊt] *prep.* о, относительно; *adv.* около, приблизительно, почти. # **to about** примерно на. # **to be about** + *inf.* быть готовым + ; собираться + .

above [ə'boʊv] *adv.* наверху; выше; *prp.* 1. над; 2. выше; *adj.* вышеупомянутый. # **above all** главным образом; прежде всего. # **as stated above** как сказано выше. # **over and above** сверх, в добавлении; к тому же.

absent ['æbsənt] *adj.* отсутствующий. # **to be absent** отсутствовать.

abuse [ə'bjʊ:z] *n.* злоупотребление; *v.* злоупотреблять. @ **abuse-free** не допускающий злонамеренного использования. @ **abuse-free cryptosystem** криптосистема, не допускающая злонамеренного её использования.

"Abwehr" "Enigma" "Энигма" "абвера".

accept [ək'sept] *n.* 1. ввод (с клавиатуры); 2. согласие (в сетевых протоколах); *v.* 1. принимать; 2. соглашаться; признавать. @ **accept as an authenticator** в криптологии – принимать в качестве аутентификатора. # **generally accepted** общепринятый. # **to gain acceptance** получить признание.

access ['ækses] *n.* доступ. *v.* осуществлять доступ. @ **access control cryptosystem** криптосистема управления доступом. @ **access Internet traffic** осуществлять доступ к трафику "Интернет". @ **access private and commercial communications** осуществлять доступ к частным и коммерческим линиям связи. @ **access to keys** доступ к ключам. @ **access to two cryptograms in different keys for the same plaintext is very helpful to a cryptanalyst** доступ к двум криптограммам, полученным из одного и того же открытого текста с использованием разных ключей, очень помогает криптоаналитику.

accord [ə'kɔ:d] *n.* согласие; соответствие; *v.* 1. оказываться; подвергать; 2. согласовывать(ся); соответствовать (**with**). # **in accord with** в соответствии с чем-л. # **of one's own accord** добровольно. # **to accord attention** обращать внимание

accordance [ə'kɔ:dəns] *n.* согласие; соответствие. # **in accordance with** в соответствии с чем-л.; согласно чему-л.

according [ə'kɔ:diŋ] *prp.* 1. согласно, по (**to**); по утверждению; по словам (**to**). # **according as** соответственно; смотря по; в зависимости от того

account [ə'kaʊnt] *n.* 1. бюджет. @ Объем ресурсов вычислительной системы, который данный пользователь или группа пользователей может использовать в течение определенного периода времени. 2. счет; расчет; 3. отчет; описание; представление; *v.* объяснять (**for**); составлять (**for**); отсчитываться в чем-л. (**for**). # **of no account** незначительный. # **on account of** из-за, вследствие. # **on (his, her) account** из-за (него, нее). # **on no account** ни в коем случае. # **on one's own account** самостоятельно; сам по себе. # **on this account** ввиду этого. # **to come into account** учитываться. # **to leave (put) out of account** не принимать во внимание, упускать из виду. # **to take account of** учитывать. # **to take into account** принимать во внимание.

acquaint [ə'kweɪnt] *v.* знакомить. # **to get acquainted with** познакомиться, ознакомиться с. # **to have acquaintance with** быть знакомым с.

action ['æksjən] *n.* 1. действие; 2. воздействие; 3. операция. # **to bring (call) into action (play)** приводить в действие, осуществлять.

activation ['ækti'veɪʃən] *n.* активация (приведение в действие), вызов; очуствление, возбуждение. @ **activation key** ключ активации криптографического устройства.

active ['æktɪv] *adj.* 1. действующий; 2. деятельный; 3. активный. @ Выполняемый или используемый в данный момент. @ **active eavesdropping (wiretap)** активный перехват (у противника имеется возможность не только наблюдать за обменом сообщениями, но и влиять на него, напр, задерживать или удалять сигналы, передаваемые по каналам связи). @ **active key** действующий ключ.

actual ['æktʃuəl] *adj.* 1. действительный, фактический; истинный; данный; в данный момент; 2. существующий, действующий. @ **actual cryptosystem** существующая криптосистема. @ **actual key** фактический ключ.

actually ['æktʃuəli] *adv.* фактически. @ **actually-used key** фактически используемый ключ.

adaptive [ə'dæptɪv] *adj.* адаптивный. @ **adaptive-chosen-plaintext attack** адаптивная атака на основе выбранного открытого текста (противник не только может по своему усмотрению выбирать открытый текст, подлежащий зашифрованию, но и в дальнейшем имеет возможность модифицировать его, зная результат предыдущего сеанса шифрования). @ **adaptive-chosen-plaintext attack secure** защищённый от адаптивной атаки на основе выбранного открытого текста.

add [æd] *v.* 1. складывать, добавлять, прибавлять, присоединять; увеличивать; придавать. @ **add bit by bit (bitwise)** складывать бит за битом (побитово).

addition [ədɪ'ʃən] *n.* 1. прибавление, добавление; 2. сложение. @ **addition modulo 2** сложение по модулю 2. # **in addition (to)** в дополнение к; кроме; кроме того, к тому же. # **in addition to the fact that** кроме того, что.

additional [ədɪ'ʃənəl] *adj.* дополнительный. @ **additional decryption key (ADK)** дополнительный ключ расшифрования (предназначен для расшифрования криптограммы в случае, если ключ, при помощи которого производилось шифрование, по какой-то причине недоступен – утерян, умышленно уничтожен и т.д.). @ **additional key** дополнительный ключ.

additive ['ædɪtɪv] *adj.* аддитивный. @ **additive combiner** аддитивный смеситель (функция или устройство для объединения нескольких числовых последовательностей в одну путем покомпонентного сложения соответствующих элементов этих последовательностей). @ **additive stream cipher** аддитивный шифр (шифр гаммирования).

add-on [æd'ɒn] *adj.* дополнительный; *n.* расширение. @ аппаратное или программное средство, не входящее в стандартный комплект вычислительной

системы. @ **add-on cryptographic software package** дополнительный пакет программ для выполнения криптографических функций.

adherence [əd'hɪərəns] *n.* 1. приверженность; верность; 2. прилипание, сцепление; 3. соблюдение (правил и т.п.). # **adherence to specification** соблюдение технических условий.

adjacent [ə'dʒeɪsənt] *adj.* 1. примыкающий, смежный; соседний. @ **adjacent network nodes** соседние узлы сети (связи).

advance [əd'vɑːns] *v.* 1. продвигаться вперед; 2. выдвигать; приводить; 3. делать успехи; развиваться; 4. упреждать; *n.* 1. продвижение; 2. прогресс; развитие; успех; 3. упреждение, опережение. *adj.* предварительный, заблаговременный. @ **advance distribution of keys** предварительное распределение ключей. # **in advance** заранее; до. # **in advance of** впереди. # **to be far in advance** значительно опережать.

advances [əd'vɑːnsɪz] *n. pl.* успехи, прогресс, достижения. @ **advances in cryptology** достижения криптологии. @ **advances in the cryptanalysis of a cipher** успехи в криптоанализе шифра.

advanced [əd'vɑːnst] *adj.* 1. новейший; 2. основанный на последних достижениях (науки, техники и т.д.); 3. передовой; продвинутый; усовершенствованный; прогрессивный. @ **advanced cryptanalysis** криптоанализ на основе последних достижений в этой области. @ **advanced Encryption Standard (AES)** новейший стандарт шифрования (USA), основанный на последних достижениях науки. В 2000 г. для криптографии с секретным ключом был принят шифр Rijndael, который сейчас носит название AES

advantage [əd'vɑːntɪdʒ] *n.* преимущество. # **to advantage** выгодно; с успехом, успешно. # **to full advantage** полностью. # **to the best advantage** наилучшим образом. # **to be of advantage** быть выгодным; быть удобным. # **to gain (get, have) an (the) advantage over (of)** получить, иметь преимущество перед. # **to gain advantage** использовать. # **to take advantage of** воспользоваться, использовать.

adversary ['ædvə:səri] *n.* @ в криптологии – нарушитель (противник)

affected [ə'fektɪd] *p.p.* 1. нарушенный, поврежденный; 2. затронутый. # **as affected** под влиянием (действием)

affine [ə'faɪn] *adj.* аффинный. @ **affine mapping** аффинное отображение. @ **affine cipher** в криптологии – аффинный шифр.

after ['ɑːftər] *prp.* 1. после, по; 2. согласно, по; 3. вслед за; 4. в честь; *cj.* после того как. # **after all** в конце концов. # **after a while** через некоторое время. # **after the fashion** подобно; следуя методу, по методу; по способу. # **after the manner** подобно; следуя методу, по методу; по способу. # **shortly after** вскоре после (того как). # **well after** значительно позже.

again [ə'geɪn] *adv.* 1. снова, опять; 2. кроме того, к тому же; 3. с другой стороны. # **again and again** снова и снова; неоднократно. # **as much again** иногда, время от времени. # **once again** еще раз; снова. # **over and over again** много раз, неоднократно. # **time and again** неоднократно.

against [ə'geɪnst] *prp.* 1. против; 2. о, об, по, к, на; 3. в зависимости от; по отношению, относительно; 4. на фоне; 5. рядом.# **as against** по сравнению.# **to be against** противоречить; быть против.

agency ['eɪdʒənsɪ] *n.* 1. воздействие; 2. средство; 3. фактор; 4. агентство, организация; в криптологии – агентствоуправление.# **through (by) the agency** посредством.

ago [ə'ɡəʊ] *adv.* тому назад.# **as long ago as** еще, уже.# **long ago** давно.# **not long ago** недавно.# **a while ago** недавно.

agree [ə'ɡri:] *v.* 1. соглашаться; 2. решать, договариваться; 3. соответствовать, совпадать.@ **agree on a key in advance** в криптологии – заранее договориться о ключе **aids** *n. pl.* средства.

agreed-upon [ə'ɡri:də'pɒn] *adj.* согласованный.@ **agreed-upon key** согласованный ключ (в одноключевой криптосистеме).

ahead [ə'hed] *adv.* вперед; впереди.# **ahead of time (schedule)** досрочно.

aid [eɪd] *v.* помогать; способствовать; *n.* 1. помощь; 2. средство (вспомогательное).

aim [eɪm] *n.* цель, намерение; *v.* 1. иметь своей целью, стремиться к (**at**); 2. наводить на цель.# **to be aimed at** быть предназначенным, быть направленным на.

algebraic ['ældʒɪ'breɪk] *adj.* алгебраический.@ **algebraic attack** алгебраическая атака (ведется с привлечением алгебраической теории). @ **algebraic cipher** алгебраический шифр.@ **algebraic normal form (ANF)** алгебраическая нормальная форма.

algorithm (ALG) ['ælɡɒrɪðzəm] *n.* 1. алгоритм; 2. метод, правило.

algorithm-supported encryption = algorithmic encryption

algorithmic ['ælɡɒrɪðzmɪk] *adj.* алгоритмический.@ **algorithmic diagram** ['ælɡɒrɪðzmɪk 'daɪəɡræm] алгоритмическая схема.@ **algorithmic encryption** шифрование по алгоритму.

all [ɔ:l] *adj.* весь, вся, все, всё.@ **all-key** в криптологии – характеризующийся перебором всех возможных вариантов ключа.@ **all-key attack** в криптологии – атака с перебором всех возможных вариантов ключа.# **after all** в конце концов.# **all along** на всем протяжении; все время.# **all at once** неожиданно.# **all but** почти; кроме; чуть не, далеко не.# **(all) in all** всего; вообще.# **all of which** все они.# **all over** повсюду, кругом; совершенно, полностью.# **all the better** тем лучше.# **all the more** тем более.# **all the same** все равно; тем не менее.# **all the worse** тем хуже.# **all through** на всем протяжении.# **all too often** слишком часто.# **at all** совсем, вообще.# **at all events** во всяком случае.# **first of all** прежде всего.# **for all that** несмотря на все это.# **in all** полностью; всего.# **not at all** нисколько, ничуть.

allege [ə'leɪdʒ] *v.* 1. ссылаться на что-л.; 2. утверждать (без основания).# **alleged to be due to** якобы обусловленный.

Allied Communications and Computer Security Agency (ACCSA) *n.* Агентство коммуникационной и компьютерной безопасности объединенных вооруженных сил (НАТО).

allophone ['æləˌfoun] *n.* @ в криптологии – аллофон (набор звуков, имеющих одинаковые свойства или одинаковую информативность).

almost ['ɔːlmoust] *adj.* почти. @ **almost perfect non-linear function (APNF)** почти совершенная нелинейная функция.

allow ['ælaʊ] *v.* 1. позволять; 2. допускать; 3. предусматривать, учитывать, делать поправку на что-л. (**for**).# **to allow for** учитывать; делать допуск (поправку) на что-л.# **to allow for the fact** с учетом того, что .

allowance ['ælaʊəns] *n.* допуск, допущение.# **to make allowance for** с учетом того, что.

alphabet wheel = cipher clock

alphabet ['ælfəbit] *n.* алфавит.

alphabetic ['ælfəbetɪk] *adj.* алфавитный. @ **alphabetic character** буква. @ **alphabetic code** буквенный код, алфавитный код. @ **alphabetic printer** буквопечатающее устройство. @ **alphabetic progression** алфавитная прогрессия. @ **alphabetic word** буквенное слово.

alphabetic string ['ælfəbetɪk strɪŋ] 1. текстовая строка. @ Строка символов, принадлежащих данному алфавиту. 2. строка букв.

alone [ə'laʊn] *predic.* один; *adv.* только.# **let alone** не говоря уже о.

along [ə'lɒŋ] *prp.* вдоль по.# **all along** на всем протяжении; все время.# **along the lines** в направлении; по типу; в соответствии с.# **along with** наряду с, вместе.

alongside [ə'lɒŋ'saɪd] *adv.* рядом.# **alongside with** наряду с.

alphanumeric(al) ['ælfənju'merɪ(əl)] *adj.* буквенно-цифровой; алфавитно-цифровой; текстовый. @ **alphanumerical character** буква или цифра. @ **alphanumeric key** @ в криптологии – буквенно-цифровой ключ.

alterable ['ɔːltəbl] *adj.* изменяемый. @ **alterable key** в криптологии – изменяемый ключ.

alternative ['ɔltəːneɪtɪv] *n.* 1. вариант. @ Вариант, одна из двух или более возможностей; то, что можно иметь, использовать и т.п. вместо чего-то еще. На множестве альтернатив осуществляется выбор. 2. выбор; 3. другой выход (из положения); *adj.* другой; альтернативный. @ **alternative hypothesis** альтернативная гипотеза.

alternatively ['ɔltəːneɪtɪvli] *adv.* 1. поочередно; 2. или же, иначе; наоборот; 3. попеременно.# **alternatively to** в отличие от; вместо.

amateur ['æmətəː] *adj.* любительский. @ **amateur cryptanalyst** криптоаналитик-любитель. @ **amateur cryptographer** криптограф-любитель.

ambiguous [æm'bigjuəs] *adj.* 1. двусмысленный, неоднозначный; 2. неясный, сомнительный. @ **ambiguous cryptogram** неоднозначная криптограмма.

amenable [ə'miːnəbl] *adj.* поддающийся; доступный; подверженный.# **to be amenable** поддаваться чему-л.

American [ə'merikən] *adj.* американский. @ 1. **American Black Chamber (ABC)** 1. "Американский черный кабинет" (дешифровальное бюро, существовавшее с 1917 по 1929 г. при государственном департаменте USA); 2. "Американский черный кабинет" (название книги мемуаров бессменного руководителя "Американского черного кабинета" Ярдли). 2. **American Cryptogram Association** Американская криптологическая ассоциация. 3. **American National Standards Institute (ANSI)** Американский национальный институт стандартов (занимается стандартизацией во многих технических областях, включая разработку криптографических стандартов). 4. **American Standard Code for Information Interchange (ASCII)** Американский стандартный код для обмена информацией.

among (amongst) [ə'mʌŋ] *prp.* среди, между. # **among other things** между прочим; в частности.

amount [ə'maʊnt] *v.* достигать, составлять, сводиться к чему-л. (**to**); *n.* 1. величина, количество, степень; 2. сумма. @ **amount of information in a message** количество информации в сообщении.

anagram ['ænəgræm] *n.* анаграмма.

anagramming ['ænəgræmɪŋ] *n.* анаграммирование.

analog ['ænəlɒɡ] *adj.* аналоговый. @ **analog communication (com, comm)** аналоговая связь.

analogy [ə'nælədʒɪ] *n.* аналогия; сходство. # **by analogy with** по аналогии. # **on the analogy of** по аналогии. # **to give analogy to** проводить сравнение с.

analysability [ə'næləs,ə'bɪlɪtɪ] *n.* @ в криптологии – подверженность криптоанализу.

analysis [ə'næləsɪs] *n.* анализ. @ 1. Мысленное или реальное разделение целого на части (например, химический анализ вещества, декомпозиция глобальной цели и т. д.). 2. Синоним научного исследования вообще («подвергнуть анализу» означает «изучить»). 3. криптоанализ. @ **analysis of pseudorandom number generators** в криптологии – анализ генераторов псевдослучайных чисел. # **in the last analysis** в конечном счете.

analyst [ænə'lɪst] *n.* аналитик. @ 1. Специалист по системному анализу. 2. В криптологии – криптоаналитик.

ancestor ['ænsɪstə] *n.* предок. @ Вершина дерева, расположенная выше данной вершины. @ В криптологии – предшественник. @ **ancestor key** в криптологии – предшествующий (исходный) ключ.

antenna [æn'tenə] *n.* антенна.

a posteriori ['eɪpɒs,tɪrɪ'ɔːraɪ] *adj.* лат. @ в криптологии – апостериорный.

and [ænd] *conj.* и, а. # **and so on** и так далее. # **and so forth** и так далее.

"ant" [ænt] *n.* "муравей" (сверхминиатюрная аппаратная закладка, предназначенная для внедрения в аппаратуру шифрования).

anu ['eni] *adj., pron.* какой-либо (в *вопросит. предл.*); любой (в *утверд. предл.*); никакой (в *отрицат. предл.*). # **anu longer** больше не. # **anu more** больше не. # **at anu cost** во что бы то ни стало. # **at anu rate** по крайней мере;

во всяком случае. # **if anu (anuthing)** если вообще (имеется, требуется и т.п.). # **in anu case (event)** во всяком случае.

apart [ə'pa:t] *adv.* 1. отдельно, в стороне; 2. кроме; 3. на расстоянии; 4. с интервалом в. # **apart from apart** помимо, за исключением. # **wide apart** на большом расстоянии друг от друга.

a periodic ['eɪpɪrɪdɪk] *adj.* апериодичный. @ **aperiodic polyalphabetic substitution cipher** апериодичный шифр многоалфавитной замены.

aperiodic *n.* = **aperiodic polyalphabetic substitution cipher**

a posteriori ['eɪpɒstərɪəri] *adj.* лат. апостериорный (Апостериорный язык (от лат. a posteriori — из последующего) — искусственный язык, элементы которого заимствованы из существующих языков, в противоположность априорному языку). @ **aposteriori probability** апостериорная вероятность.

appear [ə'pɪə] *v.* 1. появляться; 2. казаться; 3. оказываться. # **appear + inf.** по-видимому + *inf.* # **it appears** представляться

appearance [ə'pɪərəns] *n.* 1. появление; 2. (внешний) вид, наружность. # **to all appearance(s)** судя по всему. # **to make appearance** появляться

append [ə'pend] *v.* добавлять в конец; конкатенировать. @ **append MAC to information being authenticated** добавлять MAC к информации, подлежащей аутентификации.

application (layer) protocol [æplɪ'keɪʃən ('leɪə) 'prəʊtəkwɔːl] протокол прикладной программы, прикладной протокол. @ Уровень протокола сети передачи данных, определяемый конкретным приложением.

application [æplɪ'keɪʃən] *n.* 1. прикладная программа. 2. приложение, применение, употребление; применимость; 3. обращение, просьба; заявление. @ **application-directed cryptography** прикладная криптография. @ **application call** вызов из прикладной программы. @ **application programmer** прикладной программист, разработчик прикладного программного обеспечения. @ **application system** прикладная система. @ **application-oriented** проблемно-ориентированный.

application domain [æplɪ'keɪʃən də'meɪn] прикладная область, предметная область. @ Совокупность понятий и объектов, информация о которых хранится в базе данных или обрабатывается программой.

application package [æplɪ'keɪʃən 'rækɪdʒ] пакет прикладных программ. @ Набор программ и средств обращения к ним для решения определенного класса задач.

application program [æplɪ'keɪʃən 'prəʊgræm] прикладная программа. @ 1. Программа, использующая средства, предоставляемые системной программой; одна и та же программа может считаться как системной, так и прикладной в зависимости от того, какой уровень программных средств считается базовым. 2. Программа для решения определенной задачи.

application terminal [æplɪ'keɪʃən 'tɜːmɪnəl] прикладной терминал. @ Аппаратное средство, в котором объединены в целостную конфигурацию различные устройства ввода-вывода с целью удовлетворения потребителей.

applications software [æplɪ'keɪʃən 'sɒftweə] прикладное программное обеспечение, прикладные программы. @ Программное обеспечение, предназначенное для решения определенной задачи или класса задач или для предоставления пользователю определенных услуг.

application-directed cryptography = applied cryptography

applied [ə'plaɪd] *adj.* прикладной. @ **applied mathematics** прикладная математика. @ **applied research** 1. научно-технические исследования; 2. исследования в области прикладных наук.

applied cryptanalysis [[ə'plaɪd kriptə'næləsɪz] прикладной криптографический анализ. @ Обработка зашифрованного сообщения с целью выделения исходной информации лицом, не знающим секретного ключа.

applied cryptography [ə'plaɪd 'kriptəʊgrə:fɪ] *n.* прикладная криптография. @ Защита сообщения путем превращения его в набор знаков, расшифровать который может только человек, знающий ключ.

approach [ə'prəʊtʃ] *n.* 1. аппроксимация, приближение, подход к решению; 2. метод, методика; 3. рассмотрение; *v.* приближаться; подходить; достигать. @ в криптологии – подход-метод. @ **approach to the solution of a cipher** метод вскрытия шифра.

appropriate [ə'prəʊprɪət] *adj.* 1. соответствующий, уместный; 2. свойственный, присущий; 3. подходящий; *v.* 1. присваивать; 2. предназначать. @ **appropriate key** соответствующий ключ (напр., ключ расшифрования, соответствующий ключу зашифрования).

approximation [ə'prɒksɪ'meɪʃən] *n.* аппроксимация, приближение, приближенное значение.

apriory ['eɪprɪə'i:ɹɪ] *adj.* лат. априорный. @ **apriory probability** априорная вероятность.

apt [æpt] *adj.* 1. подходящий; 2. *perdic.* вероятный, возможный; 3. склонный. # **to be apt** иметь тенденцию к; вероятно.

arbiter ['a:bitə] *n.* арбитр.

arbitrary ['a:bitrəri] *adj.* 1. произвольный; 2. необоснованный. @ **arbitrary key** произвольный ключ. @ **arbitrary-chosen key** произвольно выбранный ключ. # **arbitrary signs and symbols** условные знаки и обозначения.

arbitrate ['a:bitrəɪt] *n.* разрешать (споры, конфликты).

arbitration ['a:bitrəɪʃən] *n.* арбитраж.

arbitrator *n.* = **arbiter**

arithmetic [ə'ɪθmətɪk] *n.* 1. арифметика, арифметические операции. @ Выполнение операций над числами. 2. арифметический процессор. @ Сопроцессор для выполнения арифметических операций. @ **arithmetic of primes, prime products, Galois fields** арифметика простых чисел, произведений простых чисел, полей Галуа.

-ary [:əri] *suff.* –арный. @ **q-ary (q-valued)** q-нарный, q-значный, q-ичный. @ **q-ary logic** q-ичная логика; многозначная логика.

arm [a:m] *n.* 1. рука (от кисти до плеча); 2. рукав (реки); 3. рычаг; 4. *pl.* оружие; род войск; *v.* вооружать(ся).# **arms race** гонка вооружений.# **to be armed with information** располагать исчерпывающей информацией.

arrive [ə'raɪv] *v.* 1. прибывать (**at, in**); 2. достигать (**at**).# **to arrive at a conclusion** приходить к заключению.# **to arrive at a decision** принять решение

art [a:t] *n.* 1. искусство; 2. ремесло; 3. умение, знание.# **state of (the) art** уровень развития науки (техники и т.п.) на данном этапе.

as [æz] *adv.* как; *prp.* в качестве; *тж.* переводится творительным падежом; *сj.* 1. как; 2. когда, в то время как; по мере того как; 3. так как, поскольку; 4. хотя; как ни, как бы ни (*после прилагательного или наречия, например: strange as it is* как это ни странно); *pron.* который, какой; что.# **as ... as** так же ... как и; такой же ... как.# **as affected** под влиянием (действием).# **as against** по сравнению с.# **as between** в отношениях между.# **as compared to (with)** по сравнению с.# **as a consequence** в результате.# **as consistent with** в соответствии с.# **as contrasted to (with)** в противоположность чему-л.# **as distinct from** в отличие от.# **as early as** еще, уже.# **as (is) evidenced by** о чем свидетельствует.# **as far as** насколько; поскольку; до.# **as far as ... is concerned** что касается; когда речь идет о.# **as far as it goes** поскольку дело касается, что касается.# **as far back as** еще, уже.# **as following from** исходя из.# **as follows** следующим образом; следующее.# **as for** что касается, в отношении.# **as from** начиная с.# **as good as** все равно, что; фактически.# **as granted** без доказательства.# **as judged by (from)** судя по.# **as if** как будто, как если бы.# **as though** как будто, как если бы.# **as inferring that** как то, что; как указывающее на то, что.# **as is also** а также и.# **as it is (as they are)** фактически, в действительности.# **as it does (as they do)** фактически, в действительности.# **as it stands** при создавшемся положении вещей.# **as it were** как бы; так сказать.# **as late as** только.# **as long as** пока; поскольку.# **as long ago as** еще, уже.# **as a conservative estimate** по скромному подсчету.# **as a matter of convenience** для удобства.# **as a matter of course** как нечто само собой разумеющееся.# **as a matter of engineering judgement** с точки зрения техники; по техническим соображениям.# **as a matter of experience** исходя из опыта.# **as a matter of fact** фактически, на самом деле.# **as a matter of record** на основании полученных данных.# **as it were** так сказать, как бы.# **as many (much)** столько же.# **as much as** (*ср.* **as high as, as large as, as little as, as low as**) до (*обычно перед цифрами*); столько же, сколько.# **as of** (2000) по данным на (2000 г.).# **as often as not** нередко.# **as on** по состоянию.# **as opposed to** в противоположность, в отличие от.# **as per** согласно.# **as regards** что касается, в отношении.# **as relating to** относительно.# **as soon as** как только.# **as such** как таковой; сам по себе; по существу.# **as time goes on** с течением времени.# **as to** что касается; относительно; о.# **as well** также; с таким же успехом.# **as well as** а также (и); так же как (и).# **as a whole** в целом.# **as yet** еще; пока, до сих пор.# **in as much as** поскольку; ввиду того, что.# **so as + inf.** так, чтобы + *inf.*.# **(in) so far as** поскольку.# **(in) so far as ... is concerned** что касается; поскольку речь идет

о; когда дело касается. @ **as yet unbroken knapsack cryptosystem** все ещё не вскрытая ранцевая криптосистема.

asymmetric [æsi'metrik] *adj.* асимметричный. @ **asymmetric relation** асимметричное отношение.

ascending [ə'sendɪŋ] *adj.* возрастающий. @ **ascending key** в криптологии – возрастающий ключ.

ascending sort [ə'sendɪŋ sɔ:t] сортировка по возрастанию. @ Сортировка, при которой записи упорядочиваются по возрастанию значений ключевых полей.

aside [ə'saɪd] *adv.* в сторону; в стороне. # **aside from** за исключением, помимо. # **to put aside** отложить. # **to set aside** не учитывать.

assess [ə'səs] *v.* оценивать, определять. @ **assess security of cryptosystems** @ оценивать стойкость криптосистем.

assignment [ə'saɪnmənt] *n.* 1. присваивание. @ Операция изменения значения переменной, регистра, элемента массива, поля записи или другого элемента данных. 2. назначение. @ Приписывание устройству или другому ресурсу имени, по которому к нему могут обращаться программы. 3. задание. @ **assignment problem** 1. задача присвоения (напр. адресов); 2. задача о назначениях. @ **assignment statement** оператор присваивания. @ **assignment symbol** символ присвоения. @ **assignment-free language** язык программирования без присваивания.

assumption [ə'sʌmpʃən] *n.* допущение, предположение. @ **assumption unbroken knapsack cryptosystem** все еще не вскрытая ранцевая криптосистема. # **on the assumption** исходя из предположения.

asymmetric [æsi'metrik] *adj.* асимметричный. @ **asymmetric relation** асимметричное отношение. @ **asymmetric algorithm** в криптологии – асимметричный алгоритм (шифрования). @ **asymmetric encryption** в криптологии – асимметричное шифрование. @ **asymmetric key** в криптологии – асимметричный ключ (только для шифрования или только для расшифрования). @ **asymmetric keys** ключи асимметричной криптосистемы (разные для шифрования и расшифрования).

asymmetrically [æsi'metrikəlɪ] *adv.* асимметрично. @ **asymmetrically encrypted** в криптологии – зашифрованный с помощью асимметричного алгоритма.

asynchronous [ei'sɪŋkrənəs] асинхронный (режим). @ Режим синхронизации работы ЭВМ, при котором выполнение каждой конкретной операции начинается после получения сигнала, указывающего на окончание предыдущей операции. @ **asynchronous attack** в криптологии – асинхронная атака. @ **asynchronous attack secure** в криптологии – защищённый от асинхронной атаки. @ **asynchronous circuit** асинхронная схема. @ **asynchronous communication (com, comm.)** асинхронная передача данных, асинхронная связь. @ **asynchronous communications interfase adapter (ACIA)** адаптер асинхронной связи. @ **asynchronous mode (A-mode)** асинхронный режим. @ **asynchronous time divi-**

sion multiplexing (ATDM) асинхронное временное уплотнение, асинхронное временное мультиплексирование. @ **asynchronous transmission** асинхронная передача данных.

asynchronous system trap (AST) [eɪ'sɪŋkrənəs 'sɪstɪm træp] асинхронное прерывание. @ Прерывание, возникновение которого не привязано к определенной точке программы: внешнее прерывание или прерывание, связанное с работой другого процесса (например, поступление сигнала, завершения обмена).

attachment [ə'tætʃmənt] *n.* 1. приспособление; 2. присоединение; 3. ставка

attack [ə'tæk] *v.* 1. нападать; 2. приступать к разрешению проблемы; 3. воздействовать. @ в криптологии – атаковать, подвергать криптоанализу, пытаться вскрыть. @ **attack the DES** в криптологии – пытаться вскрыть DES. *n.* 1. атака, наступление; 2. подход. @ в криптологии – криптоанализ, попытка вскрытия (криптосистемы). @ **attack by iteration** криптоанализ методом итераций. @ **attack by liberation on an encryption algorithm** атака на алгоритм шифрования. @ **attack by liberation-proof** криптостойкий, стойкий к криптоанализу; @ **attack-proof** криптостойкий, стойкий к криптоанализу.

attack by liberation-resistant = attack by liberation-proof

attack-resistant = attack-proof

attacker [ə'tækə] *n.* @ в криптологии – нарушитель противник криптоаналитик.

attend [ə'tend] *v.* 1. присутствовать (*на лекциях, собраниях и т.п.*); 2. сопровождать; сопутствовать; 3. принимать участие. # **to attend to** уделять внимание чему-л.; заниматься чем-л., быть внимательным к кому-л., чему-л.

attention [ə'tenʃən] *n.* внима-ние. # **to attract (draw. call) attention to** привлекать внимание к. # **to give attention to** обращать внимание. # **to pay attention to** обращать внимание

attribute [æ'tribju:t] *n.* 1. атрибут, свойство. @ Признак, характеризующий объект. 2. атрибут. @ 1. В реляционных базах данных – поименованный домен, столбец таблицы. 2. В машинной графике – свойство примитива или сегмента изображения, определяющее цвет, вид линии, фактуру поверхности, шрифт текста. 3. свойство; характерный признак, характерная черта. @ **attributes of a cryptosystem** в криптологии – свойства криптосистемы. *v.* приписывать чему-л.; относить за счет кого-л. (**to**); в криптологии – приписывать авторство. @ **attribute a message to a transmitter** в криптологии – приписывать авторство сообщения передатчику. # **to be attributable to** приписывать чему-л.; относить за счет чего-л., кого-л.

audio ['ɔ:diəu] *n.* звук. @ **audio encryption** в криптологии – шифрование звуковых сигналов. *adj.* звуковой.

authentic [ɔ:'θentɪk] *adj.* истинный, настоящий. @ **authentic messages** в криптологии – истинные сообщения.

authenticate [ɔ:'θentikeit] *n.* аутентифицировать. @ **authenticate a message** в криптологии – аутентифицировать сообщение.

authenticated [ɔ:'θentikeitɪd] *adj.* аутентифицированный. @ **authenticated communication (com, comm.)** в криптологии – связь с (взаимной) аутентификацией партнёров. @ **authenticated key agreement protocol** в криптологии – протокол согласования ключа с аутентификацией.

authenticating [ɔ:'θentikeitɪŋ] *adj.* @ в криптологии – аутентификационный.

authentication [ɔ:'θentikeɪʃən] *n.* аутентификация, опознавание @ в криптологии – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности, опознание. @ **authentication channel** в криптологии – канал аутентификации. @ **authentication code (A-code)** в криптологии – аутентификационный код. @ **authentication code with arbitration (A²-code)** в криптологии – аутентификационный код с арбитражем. @ **authentication exchange** в криптологии – проверка подлинности с обменом информацией. @ **authentication function** в криптологии – аутентификационная функция. @ **authentication message** в криптологии – аутентификационное сообщение. @ **authentication pattern** в криптологии – 1. комбинация для аутентификации; 2. подтверждение права на доступ; 3. проверка подлинности (достоверности). @ **authentication problem** в криптологии – задача проверки на достоверность. @ **authentication system** 1. система аутентификации (криптосистема или криптографический процессор, используемые для аутентификации); 2. подтверждение права на доступ; 3. проверка подлинности (достоверности). @ **authentication system exchange** проверка подлинности с обменом информацией. @ **authentication system exchange** проверка подлинности с обменом информацией. @ **authentication system problem** задача проверки на достоверность.

authenticator [ɔ:'θentikeɪtə] *n.* аутентификатор (избыточная информация, добавляемая в сообщение для его аутентификации).

authenticity [ɔ:'θentisɪti] *n.* подлинность. @ **authenticity system** в криптологии – система с проверкой подлинности.

authorized [ɔ:θə'raɪzd] *adj.* 1 санкционированный; 2 назначенный. @ **authorized key** в криптологии – назначенный ключ. @ **authorized originator for messages** в криптологии – санкционированный источник сообщений.

authority [ɔ:θə'riti] *n.* 1. полномочие; 2. авторитет, крупный специалист. @ **authority on encryption** крупный специалист в области шифрования.

autoclear [ɔ:tou'kliə] *n.* @ в криптологии – автоматическое переключение (автоматический переключатель) с засекреченной на открытую связь.

autocorrelation [ɔ:tou'kɔ:ri'leɪʃən] *n.* автокорреляция. @ **autocorrelation function (ACF)** автокорреляционная функция. @ **autocorrelation function test** автокорреляционный тест (используется для проверки случайности двоичной последовательности).

autoencipherment [ˌɔːtuːen'saɪfəmənt] *n.* в криптологии – шифрование на автоключе.

autocode [ˌɔːtuː'kəʊd] *n.* автокод. @ Транслятор (обычно с языка низкого уровня).

autokey [ˌɔːtuː'kiː] *n.* @ в криптологии – автоключ. @ **autokey cipher system** в криптологии – автоключевая шифрсистема (каждая буква открытого/шифрованного текста сообщения, полученная в результате расшифрования/зашифрования очередной буквы шифрованного/открытого текста, используется в качестве ключа для расшифрования/зашифрования следующей). @ **autokeying** *n.* в криптологии – 1. шифрование на автоключе; 2. формирование автоключа.

automated [ɔː'təmətɪd] *adj.* автоматизированный. @ **automated classification and interface adapter (ACID)** автоматическая классификация и интерпретация данных. @ **automated computing equipment (ACE)** автоматический вычислитель. @ **automated data processing (ADP)** автоматическая обработка данных, применение ЭВМ. @ **automated cryptanalysis** автоматизированный (компьютерный) криптоанализ. @ **automated key distribution system (AKDS)** система автоматизированного распределения ключей. @ **automated key distribution** автоматизированное распределение ключей.

auto-manual [ˌɔːtuː'mænjuəl] *adj.* полуавтоматический. @ **auto-manual system** полуавтоматическая система; программируемое переносное криптографическое оборудование.

automatic [ɔː'təmətɪk] *adj.* автоматический. @ **automatic key distribution center (AKDC)** центр автоматического распределения ключей. @ **automatic key management** в криптологии – автоматическое управление ключами. @ **automatic remote rekeying** автоматический удаленный ввод ключа (процедура, применяемая для смены ключа в расположенном на удалении криптооборудовании и не требующая участия местного обслуживающего персонала).

automorphism [ˌɔːtuː'mɔːfɪzəm] *n.* автоморфизм. @ Изоморфизм алгебраической системы на себя называется автоморфизмом. Изоморфизм – это очень общее понятие, которое употребляется в различных разделах математики. В общих чертах его можно описать так: Пусть даны два множества с определённой структурой (группы, кольца, линейные пространства и т. п.). Биекция между ними называется изоморфизмом, если она сохраняет эту структуру. Такие множества со структурой называются изоморфными. Изоморфизм всегда задаёт отношение эквивалентности на классе таких множеств со структурой.

auto-session [ˌɔːtuː'seɪʃən] *adj.* автоматически генерируемый для сеанса. @ **auto-session key** в криптологии – автоматически генерируемый сеансовый ключ.

auxiliary (AUX, aux) [ɔː'gɪljərɪ]. @ В операционных системах на микро-ЭВМ – логическое имя файла, соответствующего последовательному каналу связи. *adj.* вспомогательный; вторичный. @ **auxiliary key (A-key)** в криптологии – вторичный ключ.

avail [ə'veɪl] *v.* быть полезным, помогать. # **of no avail** бесполезный. # **to avail (oneself) of** воспользоваться чем-л. # **to be of avail** иметь значение

available [ə'veɪlə'bəl] *adj.* 1. имеющийся; наличный; 2. доступный; 3. пригодный. # **to be available** иметься. # **to become available** стать доступным. # **to make available** делать доступным; обеспечивать.

avalanche ['ævələ:nʃ] *n.* 1. лавина; 2. лавинный процесс. @ в криптологии – "снежная лавина" (свойство блочных шифров реагировать на небольшие изменения на входе лавинообразными изменениями на выходе уже после нескольких циклов работы). @ **avalanche multiplication** лавинное умножение.

average ['ævərɪdʒ] *adj.* средний; промежуточный; *v.* 1. в среднем равняться (содержать), в среднем давать; 2. выводить среднее число; усреднять (*матем.*); *n.* среднее число; средняя величина. # **on the average** в среднем.

aware [ə'weə] *adj.* сознающий. # **to be aware of** знать, осознавать

away [ə'weɪ] *adv.* 1. на некотором расстоянии; 2. вдали. # **far away** далеко; дальний, отдаленный

-ary stiff. – арный. @ **N.-ary alphabet** N.-арный алфавит (алфавит N. знаков).

В*

back ['bæk] *adv.* 1. назад, обратно; 2. позади; *adj.* задний; *v.* поддерживать. @ **"back-break"** вскрывать (криптограмму) "задним числом" (то есть по прошествии некоторого периода времени, за который информация, полученная в результате вскрытия, успевает устареть и потерять свою актуальность) . # **back and forth** взад и вперед, туда и обратно. # **as far back as** еще, уже

backdoor *n.* = **trapdoor**

background ['bækgraʊnd] *n.* 1. фон программы. 2. фон, задний план; 3. фоновый. @ О задаче, программе или процессе, выполняемых на фоне других задач, программ или процессов. *Ср.* **foreground**. 4. основа; 5. происхождение; 6. подготовка, образование; опыт; 7. предпосылки; история вопроса; *adj.* фоновый. # **background of experience** накопленный опыт. # **historical background** история вопроса.

backup (BAK) ['bæk'ʌp] *n.* 1. резервная копия, резервный экземпляр; резервный ресурс; 2. резервирование; *v.* создавать резервную копию; *adj.* резервный.

backward ['bækwəd] *adj.* отстающий. @ **backward asymmetric encryption** в криптологии – шифрование с обратной асимметрией (ключ отправителя не может быть определен по ключу получателя). @ **backward error analysis** обратный анализ ошибок.

backward error correction (backward correction) ['bækwəd 'erə kə'rekʃən] исправление ошибок пе-респросом. @ Исправление ошибок в канале передачи посредством обнаружения их приемником, когда последний реагирует на лю-

бую ошибку в принятом блоке путем отправления передатчику запроса на повторную передачу блока.

backward read ['bækwəd ri:d] чтение в обратном направлении.@ Чтение при обратной перемотке ленты.

backward reference ['bækwəd 'refrəns] ссылка назад.@ Использование идентификатора, определенного выше.

backward-chaining ['bækwəd- 'tʃeɪnɪŋ] вывод «от цели к фактам».@ В экспертных системах и автоматическом доказательстве теорем – способ рассуждений, при котором для доказательства истинности утверждения делается попытка доказать истинность утверждений, из которых оно непосредственно следует; процесс продолжается до тех пор, пока рассуждение не дойдет до известных фактов или не будет получено утверждение, для которого нет правил.

Baconian *adj.* бэконовский,@ **Baconian cipher** бэконовский шифр, названный по имени английского философа Ф. Бэкона, который изобрел этот шифр)

bad-guy ['bæd'gai] в криптологии – 1. злоумышленник; 2. криптоаналитик (противника).

balanced ['bælənst] *adj.* уравновешенный, сбалансированный.@ **balanced function** сбалансированная функция (двоичная функция от n переменных, таблица истинности которой содержит 2^{n-1} нулей).

band (Bd, bd) [bænd] *n.* 1. полоса.@ Часть спектра частот, лежащая в пределах границ, определяемых в соответствии с некоторыми требованиями или функциональными аспектами данного сигнала или канала передачи. Термин употребляется также в значении ширина полосы. 2. зона; 3. лента; *v.* 1. собраться; 2. объединять(ся).@ **band scrambler** в криптологии – спектрально-полосный скремблер.@ **band scrambler-inverter** в криптологии – спектрально-полосный скремблер с инверсией отдельных полос.@ **band shift** сдвиг частотных полос.@ **band shift inverter** в криптологии – скремблер со сдвигом частотных полос и инверсией частот.@ **band splitting** разделение спектра сигнала на отдельные полосы.

band splitter = band scrambler

band matrix [bænd 'meɪtrɪks] ленточная матрица.@ Матрица, все элементы которой расположены на нескольких диагоналях, близких к главной диагонали

band printer [bænd 'prɪntə] ленточное печатающее устройство.@ Построчно-печатающее устройство с шрифтоносителем в виде вращающейся металлической ленты.

band limited channel [bænd 'lɪmɪtɪd 'tʃænl] канал с ограниченной полосой.@ Канал передачи с конечной шириной полосы.

bandgap ['bænd'gæp] *n.* межполосной промежуток.

bandpass ['ænd.pa:s] *n.* полоса частот.@ **band splitting** разделение спектра сигнала на отдельные полосы.@ **bandpass limiter (BPM)** полосовой ограничитель.

bandpass filter (BPF) полосовой фильтр. @ Фильтрующее устройство, пропускающее только те составляющие преобразования Фурье, частота которых лежит в пределах между двумя критическими значениями.

band-stop (-reject) filter ['bænd,stɒp(rɪ'dʒekt) 'fɪltə] режекторный фильтр. @ Фильтрующее устройство, пропускающее только те составляющие преобразования Фурье, частота которых лежит ниже одной (нижней) критической частоты или выше другой (верхней) критической частоты.

bandwidth (BW, bw) ['bænd,wɪdθ] ширина полосы. @ Характеристика канала передачи.

base [beɪs] *n.* 1. основа, основание; 2. основание системы счисления, уровень основной; 3. база, опорный пункт; *v.* 1. основывать, базировать; 2. закладывать основание; *adj.* основной. @ **base key** в криптологии – основной ключ.

basic ['beɪsɪk] *adj.* 1. основной; 2. фундаментальный; 3. поисковый. @ **basic cryptanalysis** элементарный криптоанализ (основы криптоанализа). @ **basic automatic checkout equipment (BACE)** основная аппаратура автоматической проверки. @ **basic circuit** основная (принципиальная) схема. @ **basic concept** основное понятие. @ **basic instruction** ['beɪsɪk ɪn'strʌkʃən] исходная команда. @ **basic order circuit** ['beɪsɪk ɔ:'dɜ 'sə:kɪt] код основной команды. @ **basic processing unit (BPU)** центральный процессор. @ **basic research** проблемное исследование. @ **basic symbol** основной символ.

basic access method [beɪsɪk 'ækses 'meθəd] базисный метод доступа. @ В операционных системах IBM – группа методов доступа, не поддерживающих буферизацию и очередей.

basic direct access method (BDAM) ['beɪsɪk dɪ'rekt 'ækses 'meθəd] базисный прямой метод доступа. @ Метод доступа низкого уровня, при котором запись идентифицируется номером записи внутри файла или физическим адресом на устройстве.

basic disk operating system (BDOS) ['beɪsɪk dɪsk 'ɔpəreɪtɪŋ 'sɪstɪm] БДОС, базовая дисковая операционная система. @ Часть операционной системы микро- или персональной ЭВМ, обеспечивающая обмен с дисками или другими внешними устройствами. Как правило, в БДОС входят все машинно-зависимые части операционной системы.

basic indexed sequential access method (BISAM) ['beɪsɪk 'ɪndekst sɪ'kwɛnsjəl 'ækses 'meθəd] базисный индексно-последовательный метод доступа. @ Метод доступа, позволяющий обращаться к записям файла как последовательно, так и по ключу. Преобразования ключа в адрес осуществляется с помощью индекса, являющегося частью файла.

basic partitioned access method (BPAM) ['beɪsɪk pa:'tɪʃənd 'ækses 'meθəd] базисный библиотечный метод доступа. @ Метод доступа, обеспечивающий работу с большими записями переменной длины с использованием символических имен.

basic sequential access method (BSAM) ['beɪsɪk sɪ'kwɛnsjəl 'æksɪs 'meθəd] базисный последовательный метод доступа.@ Метод доступа низкого уровня, позволяющий последовательно обрабатывать записи физического файла.

basic telecommunication access method (BTAM) ['beɪsɪk 'telɪkə'mjuː-nɪ'keɪʃən 'æksɪs 'meθəd] базисный телекоммуникационный метод доступа.@ Метод доступа низкого уровня, обеспечивающий минимальные средства для работы с терминалом.

basis ['beɪsɪs] *n.* (*pl.* **bases**) 1. основание, базис; 2. исходный пункт; 3. база; 4. базис (векторного пространства).# **on a weight basis** в весовом отношении.# **on this basis** исходя из этого.

batch [bætʃ] *n.* 1. пакет.@ Совокупность данных или программ, обрабатываемых или перерабатываемых как единое целое; группа программ, выполняемых в пакетном режиме. 2. группа целей, партия; серия; *adj.* периодический.@ **batch key** в криптологии – групповой ключ.@ **batch design** проектирование с использованием групповой обработки данных.@ **batch entry** пакетный ввод (данных).@ **batch file (BAT)** командный файл.@ **batch mode** пакетный режим, режим пакетной обработки.@ **batch production** серийное производство.

batch control [bætʃ kən'trəʊl] контроль пакетов.@ Способ проверки информации в системах обработки данных, используемый для контроля пакетов входных данных, в частности на этапе их подготовки.

batch header [bætʃ 'hedə] заголовок пакета.@ Первый элемент пакета, содержащий информацию о его структуре.

batch job [bætʃ dʒɒb] пакетное задание.@ Задание, выполняемое в пакетном режиме.

batch processing [bætʃ 'prəʊsesɪŋ] пакетная обработка.@ Обработка данных или выполнение программ, при которых элементы пакета обрабатываются последовательно без вмешательства оператора.

batch trailer [bætʃ 'treɪlə] завершитель пакета.@ Последний элемент пакета, указывающий на его окончание.

batching ['bætʃɪŋ] *n.* 1. группирование; 2. сортировка.

batch-oriented ['bætʃ'ɔːrɪəntɪd] пакетный, пакетно-ориентированный.@ Предназначенный для обработки пакета или обработки в пакетном режиме.

batchwise ['bætʃwaɪz] *adv.* периодически.

B-Dienst (от нем. Beobachtungs-Dienst) "Служба наблюдения" (военно-морская спецслужба радиоперехвата гитлеровской Германии).

be [biː] *v.* (*sing.* **was**, *pl.* **vere**; **been**) 1. быть, существовать; 2. жить, находиться.# **to be** + *inf.* должен + инф.; может + инф.; намерен + инф.; состоит в том, чтобы + инф..# **to be about** собираться + инф..# **to be going** собираться + инф..# **to be of importance (value)** иметь значение.# **to be of interest** представлять интерес.# **to be of no help** быть бесполезным; не оказывать помощи.

Beale cipher в криптологии – шифр Билля.

bear [bɛə] *v.* (**bore**, **born**) 1. носить; 2. рождать; производить; 3. выдерживать; 4. иметь отношение; 5. опираться, основываться (**on**, **upon**); 7. поддержи-

вать.# **to bear in mind** помнить; учитывать.# **to bear a relation(ship) to** иметь отношение к.# **to bear a similarity** иметь сходство.# **to have a bearing on (upon)** иметь отношение к; влиять на.

Beaufort cipher в криптологии – шифр Бофора.

Beaufort square в криптологии – квадрат Бофора.

Beaufort square = Beaufort cipher

because [bi'kɔ:z] *conj.* потому что; так как.# **because of** из-за, вследствие.# **because of momentum** по инерции; по привычке.

before [bi'fɔ:] *prep.* 1. перед; 2. до; *conj.* прежде чем; до того как; *adv.* 1. впереди; 2. раньше, прежде.# **before long** скоро, вскоре.# **long before** задолго до (того как).# **shortly before** незадолго до (того как).# **well before** задолго до (того как).

begin [bi'ɡɪn] *v.* (**began, begun**) начинать(ся).# **to begin with** прежде всего, во-первых.

behalf [bi'ha:f] *n.* употребляется в выражениях: .# **in behalf of** ради.# **on behalf of** от имени.# **on my behalf** от моего имени.

benefit ['benɪt] *n.* польза, выгода; *v.* 1. извлекать пользу, выгоду из чего-л. (**by**); 2. приносить пользу; оказывать благоприятное влияние.# **for the benefit of** для, ради.# **to the benefit of** с выгодой для.# **without the benefit of** используя

best [best] *adj.* (*превосх. степень от good*) лучший; *adv.* лучше всего.@ **best of known attacks on a cipher** в криптологии – наилучший из методов криптоанализа данного шифра.@ **best possible cryptanalytic algorithm** в криптологии – наилучший криптоаналитический алгоритм.@ **best possible cryptanalytic algorithm** наилучший криптоаналитический алгоритм.# **best value** оптимальное значение.# **at best** в лучшем случае.# **to the best of our knowledge** насколько нам известно.# **to do one's best** делать все возможное.# **to make the best** использовать что-л. наилучшим образом.

between [bi'twi:n] *prep.* между.# **as between** в отношениях между.# **few and far between** немногочисленные и редкие

beyond [bi'jɒnd] *prep.* 1. по ту сторону; за; 2. вне, свыше; 3. позже; *adv.* вдали; на расстоянии.# **beyond the reach** недостижимый.# **to be (go) beyond (outside) the scope** выходить за пределы чего-л.

bicomposite [bi'kɒmpəzɪt] *adj.* двухсоставный.@ **bicomposite modulus N** в криптологии – двухсоставный модуль N .@ **bicomposite modulus N** двухсоставной модуль N .

bidirectional [bi'dɪrekʃənl] *adj.* двухсторонний.@ **bidirectional asymmetric encryption** в криптологии – шифрование с двухсторонней асимметрией (ключ получателя не может быть определён по ключу отправителя и наоборот).@ **bidirectional cipher** раздвоенный шифр (разновидность шифра колонной перестановки).@ **bidirectional key** в криптологии – двухсторонний ключ (может быть использован как для зашифрования, так и для расшифрования сообщения).

bifid ['baɪfɪd] *adj.* раздвоенный.

Big Brother is watching you [big ɪz 'brʌðə wɒtʃɪŋ ju:] в криптологии – "Большой Брат" следит за тобой.

bigram [bi'græm] *n.* биграмма (два символа текста).@ **bigram cipher** в криптологии – биграммный шифр.@ **bigram count (counting)** в криптологии – маркировка биграмм.@ **bigram frequency** в криптологии – частота встречаемости (появления) биграмм (в тексте).

bijection [bi:'dʒækʃən] биекция (взаимно однозначное соответствие).

bilateral [baɪ'lætərəl] *adj.* двухсторонний.@ **bilateral key** в криптологии – ключ, известный двум пользователям (ключ для двухсторонней связи).@ **bilateral key exchange** в криптологии – двухсторонний обмен ключами.

bijjective [bi:'dʒɛktɪv] *adj.* биективный, объективный.@ **bijjective public-key cryptosystem** в криптологии – биективная криптосистема с открытым ключом

bi-letter = two-letter

bilinear [bi:'laɪnə] *adj.* билинейный.@ **bilinear cipher** в криптологии – билинейный шифр

biliteral [bi:'lɪtərəl] *adj.* в криптологии – состоящий из пар символов, двухбуквенный.@ **biliteral cipher alphabet** @ шифралфавит, составленный из пар символов; *n.* двухбуквенная шифрсистема.@ **biliteral cipher system with variants** вариантная двухбуквенная шифрсистема (при зашифровании каждый символ открытого текста может заменяться на различные пары символов шифрованного).@ **biliteral cipher system** двухбуквенная шифрсистема (при зашифровании каждый символ открытого текста заменяется на два символа шифрованного).

binary (bin) ['baɪnəri] двоичный.@ **binary accumulator** двоичный накапливающий сумматор.@ **binary add(ing) circuit** схема двоичного сложения.@ **binary adder** двоичный сумматор.@ **binary additive stream cipher** шифр гаммирования с двоичной шифрующей (ключевой) последовательностью.@ **binary arithmetic** 1. двоичная арифметика; 2. двоичное арифметическое устройство.@ **binary asymmetric channel (BAC)** асимметричный канал передачи двоичных данных.@ **binary carry** двоичный перенос.@ **binary cell** двоичная ячейка, двоичный элемент.@ **binary chop** двоичный поиск, поиск делением пополам.@ **binary coded decimal (BCD) arithmetic** операции над числами в двоично-десятичном представлении.@ **binary coded information (BCI)** двоично-кодированная информация.@ **binary computer** двоичная вычислительная машина.@ **binary counter** двоичный счетчик.@ **binary cryptosystem** в криптосистема с двоичным ключом.@ **binary data** двоичные данные.@ **binary decade counter** двоичный декадный счетчик, двоично-десятичный счетчик.@ **binary decoder** двоичный дешифратор. **binary digit** 1. двоичный разряд, двоичная цифра; 2. двоичный символ.@ **binary divider** двоичный делитель.@ **binary encoding** двоичное кодирование.@ **binary fraction** двоичная дробь.@ **binary function** двоичная функция.@ **binary incremental representation** представление двоичными разностями, двоично-инкрементное представление.@ **binary information** двоичная информация.@ **binary internal number base** ос-

нование внутренней двоичной системы счисления. @ **binary key** в криптологии – двоичный ключ. @ **binary keyboard** двоичная клавиатура. @ **binary loader** абсолютный загрузчик. @ **binary message** двоичное сообщение. @ **binary multiplication** умножение в двоичной системе счисления (двоичное умножение). @ **binary multiplier** двоичный умножитель (двоичное множительное устройство). @ **binary number system** двоичная система счисления. @ **binary numeral** 1. двоичная цифра; 2. двоичное число. @ **binary output** 1. двоичное выводное устройство; 2. вывод двоичной информации. @ **binary pair** симметричный элемент с двумя устойчивыми состояниями. @ **binary phase-shift keying (BPSK)** двухпозиционная фазовая манипуляция. @ **binary point** двоичная запятая. @ **binary power** степень двойки (число вида 2^n , где n – целое). @ **binary quadratic form** бинарная квадратичная форма. @ **binary representation** двоичное представление. @ **binary scale (BS)** двоичная шкала. @ **binary scaler** 1. двоичный счетчик; 2. двоичное пересчетное устройство, двоичная пересчетная схема. @ **binary sequence generator** в криптологии – генератор двоичных последовательностей. @ **binary signal** двоичный сигнал. @ **binary stage counter** счетчик по модулю два. @ **binary storage device** двоичное запоминающее устройство. @ **binary substitution cipher** шифр двоичной замены. @ **binary switch** двоичный переключатель. @ **binary symmetric dependent channel (BSDC)** двоичный симметричный зависимый канал. @ **binary symmetric independent channel (BSIC)** двоичный симметричный независимый канал. @ **binary system** двоичная система счисления. @ **binary transfer scheme** двоичная схема цифрового дифференциального анализатора. @ **binary transversal filter (BTF)** двоичный трансверсальный фильтр. @ **binary tree representation** представление в виде двоичного дерева. @ **binary variable** двоичная переменная.

binary substitution = binary substitution cipher

binary-coded ['bainəri'koudɪd] двоично-кодированный. @ **binary-coded decimal notation** 1. двоично-десятичная запись. 2. двоично-кодированная десятичная система счисления, двоично-кодированное представление десятичных чисел. @ **binary-coded decimal representation** представление десятичных чисел в двоичном коде, двоично-кодированное представление десятичных чисел. @ **binary-coded decimal system** двоично-кодированная десятичная система, двоично-десятичная система. @ **binary-coded frequency-shift keying (BCFSK)** двухпозиционная частотная манипуляция. @ **binary-coded octal** двоично-восьмеричное число. @ **binary-coded output** двоично-кодированный вывод. @ **binary-coded representation** представление в двоичном коде, двоичное представление.

binary-image processor (BIP) ['bainəri'ɪmɪdʒ 'prousesə] процессор двухградационных изображений.

binary-to-analog (BA) converter ['bainəri'tu:'ænələg kən'vɜ:tə] преобразователь из двоичной цифровой формы в аналоговую.

binary-to-decimal (Bd, bd) ['baɪnəri'tu:'desɪməl] (преобразование) из двоичной системы счисления в десятичную.@ **binary-to-decimal conversion** преобразование из двоичного (представления) в десятичное.

binary card ['baɪnəri ka:d] двоичная карта.@ Перфокарта с нетекстовой информацией.

binary code ['baɪnəri kəʊd] 1. двоичный код.@ Представление в виде последовательности нулей и единиц. 2. программа в двоичном коде.@ Программный модуль в пригодном для выполнения виде, содержащий только машинные команды и константы.

binary (binomial) distribution ['baɪnəri baɪ'nəʊmjəl dɪs'trɪbjʊ:ʃən] биномиальное распределение.@ Основное дискретное распределение вероятностей для данных, характеризующихся частотой их появления.

binary dump ['baɪnəri dʌmp] двоичный дамп.@ Распечатка содержимого памяти в двоичном представлении.

binary format ['baɪnəri 'fɔ:mæt] двоичный формат.@ Формат с представлением данных в двоичной форме.

binary image ['baɪnəri 'ɪmɪdʒ] 1. двухуровневое изображение.@ Растровое изображение с двумя уровнями яркости. 2. двоичное изображение в памяти.

binary logic ['baɪnəri 'lɒdʒɪk] двузначная логика.@ Логика, оперирующая двумя значениями «истина» и «ложь».

binary notation ['baɪnəri nou'teɪʃən] двоичная запись.@ 1. Запись в виде последовательности нулей и единиц. 2. Представление числа в двоичной системе счисления.

binary number ['baɪnəri 'nʌmbə] двоичное число.@ Число, представленное в двоичной системе счисления.

binary operation ['baɪnəri ɔpə'reɪʃən] 1. бинарная операция.@ Операция над двумя аргументами. 2. двоичная операция.@ Операция над числами в двоичном коде.

binary relation ['baɪnəri rɪ'leɪʃən] бинарное отношение.@ Отношение между двумя множествами.

binary search ['baɪnəri sə:tʃ] двоичный поиск, поиск делением пополам.@ Метод поиска в упорядоченном множестве, на каждом шаге которого средний элемент множества сравнивается с искомым и в зависимости от результата сравнения выбирается половина множества для обработки на следующем шаге.

binary search tree ['baɪnəri sə:tʃ tri:] двоичное дерево (поиска).@ Двоичное дерево, с каждой вершиной которого связано некоторое значение ключа поиска таким образом, что все ключи в ее левом поддереве меньше, а в правом — больше.

binary semaphore ['baɪnəri 'seməfo:] двоичный семафор.@ Семафор, принимающий значение 0 и 1. Операция «занять», примененная к семафору, имеющему значение 1, равносильна пустой операции.

binary sequence ['baɪnəri 'si:kwəns] двоичная последовательность. @ Последовательность двоичных знаков. Такая последовательность, формируемая случайным или псевдослучайным способом и обычно имеющая известные статистические свойства, может быть использована либо в качестве модуля шума, либо как средство контроля синхронизации между передатчиком и приемником.

binary subtraction ['baɪnəri səb'trækʃən] двоичное вычитание. @ Вычитание в двоичной системе счисления.

binary symmetric channel (BSC) ['baɪnəri 'sɪmetrɪk 'tʃænl] двоичный симметричный канал. @ Двоичный канал связи, в котором случайные ошибки типа замены нуля единицей возникают с той же вероятностью, что и ошибки типа замены единицы нулем. В теории кодов с исправлением и кодов с обнаружением ошибок чаще всего предполагается, что канал связи является двоичным симметричным каналом.

binary synchronous communication (BSC, bisync) ['baɪnəri 'sɪŋkrənəs kə-'mju:nɪ'keɪʃən] двоичная синхронная (познаковая) передача. @ Протокол фирмы IBM, используемый для связи удаленных терминалов с центральной ЭВМ.

binary tree ['baɪnəri tri:] двоичное дерево. @ Дерево, каждая вершина которого имеет не более двух потомков.

binary-coded decimal digit (BCDD) ['baɪnəri'kəʊdɪd 'desɪməl 'dɪdʒɪt] двоично-десятичный код. @ Представление чисел, при котором каждая десятичная цифра записывается четырех битным двоичным эквивалентом.

bind [baɪnd] *v.* (**bound**) 1. связывать. @ Устанавливать связь имени и значения. 2. компоновать, связывать. 3. обязывать. # **to be bound** быть вынужденным, обязанным (**to**); направляться (**for**). # **to be bound up with** быть связанным с кем-л., чем-л.

binomial [baɪ'nəʊmjəl] *n.* бином, двучлен. @ **binomial series** биномиальный ряд.

binomial distribution [baɪ'nəʊmjəl dɪs'trɪbjʊ:ʃən] биномиальное распределение. @ Основное дискретное распределение вероятностей для данных, характеризующихся частотой их появления.

birthday ['bɜ:θdeɪ] *n.* день рождения. @ **birthday attack** в криптологии — криптоанализ на основе парадокса дней рождения. @ **birthday paradox** в криптологии — парадокс дней рождения.

bit (binary digit) [bɪt ('baɪnəri 'dɪdʒɪt)] *n.* бит, двоичный разряд. @ **bit of a key** в криптологии — бит ключа. @ **m-bit cipher text** шифр с обратной связью по *m* битам (предшествующего) шифртекста. @ **bit cell** одноразрядный регистр. @ **bit handling** поразрядные операции, операции над разрядами. @ **bit loss** потеря (выпадение) двоичного разряда. @ **bit manipulation** поразрядные операции, операции над разрядами. @ **bit operation** битовая операция. @ **bit pattern** двоичный код; маска, комбинация разрядов; в криптологии — битовая комбинация (набор битов) (напр, для представления знака кода). @ **bit plane** матрица одного разряда. @ **bit rate** скорость передачи в битах. @ **bit se-**

rial побитовый.@ **bit slot** время передачи бита, такт передачи.@ **bit stream cipher** поточный шифр с двоичной шифрующей (ключевой) последовательностью.@ **bit stuffing** вставка битов, подстановка битов.@ **bit substitution cipher** в криптологии – шифр побитовой замены.@ **bit time** время передачи бита, такт передачи.

bit density [bit 'densɪtɪ] плотность записи.@ Число битов, записываемых на единицу длины носителя.

bit flipping [bit 'flɪpɪŋ] 1. поразрядные операции, операции над разрядами; 2. «жонглирование битами».@ О системном программировании или об изолированных приемах программирования.

bit image [bit 'ɪmɪdʒ] двоичный образ, битовый образ.@ Представление в виде двоичного массива.

bit map [bit mæp] 1. битовый массив; растр.@ Представление данных (обычно графического изображения), при котором каждому элементу данных (точке изображения) соответствует один или несколько разрядов памяти, адрес которых определяется номером элемента, а значение описывает состояние элемента данных, например, цвет точки изображения, состояние блока памяти. 2. буфер изображения.

bit mapping [bit 'mæpɪŋ] побитовое отображение.@ Метод отображения информации на экране дисплея, при котором каждому элементу изображения соответствует один или несколько битов в памяти.

bit matrix [bit 'meɪtrɪks] битовая матрица.@ Двумерный массив, в котором каждый элемент равен нулю или единицу.

bit stream generator = binary sequence generator

bit string [bit strɪŋ] строка битов.@ Тип данных в языках программирования, обеспечивающий работу с последовательностями двоичных разрядов как со строками.

bit-BLT (bit block transfer) [bit blɒk 'trænsfɜː] пересылка строки битов.@ Операция пересылки последовательности разрядов произвольной длины с адресацией с точность до бита.

bit-by-bit [bɪt'baɪ'bɪt] поразрядный.@ **bit-by-bit encryption** побитовое шифрование.

bit-cipher feedback [bit 'saɪfə 'fiːd,bæk] обратная связь по битам шифртекста.

bit-differences [bit'dɪfrənsɪz] различия в битах.

bit-interleaved [bɪt,ɪntə'liːvɪt] битмультиплексный.@ О передаче данных, при которой по одному физическому каналу последовательно передаются биты разных сообщений.

bit-interleaving [bɪt,ɪntə'liːvɪŋ] чередование битов.

bit-length [bɪt,leŋθ] в криптологии – длина (сообщения/ключа) в битах.

bitmap [bɪt'mæp] двоичное (побитовое) отображение.@ **bitmap color mask** цветовая маска.

bitmap extrude ['bitmæp eks'tru:d] растровая экструзия. @ Растровая экструзия – обтекание фигур и растровых изображений текстом.

bit-map(ped) display [bit' mæp(t) dɪs'pleɪ] (растровый) дисплей с поточечной адресацией, дисплей с общей памятью. @ Организация взаимодействия растрового дисплея с процессором, при которой каждой точке изображения соответствует один или несколько разрядов памяти в адресном пространстве ЭВМ; изменяя содержание ячеек памяти, программа изменяет изображение на экране.

bit-map(ped) graphics [bit'mæp(t) g'ræfɪks] растровая графика.

bit-organized memory [bit'ɔ:gənəɪzd 'meməri] память с поразрядной выборкой.

bit-oriented cipher feedback = bit-cipher feedback

bitpad ['bitpæd] планшетный цифратор. @ Устройство для оцифровки положения пера.

bits per inch (BPI, bpi) [bits pə: ɪntʃ] бит на дюйм. @ Единица измерения плотности записи информации на магнитном носителе.

bits per second (BPS, bps) [bits pə: 'sekənd] бит в секунду, бит/сек.

bit-security [bit'si'kjʊərɪti] в криптологии – стойкость по битам (невозможность определения отдельных битов открытого текста по имеющему шифрованному тексту).

bit-sequence [bit'si:kwəns] битовая двоичная последовательность.

bit(-)serial [bit'siəriəl] поразрядный. @ О передаче или обработке данных, при которой последовательно передаются или обрабатываются разряды.

bit-slice architecture [bit'slaɪs 'a:kɪtektʃə] разрядно-модульная архитектура

bit-slice processor [bit'slaɪs 'prəʊsesə] секционированный процессор, разрядно-модульный процессор, процессорная секция.

bitstring [bit'striŋ] строка битов.

bit-timing recovery (BTR) [bit'taɪmɪŋ rɪ'klɒvəri] восстановление тактовой синхронизации символов

bitwise addition [bit'waɪz ə'dɪʃən] поразрядное сложение. @ Операция над двоичными числами, при которой каждый разряд результата равен сумме по модулю 2 соответствующих операндов.

bitwise [bit'waɪz] *adj.* побитовый, поразрядный; *adv.* побитово, поразрядно. @ **bitwise operation** поразрядная операция. @ **bitwise XOR** побитовое исключение ИЛИ.

bitwise substitution cipher = bit substitution cipher

black [blæk] *adj.* 1. черный; 2. шифрованный, зашифрованный. @ **black box** в криптологии – блок обработки шифрованной информации. @ **black box cryptanalysis** в криптологии – криптоанализ по методу "чёрного ящика". @ **black box designation** в криптологии – обозначение систем, линий и аппаратуры связи для передачи и обработки шифрованной информации. @ **black box**

side в криптологии – сторона шифратора, обрабатывающая секретные данные. @ **black chamber** в криптологии – "чёрный кабинет".

"**black Code**" "Черный" код (американский дипломатический код, выкраденный итальянской спецслужбой из посольства USA в Италии незадолго до второй мировой войны).

"**black(-)box**" [blæk bɒks] "черный ящик".

black(-)box(-)model [blæk bɒks 'mɒdl] модель «черного ящика». @ Модель, описывающая только входы и выходы системы, но не внутреннее устройство системы. Например, математическая модель «черного ящика» – это просто совокупность множеств **X** и **Y** (**X** соответствует входам, **Y** – выходам); если оператор **F**, связывающий их (**Y = F(X)**), и предполагается существующим, то он считается неизвестным.

black-and-white display (BW-display) [blæk'ænd'waɪt dɪs'pleɪ] черно-белый дисплей; монохромный дисплей

blackboard [blæk'bɔ:d] *n.* рабочая область. @ В экспертных системах – часть базы данных, содержащая факты, полученные в процессе логического вывода, доступная всем компонентам вывода и используемая для взаимодействия между ними.

blank [blæŋk] *n.* 1. пробел, символ «пробел»; 2. пустой; 3. пробел, пропуск, пауза, пустое место; 4. в криптологии – пробел (в тексте); *v.* запирать. # **blank run** холостой ход.

blind [blaɪnd] *adj.* слепой. @ **blind signature scheme** схема слепой цифровой подписи, схема цифровой подписи вслепую.

blind keyboard [blaɪnd 'ki:bɔ:d] «слепая» клавиатура. @ Клавиатура, используемая для ввода данных без одновременного их отражения на экране дисплея.

block [blɒk] *n.* 1. блок. @ 1. Несколько последовательных логических записей, объединенных в одну физическую. 2. Единица доступа к диску или магнитной ленте. 3. В языках программирования – группа операторов и описаний, объединенных в одно целое. 4. В системах подготовки текстов – выделенный фрагмент, который можно удалить, переместить или выполнить над ним некоторое преобразование. *v.* блокировать. @ 1. объединять записи в блоки. 2. создавать условия, делающие невозможным продолжение. @ **block address** адрес блока. @ **block check** проверка по блокам. @ **block cipher with chaining** в криптологии – блочный шифр со сцеплением блоков. @ **block cipher** в криптологии – блочный шифр. @ **block constant** постоянная (признак) группы. @ **block design** блочная конструкция. @ **block diagram symbol** символ (графический знак) на блок-схеме. @ **block frequency analysis** криптоанализ на основе частоты встречаемости (появления) блоков в тексте. @ **block one-time pad of plaintext** блок открытого текста. @ **block one-time pad padding** холостое заполнение блока (ничего не значащей или фальшивой информацией). @ **block one-time pad size** размер (длина) блока. @ **block padding** в криптологии – холостое заполнение блока (ничего не значащей или фальшивой информацией). @ **block parity** поблочный контроль четности. @ **block repre-**

sentation блок-схема.@ **block retrieval** считывание блока (*в системе управления па-мятью*).@ **block size** размер (длина) блока.@ **block transfer** 1. поблочная передача; 2. пересылка блока, блочная пересылка.@ **block-by-block** в криптологии – поблочно (блоками).@ **block-cipher cryptanalysis** криптоанализ блочных шифров.@ **block-ciphering algorithm** алгоритм блочного шифрования.

block note = one-time pad (OTP)

block chaining (BC) [blɒk 'tʃeɪnɪŋ] сцепление блоков.@ Объединение блоков в одну последовательность при передаче с блочным шифрованием. Невозможность выделить порцию шифрования затрудняет расшифровку.

block buffer [blɒk 'bʌfə] буфер блоков.@ Буфер ввода-вывода при обмене блоками.

block cancel character [blɒk 'kænsəl 'kærɪktə] символ отмены блока.@ Управляющий символ, указывающий, что предшествующая часть блока должна быть проигнорирована.

block multiplexer channel [blɒk 'mʌltɪpleksə 'tʃænl] блок-мультиплексный канал.@ Мультиплексный канал с поблочной передачей данных.

block check character (BCC) [blɒk tʃek 'kærɪktə] символ контроля блока.@ Служебный символ, добавляемый к передаваемому блоку данных и содержащий контрольную сумму.

block code [blɒk kɔʊd] блочный код.@ Код с исправлением ошибок или код с обнаружением ошибок, в котором за одну операцию на вход кодера поступает фиксированное число (например, k) знаков, а на выходе генерируется кодовое слово, состоящее из большего числа знаков (например, n). Этот код иногда называют (n,k) -кодом, т. е. с длиной блока k и длиной кодового слова n .

block diagram [blɒk 'daɪəgræm] блок-схема, структурная схема.@ Схема, на которой графически представлены связи между элементами электронной схемы, например вычислительной.

block encryption [blɒk ɪn'krɪptʃən] в криптологии – блочное шифрование.@ Способ шифрования, при котором каждый передаваемый блок шифруется независимо.

block gap [blɒk ɡæp] межблочный промежуток.@ Часть поверхности носителя (диска или магнитной ленты) между последовательными блоками.

block head [blɒk hed] «шапка» блока, начало блока.@ Описание блока в начале того же блока.

block length [blɒk leŋθ] длина блока.@ Число байтов (иногда слов) в блоке.

block number [blɒk 'nʌmbə] номер блока.@ Число, идентифицирующее блок устройства (обычно диска) или файла. Физический номер задает адрес (номер дорожки и номер на дорожке). Логический номер обозначает порядковый номер блока на устройстве и отображается драйвером устройства в физический номер. Виртуальный номер задает номер блока внутри файла и ото-

бражается файловой системой в логический номер. В более простых системах понятия «логический номер блока» и «виртуальный номер блока» совпадают.

block sort [blɒk sɔ:t] блочная сортировка.@ Метод сортировки, при котором все множество разбивается на подмножества с близкими значениями ключа, каждое из которых затем сортируется отдельно.

blocked process [blɒkt 'prəʊses] блокированный процесс.@ Процесс, который имеет надлежащее описание, но не может выполняться дальше из-за отсутствия необходимого ресурса.

blocking *n.* ['blɒkɪŋ] в криптологии – разделение (текста) на блоки, формирование блоков (сообщения).@ **blocking order** блокирующая команда.@ **blocking oscillator (BO)** блокинг-генератор.

blocking factor [blɒkɪŋ 'fæktə] 1. коэффициент блокирования.@ Число записей в блоке. 2. емкость блока.

blockmark ['blɒkmɑ:k] *n.* маркер блока, блок-маркер.@ Маркер, указывающий конец информационной части блока диска.

block-oriented device [blɒk'ɔ:riəntɪd di'vaɪs] блочно-ориентированное устройство, устройство с поблочным доступом.@ Внешнее запоминающее устройство, обмен с которым производится блоками (например, диск).

block-structured language [blɒk 'strʌktʃəd 'læŋgwɪdʒ] язык с блочной структурой.@ Язык высокого уровня, в котором описание одного действия может включать описание объекта того же класса (например, вложенные процедуры или вложенные блоки).

bogus ['bougəs] *adj.* поддельный.@ **bogus key** поддельный ключ.

"bomber" operator ['bɒmə 'ɒpəreɪtə] в криптологии – оператор "Бомбы".

book [buk] *n.* книга.@ **book cipher** книжный шифр (шифр, составленный с использованием книги шифрования).

book code = book cipher

Boolean [bu:lɪn] Булева алгебра.@ **Boolean algebra system of notation** система обозначений Булевой алгебры.@ **Boolean calculation** Булево исчисление.@ **Boolean expression** логическое (Булево) выражение.@ **Boolean function** Булева функция.@ **Boolean matrix** Булева матрица.@ **Boolean operation** логическая (Булева) операция.@ **Boolean operator** знак логической (Булевой) операции.@ **Boolean tree** Булево дерево.@ **Boolean value** логическое (Булево) значение.@ **Boolean variable** логическая (Булева) переменная.

boot [bu:t] *n.* начальная загрузка. См. **bootstrap**. *v.* загружать(ся), запускать(ся).

boot protection encryption [bu:t prə'tekʃən ɪn'krɪptʃən] в криптологии – шифрование для защиты (от) начальной загрузки.

bootstrap ['bu:tstræp] *n.* 1. начальная загрузка.@ Считывание с внешнего носителя в память и выполнение программы, которая считывается, настраивается и запускает остальную часть системы. 2. раскрутка.@ Способ разработки программного обеспечения, при котором сначала разрабатывается простой вариант программы, используемый для реализации более сложных. Применя-

ется при разработке трансляторов и переносе программного обеспечения на другую ЭВМ. *v.* 1. загружать, запускать; 2. раскручивать. @ **bootstrap loader** начальный загрузчик, программа начальной загрузки (*обычно расположенная в ПЗУ*). @ **bootstrap loading** начальная загрузка.

bootstrap block ['bu:t,straep blɒk] блок начальной загрузки. @ Блок диска, автоматически считываемый при запуске системы и содержащий программу загрузки остальных частей системы с этого диска.

bootstrap memory ['bu:t,straep 'meməri] память начального загрузчика. @ ПЗУ, в котором записана программа начальной загрузки.

both [bəʊθ] *pron.* оба. # **both ... and** как ... так и; и ... и.

bottle ['bɒtl] *n.* бутылка, флакон. # **bottle-neck** узкое место.

box [bɒks] *n.* 1. прямоугольник, рамка. @ Изображение прямоугольника на блок-схеме, графике или экране дисплея. 2. блок; 3. коробка, ящик, кожух.

break [breɪk] *v.* (**broke**; **broken**) 1. ломать(ся), разрушать(ся); разлагать(ся) (**down**); 2. разразиться (**out**); 3. прорывать(ся) (**through**); 4. в криптологии – вскрывать, дешифровывать; *n.* 1. поломка; 2. разрыв; 3. прерыватель; 4. в криптологии – вскрытие (ключа или шифра). @ **break a cipher** вскрывать шифр. @ **break a code** вскрывать код. @ **break a cryptogram** дешифровывать криптограмму. @ **break a cryptographic protocol** вскрывать криптографический протокол. @ **break a text into digraphs** разбивать текст на биграммы. @ **break in a system** в криптологии – взламывать (вторгаться в) систему. @ **break in** *v.* взламывать, вторгаться; *n.* взлом, вторжение; *n.* в криптологии – взлом, вторжение. @ **break-in of a system** в криптологии – взлом системы, вторжение в систему. @ **break into "Enigma"** вскрытие "Энигмы". @ **break length** в криптологии – длина шифртекста, достаточная для вскрытия ключа. @ **break point** 1. точка разрыва (прерывания); 2. точка останова. @ **break storage cycle** прерывистый цикл работы запоминающего устройства. @ **break time of a base key** в криптологии – время, требуемое для вскрытия основного ключа.

break key [breɪk ki:] клавиша прерывания. @ Управляющая клавиша, вызывающая прерывание работы программы.

breakability [breɪk,ə'bɪlɪtɪ] *n.* в криптологии – вскрываемость, дешифруемость.

breakable [breɪk'eɪbl] *adj.* в криптологии – вскрываемый, дешифруемый, поддающийся вскрытию или дешифрованию. @ **breakable cipher** вскрываемый шифр.

breakdown ['breɪkdaʊn] *n.* 1. упадок; 2. разрушение; нарушение; авария; пробой; 3. провал; прекращение; 4. распределение; классификация; разборка (на части).

breaker *n.* [breɪkə] в криптологии – криптоаналитик (букв взломщик).

breakeven ['breɪki:vən] *n.* (результат и т. п.) без прибыли и убытка.

breaking [breɪkɪŋ] *n.* вскрытие. @ **breaking algorithm** алгоритм вскрытия (шифра). @ **breaking program** программа вскрытия (ключа или шифра).

breakpoint ['breɪkpɔɪnt] *n.* 1. контрольная точка. @ Точка программы, в которой ее выполнение прерывается и управление передается отладчику. 2. точка прерывания. @ Адрес команды, выполняющейся в момент прерывания. После завершения обработки прерывания выполнение программы продолжается с этого адреса. @ **breakpoint instruction** команда контрольного перехода или остановки.

breakthrough ['breɪk'θru:] *n.* 1. прорыв; 2. важное научное открытие; техническое достижение.

bring [brɪŋ] *v.* (**brought**) 1. приносить; доставлять; 2. вызывать, влечь за собой (**about**); 3. осуществлять, приводит к (**about**); 4. выявлять (**out**); 5. снижать (**down**); 6. доводить до (**to**); 7. воспитывать (**up**). # **to bring (call) into action (play)** приводить в действие, осуществлять. # **to bring (call) into being** вводить в действие, создавать. # **to bring forward (forth)** выдвигать. # **to bring home** убедить кого-л.; довести до сознания. # **to bring to notice** обратить внимание на. # **to bring to correspond** приводить в соответствие.

British Telecom Cryptoalgorithm (B-Crypt) алгоритм шифрования, разработанный английской фирмой "Бритиш Телеком".

broad [brɔ:d] *adj.* широкий, обширный. # **broadly speaking** вообще говоря.

broadband (BB, bb) ['brɔ:dbænd] широкополосный.

broadband coaxial systems ['brɔ:dbænd 'kou'æksjəl 'sɪstɪms] широкополосные коаксиальные системы. @ Системы связи на базе коаксиального кабеля, используемые для организации широкополосных сетей. Полоса частот коаксиального кабеля разбивается на несколько каналов с использованием частотного уплотнения.

broadband LAN ['brɔ:dbænd læn] локальная сеть с модулированной передачей, широкополосная локальная сеть. @ Локальная сеть, в которой сигналы передаются с помощью модуляции несущей» при этом в одной среде передачи может передаваться несколько сигналов одновременно.

broadband networking ['brɔ:dbænd net'wɜ:kɪŋ] организация широкополосных сетей. @ Способ организации сетей, при котором для переноса аналоговых сигналов в среду передачи используется модулированная несущая.

broadcast ['brɔdka:st] *n.* в криптологии – циркулярная передача, циркулярная связь; *v.* передавать сообщение (*всем узлам сети, терминалам, заданам, ждущим события*); *adj.* радиовещательный. @ **broadcast authentication** аутентификация при циркулярной передаче. @ **broadcast authentication channel** канал циркулярной передачи. @ **broadcast authentication encryption scheme** схема шифрования для циркулярной связи. @ **broadcast channel** канал циркулярной передачи. @ **broadcast encryption scheme** схема шифрования для циркулярной связи.

broadcast address ['brɔdka:st ə'dres] «широковещательный» адрес. @ В локальных сетях – адрес, указывающий, что сообщение адресовано всем станциям данной сети.

broadcast network ['brɒdkɑːst 'netwɜːk] широковещательная сеть. @ Сеть ЭВМ (обычно локальная сеть), в которой сигнал, передаваемый одной станцией сети, может быть воспринят всеми ее другими станциями.

broadcasting ['brɒdkɑːstɪŋ] широковещательная передача. @ Алгоритм маршрутизации сообщений, при котором сообщения передаются всем узлам сети.

broadcasting *n.* = **broadcast**

broaden ['brɒdn] *v.* 1. расширять(ся); 2. уширять.

broadening ['brɒdnɪŋ] *n.* уширение.

brute [brut] *adj.* грубый. @ **brute-force attack** атака на шифр с применением грубой силы (силовая атака на шифр).

brute-force search = **brute-force attack**

build [bɪld] *v.* 1. встраивать; 2. создавать, конструировать. @ **build a trap-door into a knapsack one-way function** в криптологии – встраивать лазейку (потайной ход) в одностороннюю ранцевую функцию. @ **build a secure cryptographic system** создавать надежную криптографическую систему.

building ['bɪldɪŋ] *n.* 1. здание; 2. строительство. @ **building block principle** блочный принцип.

build-up ['bɪldʹʌp] *n.* 1. построение; образование; скопление; 2. создание; 3. развитие; рост; 4. нарастание; 4. пространственные комментарии; *v.* 1. монтировать, собирать; 2. воздвигать, строить.

built-in ['bɪlt'ɪn] *adj.* 1. встроенный, предопределенный, вмонтированный. @ О программном объекте, который является частью языка или системы программирования и может быть использован без описания в программе пользователя. 2. встроенный. @ Являющийся конструктивной частью. @ **built-in encryption module** встроенный модуль шифрования. @ **built-in function** 1. встроенная функция; 2. стандартная функция (напр. из стандартной библиотечной программы). @ **built-in key** вмонтированный ключ. @ **built-in logic block observer (BILBO)** встроенный логический блок наблюдения. @ **built-in pulser (BIP)** встроенный генератор импульсов. @ **built-in storage** встроенное запоминающее устройство.

built-in check ['bɪlt'ɪn tʃek] 1. встроенный контроль, встроенная проверка. @ Операции проверки значения переменных, вставляемые транслятором в тело программы. 2. встроенные средства проверки. @ Аппаратура проверки обрабатываемых или передаваемых значений.

built-in macro instruction ['bɪlt'ɪn 'mækrou ɪn'strʌkʃən] встроенная макрокоманда. @ Команда ассемблера, транслируемая в несколько машинных команд.

built-in type ['bɪlt'ɪn taɪp] предопределенный тип, встроенный тип. @ В языках программирования с развитой системой типов – тип данных, определение которого является частью языка (например, «целое», «логическое», «строка»).

bulk [bʌlk] *n.* 1. масса, основная часть чего-л.; большое количество 2. объем, вместимость. # **in bulk** в целом; в массе.

bulk encryption [bʌlk ɪn'krɪptʃən dɪ'vaɪs] групповое шифрование (одновременное шифрование информации, передаваемой по всем каналам многоканальной телекоммуникационной системы).@ **bulk encryption device** групповой шифратор.

bulk sampling [bʌlk 'sɑ:mplɪŋ] выборка из «кучи».

bulk storage [bʌlk 'stɔ:ɹɪdʒ] 1. внешняя память, внешнее запоминающее устройство.

bulky [bʌlkɪ] *adj.* большой; громоздкий; объемный.

burst [bɜ:st] *n.* 1. пакет. 2. взрыв; 3. вспышка; *v.* разрывать.@ Разделять распечатку на фальцованной бумаге на страницы.@ **burst communication (transmission)** сверхбыстрая пакетная связь (передача).@ **burst performance** максимальная производительность (*при обработке специально подобранной задачи*).

burst error (error burst) [bɜ:st 'erə] пакет ошибок.@ Комбинация ошибок, которая воспринимается как единая ошибка, если ошибочными являются ее определенные элементы («первый» и «последний»), причем промежуточные элементы не обязательно ошибочны.

burst mode [bɜ:st mɔ:ɹd] монопольный режим, пакетный режим.@ Режим работы мультиплексного канала, при котором канал временно выделяется одному устройству для пересылки блока информации (пакета).

busting [bɜ:stɪŋ] *n.* в криптологии – вскрытие (шифра или ключа).

but [bʌt] *adv.* только лишь, всего лишь; *prp.* кроме; *conj.* но, а.# **but for** если бы не.# **all but** почти; кроме; чуть не; далеко не.# **cannot but** не может не + инф.# **last but one** предпоследний.# **next but one** через одного.# **nothing but** только лишь.

button [bʌtn] *n.* кнопка, клавиша.

by [baɪ] *prp.* 1. у, при, около; 2. посредством; 3. согласно, по; 4. к (о времени); 5. на.# **by the agency** посредством.# **by all means** во что бы то ни стало; конечно, безусловно, обязательно.# **by and by** постепенно; вскоре.# **by and large** вообще говоря.# **by as many (much)** на столько же.# **by chance** случайно.# **by constant to (with)** по сравнению с.# **by degrees** постепенно.# **by dint of** посредством.# **by eye** на глаз.# **by far** значительно; несомненно.# **by hand** вручную.# **by means of** посредством; с помощью.# **by no means** никоим образом; до сих пор.# **by now** к тому времени.# **by turns** по очереди.# **by (in) virtue of** благодаря (чему-л.), посредством (чего-л.); в силу, на основании (чего-л.).# **by the way** между прочим.# **by way of** в качестве; с целью; через, посредством, путем.# **by which means** посредством чего.# **far and by** в общем, вообще говоря.

by-pass [baɪ'pa:s] *n.* обход.@ **by-pass mode** режим обхода (режим работы с обходом) (открытый текст подаётся, минуя криптографическое устройство, и в силу этого не подвергается шифрующим преобразованиям).

byte [baɪt] *n.* байт (набор из 8 бит), слог.@ **byte machine** вычислительная машина с байтовой организацией.@ **byte of a key** байт ключа.@ **byte per sec-**

ond байт в секунду. @ **byte substitution table** таблица байтовых замен (одномерный массив из 256 чисел от 0 до 255, каждое из которых встречается в нём лишь единожды). @ **byte transposition cipher** шифр побайтовой перестановки.

byte instruction [baɪt ɪn'strʌkʃən] байтовая команда. @ 1. Команда операции над байтами. 2. Команда, занимающая один байт.

byte-interleaved [baɪt,ɪntə'li:vɪt] байт-мультиплексный. @ О передаче данных, при которой по одному физическому каналу последовательно передаются байты (символы) разных сообщений.

byte-multiplexer channel [baɪt'mʌltɪpleksə 'tʃænl] байт-мультиплексный канал. @ Мультиплексный канал с посимвольной (побайтовой) передачей данных.

byte-multiplexing [baɪt'mʌltɪpleksɪŋ] побайтовое мультиплексирование. @ Временное мультиплексирование, при котором каналу периодически выделяется время для передачи одного байта.

byte-organized memory [baɪt'ɔ:gənəɪzd 'meməri] память с побайтовой организацией. @ Память, данные в которой записываются и считываются по одному байту.

byte-oriented block-ciphering algorithm [baɪt'ɔ:riəntɪd blɒk'saɪfəɪŋ 'ælɡərɪdʒəm] в криптологии — алгоритм побайтового блочного шифрования (при зашифровании и расшифровании используются только операции над байтами).

byte-serial [baɪt'sɪəriəl] посимвольный, побайтовый. @ О передаче или обработке данных, при которой последовательно передаются или обрабатываются отдельные символы (байты), при этом все разряды каждого символа передаются или обрабатываются параллельно. Фоновые задачи выполняются в пакетном режиме.

C*

"Capstone" *n.* "Кэпстоун" ("Облицовочный камень") (название долгосрочной программы правительства USA по разработке открытых криптографические стандарты)

"Clipper" *n.* "Клиппер" название чипа для криптографической защиты информации в каналах аналоговой связи

"code breakers" "Взломщики кодов" (название книги американского писателя Д. Кана, посвященной истории криптологии с древних времен до наших дней)

"code Compilation Company" "Компания по составлению кодов" (название фиктивного коммерческого предприятия, служившего прикрытием для "Американского черного кабинета")

"Communication theory of secrecy systems" "Теория связи в секретных системах" (статья американского математика К. Шеннона, публикация в кото-

рой в 1949 г. ознаменовала наступление эры научной криптологии с секретными ключами).

cable ['keɪbl] *n.* 1. кабель; 2. трос; *v.* телеграфировать. @ **cable communication** кабельная связь. @ **cable interception** в криптологии — перехват в кабельной линии связи.

cable tapping = cable interception

cablegram ['keɪblgræm] каблограмма, телеграмма.

Caesar cipher в криптологии — шифр Цезаря

calculate ['kælkjuleɪt] *v.* 1. вычислять, считать; подсчитывать; рассчитывать; 2. думать, полагать. @ **calculate a encryption key given a decryption key** вычислять ключ зашифрования при известном ключе расшифрования.

calculating apparatus ['kælkjuleɪtɪŋ ˌæpə'reɪtəs] счетное устройство.

calculating integral ['kælkjuleɪtɪŋ 'ɪntɪgrəl] интеграл по замкнутому контуру.

calculating machine ['kælkjuleɪtɪŋ mə'ʃi:n] счетная вычислительная машина.

calculating speed ['kælkjuleɪtɪŋ spi:d] скорость вычисления.

calculating time ['kælkjuleɪtɪŋ taɪm] время счета.

calculation ['kælkjuleɪʃən] *n.* вычисление, подсчет, смета, калькуляция.

calculator ['kælkjuleɪtə] *n.* калькулятор, вычислитель.

calculus ['kælkjuləs] *n.* вычисление, вычисления, исчисление. @ **calculus of approximation** приближенное вычисление, численный метод. @ **calculus of residues** теория вычетов. @ **calculus of variations** вариационное исчисление.

call [kɔ:l] *n.* 1. вызов (*подпрограммы*), обращение (*к подпрограмме*). @ Передача параметров и управления подпрограмме или функции, которые выполняют необходимые действия и возвращают управление вызвавшей программе. 2. вызов, соединение. @ Установление логической или физической связи между двумя узлами сети передачи данных. *v.* 1. вызывать (*подпрограмму*), обращаться (*к подпрограмме*); 2. звать; 3. называть; 4. требовать; предусматривать (**for**); 5. называть (**forth**). @ **call address** адрес вызова (*подпрограммы*). @ **call by reference** передача параметра по ссылке. @ **call by value** передача параметра по значению. @ **call instruction** команда обращения, команда вызова подпрограммы. @ **call of zero (CZ)** вызов по нулю. @ **call sign** позывной сигнал. # **to call attention (to)** обращать внимание (на). # **to call (bring) into action (play)** приводить в действие; осуществлять. # **to call (bring) into being** вводить в действие, создавать.

call by name [kɔ:l baɪ neɪm] вызов по имени. @ Вызов, в котором явно указывается имя программы.

call by pattern [kɔ:l baɪ 'pætən] вызов по образцу. @ Вызов посредством задания образца, состоящего из условия и цели. При таком вызове управляющая система запускает все подпрограммы с удовлетворяющим образцу заголовком.

call sign cipher [kɔ:l 'sɪg 'saɪfə] шифратор позывных сигналов. @ Используется для шифрования позывных сигналов и другой сигнальной информации.

call up [kɔ:l ʌp] *v.* вызывать. @ **call up procedure** процедура вызова.

calligraphics display [kə'lɪgrəfiks dɪs'pleɪ] векторный дисплей.

calligraphy pen [kə'lɪgrəfi pen] каллиграфическое перо.

calling order ['kɔ:liŋ ɔ:'dɔ] вызывающая (отсылающая) команда.

calling sequence ['kɔ:liŋ 'si:kwəns] соглашение о связях. @ Последовательность команд, используемая в данной системе программирования для обращения к процедурам и передачи параметров и результатов.

callword [kɔ:l'wɔ:d] слово-позывной.

candidate ['kændɪdɪt] *n.* кандидат.

candidate for a key = candidate key.

candidate key ['kændɪdɪt ki:] 1. возможный ключ. @ В реляционной модели данных – отличное от первичного ключа подмножество атрибутов отношения, совокупность значений которых однозначно идентифицирует кортеж этого отношения. 2. возможный ключ (при криптоанализе).

canister ['kænɪstə] *n.* канистра (контейнер, используемый для хранения и транспортировки перфорированной или телетайпной ленты с ключевой информацией).

capacity [kæ'pæsɪtɪ] *n.* 1. разрядность; 2. допустимый диапазон чисел (для данного устройства); 3. мощность; 4. нагрузка; 5. производительность; 6. пропускная способность; 7. емкость; вместимость; *adj.* емкостной. # **in the capacity of** в качестве

capture ['kæptʃə] *v.* 1. захватить; 2. поймать; *n.* 1. захват; 2. область захвата
care [kɛə] *n.* 1. забота, уход; 2. внимание; осторожность. @ **capture a codebook** захватывать кодовую книгу. @ **capture all communications** перехватывать все сообщения. # **to exercise care** позаботиться. # **to take care (of)** заботиться; следить; принимать меры.

cargo ['kɑ:gou] *n.* груз. @ **cargo vector** в криптологии – вектор груза.

carrier (car) ['kæriə] *n.* 1. носитель тока; 2. носитель заряда; 3. носитель информации; 4. магнитный материал, несущий запись; 5. несущая (частота).

carrier-sense multiple access (CSMA) ['kæriə'sens 'mʌltɪpl 'ækses] множественный доступ с опросом несущей, метод доступа с опросом состояния канала. @ В сети ЭВМ или сети передачи данных – способ управления доступом к среде передачи, при котором все узлы подключены к общему каналу данных и каждый узел может принимать каждое сообщение; для передачи сообщения узел проверяет состояние канала, ждет его освобождения и затем начинает передачу сообщения.

carrier-sense multiple access and collision detection (CSMA/CD) protocol ['kæriə'sens 'mʌltɪpl 'ækses ænd kə'lɪzən detekʃən 'prəʊtəkol] метод доступа CSMA/CD. @ Множественный доступ с опросом состояния канала и разрешением конфликтов. Вариант метода доступа CSMA, при котором, если два узла

пытаются начать передачу одновременно, то оба ждут и возобновляют опрос состояния канала через случайный интервал времени.

carrier-to-noise ratio (CNC) ['kæriə'tu'nɔɪz 'reɪʃɪou] отношение сигнал-шум на частоте несущей.

carry ['kæri] *n.* 1. перенос, разряд переноса.@ Цифра, прибавляемая к старшему разряду суммы, когда сумма младших разрядов больше основания системы счисления. 2. перенос; *v.* 1. нести, поддерживать; 2. везти; 3. проводить (**on**); выполнять (**out**).@ **carry bit** разряд переноса, перенос.@ **carry circuit** цепь переноса.@ **carry clear** «нет переноса».@ **carry clearing operation** операция гашения переносов.@ **carry delay** задержка переноса.@ **carry digit** разряд переноса, перенос, цифра переноса.@ **carry handling facility** устройство для работы с переносами.@ **carry input** вход переноса.@ **carry output** выход переноса.@ **carry set** «есть перенос».@ **carry storage device** устройство запоминания переноса.@ **carry storage** ячейка для запоминания переноса.@ **carry-save adder (CSA)** сумматор с запоминанием переноса.

carry flag ['kæri flæg] признак переноса.@ Одноразрядный регистр или разряд слова состояния процессора, принимающий значение 1 («есть перенос»), если при выполнении команды произошел перенос из старшего разряда, и значение 0 («нет переноса»), в противном случае. Признак переноса используется командами условного перехода.

cascade [kæs'keɪd] *n.* каскад; *v.* каскадировать, включать каскадно; *adj.* каскадный.@ **cascade cipher** каскадный шифр.@ **cascade connection** каскадное соединение.@ **cascade linear feedback shift registers** каскадировать регистры сдвига с линейной обратной связью.@ **cascaded connection of shift registers** каскадное соединение регистров сдвига.@ **cascaded super encipherment** наложение шифров.

case [keɪs] *n.* 1. регистр клавиатуры; 2. оператор выбора. 3. случай; обстоятельство; дело; 4. заболевание; 5. судебное дело; 6. ящик; футляр.# **case history** история вопроса; история болезни.# **the case is (that)** дело в том (что).# **as the case may be** в зависимости от обстоятельства.# **as the case stands** при данном положении дел.# **as is usually the case** как это обычно имеет место.# **in case** если.# **in the case of** в случае.# **in any case** во всяком случае.# **in no case** ни в коем случае.# **in which case** и в этом случае.# **just in case** на всякий случай.# **this is far from being the case** это далеко не так, дело обстоит совсем не так.# **to be the case** иметь место, происходить.# **to meet the case** отвечать предъявленным требованиям.

cast [kɑːst] *n.* 1. приведение (типов); ядро (в языке Алгол-68). *v.* 1. приводить. 2. бросать, кидать, метать; отбрасывать; 3. отливать, лить (*металлы*).# **to cast doubt on** подвергать сомнению что-л.# **such being the cast** если дело обстоит так, в таком случае.

CAST (блочный алгоритм шифрования, разработанный сотрудниками транснациональной корпорации "Нортел Нетворкс" Карлайслом Адамсом и Стэффордом Таваресом).

category ['kætɪgəri] *n.* категория (пометка на документе, свидетельствующая о степени его секретности); категория.@ Совокупность объектов вместе с множеством морфизмов.

catoprical [kə'tɒprɪkəl] *adj.* катопрический.@ **catoprical cryptography** криптография с использованием зеркал.

cause [kɔːz] *n.* 1. причина; 2. случай, обстоятельство, дело; 3. ящик; *v.* 1. вызывать; причинять; 2. заставлять.# **be cause of** из-за, вследствие, благодаря.# **to be the cause** иметь место, происходить.# **in cause** если.# **in any cause** во всяком случае.

cellular ['seljʊlə] *adj.* 1. клеточный; 2. ячеичный, сотовый.

cellular automaton клеточный автомат.

cellular logic image processor (CLIP) процессор изображений на основе клеточной логики.

center ['sentə] *n.* центр.@ **center for Cryptologic History (CCH)** Центр истории криптологии.@ **center key** ключ центра (распределения ключей).

central ['sentrel] *adj.* центральный.@ **central Cipher Bureau (CCB)** Центральное шифровальное бюро (немецкое правительственное ведомство, занимавшееся перехватом и дешифрованием сообщений).@ **central Intelligence Agency (CIA)** Центральное разведывательное управление (шпионское ведомство USA, одной из функций которого являются организация и проведение радиошпионских операций).@ **central keying authority (CKA)** центр распределения (распространения) ключей (выдаёт ключи и образцы подписей абонентам сети связи, ведёт учёт их работы и выступает в качестве свидетеля или арбитра при возникновении споров).@ **Central Office for Cryptology** Центральная криптологическая служба (подразделение германской Федеральной разведывательной службы, занимающееся перехватом и дешифрованием сообщений).@ **Central Security Service (CSS)** Центральная служба безопасности (подразделение министерства обороны USA, находящееся в подчинении директора NSA и осуществляющее радиоперехват в интересах этого агентства).@ **Central Service for Security and Information Systems (CSSIS)** Центральная служба безопасности и информационных систем (французское правительственное ведомство, занимающееся перехватом и дешифрованием сообщений).

centralized ['sentrelaɪzd] *adj.* централизованный.@ **centralized key distribution** централизованное распределение ключей.@ **centralized key generation** централизованная генерация ключей.@ **centralized key generation** централизованная генерация ключей.@ **centralized key management** централизованное управление ключами.@ **Centralized COMINT Communications Center (CCCC)** Централизованный радиоразведывательный коммуникационный центр (ретрансляционная станция NSA USA, предназначенная для передачи радиоразведывательных данных).

centrally ['sentrelɪ] *adv.* центрально.@ **centrally-produced key** ключ, генерируемый в центре распределения ключей.

cepstrum [kep'strum] *adj.* кепстральный.@ **cepstrum analysis** кепстральный анализ.

certain ['sə:tn] *adj.* 1. некоторый; 2. определенный; несомненный; 3. *predic.* уверенный.# **for certain** наверняка, с уверенностью.# **to be (feel) certain** быть уверенным; быть определенным.# **to make certain of** удостовериться, убедиться.

certificate [sə:tifi'keit] *n.* сертификат (в криптологии – сообщение, содержащее ключ, подлинность которого устанавливается при помощи криптографической аутентификации).@ **certificate revocation list (CRL)** список аннулированных сертификатов.

certification [sə:tifi'keiʃən] *n.* 1. аттестация (проверка на соответствие определенным требованиям); 2. сертификация (доказательство соответствия нормам и стандартам); освидетельствование, удостоверение.@**certification of origination (receipt)** удостоверение источника (получателя).@ **certification authority (CA)** орган сертификации.

certificational [sə:tifi'keiʃənl] *adj.* сертификационный.@ **certificational weakness** сертификационная нестойкость (в криптологии – потенциальная возможность вскрыть шифр с помощью любого криптоаналитического метода, являющегося более эффективным по сравнению с полным перебором).

certified [sə:tifaɪd] *adj.* сертифицированный, заверенный достоверный.@ **certified cryptosystem** сертифицированная криптосистема.@ **certified key** заверенный ключ.@ **certified prime** достоверно простое число.@ **certified public directory** заверенный открытый справочник (ключей или криптоалгоритмов).

certify [sə:tifaɪ] *v.* сертифицировать, заверять, удостоверять.

chain *n.* = **chaining**

chained [tʃeɪnd] *adj.* сцеплённый.@ **chained key** сцеплённый ключ.@ **chained list** список с использованием указателей.

chained file [tʃeɪnd faɪl] цепочный файл.@ Способ организации файла, при котором каждый его элемент (запись или блок) содержит адрес следующего элемента.

chaining ['tʃeɪnɪŋ] *n.* сцепление.@ **chaining cipher** шифр со сцеплением блоков.

chaining search ['tʃeɪnɪŋ sə:tʃ] цепной поиск.@ Поиск, при котором каждый элемент имеет указатель на следующий элемент.

chance [tʃa:ns] *n.* 1. случай; случайность; 2. возможность; вероятность; шанс; *adj.* случайный; *v.* случаться, случайно оказаться.# **by chance** случайно.# **to miss a chance** упустить возможность.# **to take a chance** воспользоваться случаем.

change [tʃeɪnʃ] *n.* смена, замена; *v.* 1. изменять(ся); 2. превращать(ся); 3. переходить (*over*).@ **change a code (key)** заменять (сменять) код (ключ).@ **change of keys** смена ключей.@ **change record** запись файла изменений.

change bit [tʃeɪndʒ bɪt] разряд изменений, бит изменений.@ В системах с виртуальной памятью – разряд дескриптора сегмента памяти, указывающий на наличие изменений его ячеек.

change dump [tʃeɪndʒ dʌmp] дампы изменений.@ Распечатка измененных ячеек памяти.

change file [tʃeɪndʒ faɪl] файл изменений.@ При ведении файла – файл, описывающий изменения, вносимые в основной файл.

changeover [tʃeɪndʒ'vəʊ] *n.* переход.@ **changeover to a spare key** переход на запасной ключ.

channel ['tʃænl] *n.* 1. канал ввода-вывода; 2. (односторонний) канал связи; 3. дорожка (*перфоленты или магнитной ленты*).@ **channel coding theorem** теорема о канальном кодировании (теорема Шеннона).@ **channel selector** селектор (коммутатор) каналов.@ **channel status byte** байт состояния канала.@ **channel status word** слово состояния канала.@ **channel switching** коммутация каналов.@ **channel-to-channel adapter** адаптер «канал-канал».

channel capacity ['tʃænl kə'pæsəti] 1. пропускная способность (емкость) канала связи.@ Максимальная скорость передачи информации по каналу, при которой еще возможна передача без потери информации, т. е. при сколь угодно малой вероятности ошибок. 2. ширина канала.

channel coding ['tʃænl 'kəʊdɪŋ] канальное кодирование.@ Использование кодов с обнаружением или (и) с исправлением ошибок для обеспечения надежной передачи по каналу связи. При канальном кодировании тот или иной код выбирается в соответствии с шумовыми характеристиками канала, а не с источником информации.

channel controller ['tʃænl kən'trəʊlə] контроллер канала.@ Устройство управления каналом ввода-вывода.

channel director ['tʃænl di'rektə] процессор управления каналами.@ В больших вычислительных системах – специализированный процессор, обеспечивающий взаимодействие с каналами ввода-вывода.

channel program ['tʃænl 'prəʊ-græm] канальная программа.@ Программа канала ввода-вывода, которая размещается в памяти ЭВМ и адрес которой передается каналу для выполнения операции обмена.

character (char) ['kærɪktə] *n.* 1. символ, знак; символ, литера, буква; 2. признак, отличительная черта; 3. характер; 4. свойство; признак; 5. фигура, личность; деятель; 6. герой, действующее лицо.@ **character set** набор символов.@ **character (by-character) transfer** ознакомительная передача, передача по знакам, передача знаков.@ **character assembly** сборка символа.@ **character check** проверка по знакам.@ **character density** плотность расположения знаков.@ **character dependency** (взаимо)зависимость символов (текста).@ **character encoding** кодирование символов.@ **character field** символьное поле, текстовое поле.@ **character frequency** частота встречаемости (появления) букв (в тексте).@ **character frequency count** подсчет частоты встречаемости букв (в тексте).@ **character function** характеристическая функция.@ **character image**

изображение знака. @ **character machine** машина с символьной организацией. @ **character parity check** контроль знаков по четности. @ **character position** расположение знака. @ **character printer** посимвольное печатающее устройство. @ **character reading system** устройство считывания знаков. @ **character spacing** интервал между символами. @ **character string** строка (символов). @ **character terminal** текстовый терминал. @ **character-interleaved** байт-мультиплексный. @ **character-oriented communication** посимвольная передача данных. @ **character-to-number replacement** замена знаков числами (подстановка чисел вместо знаков).

character attribute ['kærɪktə 'ætrɪbjʊ:t] атрибут символа, атрибут литеры. @ В машинной графике – цвет, шрифт, ориентация и размер литеры.

character disassembly ['kærɪktə ,dis'æsemblaɪ] разложение символа. @ Разложение символа на двоичные разряды при передаче по битмультиплексному каналу; при приеме выполняется сборка символа.

character fill ['kærɪktə fɪl] 1. заполнение памяти, роспись памяти. @ Заполнение участка памяти, указанным символом; 2. заполнять память, расписывать память.

character generator ['kærɪktə 'dʒenəreɪtə] генератор символов, знакогенератор. @ Функциональное устройство для преобразования кода символа в его графическое изображение на экране дисплея.

character graphics ['kærɪktə ɡ'ræfɪks] символьная графика, псевдографика. @ Построение графических изображений на экране дисплея или бумаге из текстовых литер или литер «графического набора».

character literal ['kærɪktə 'lɪtərəl] текстовая константа, символьная константа. @ Константа, значением которой является символ (литера).

character mode ['kærɪktə mɔd] текстовый режим, символьный режим. @ Режим работы видеотерминала, при котором на него выводятся только текстовые изображения.

character recognition ['kærɪktə rɪ'kɒɡnɪʃən] распознавание символов. @ Процесс восприятия и декодирования машиной печатных знаков, понятных и для человека.

character representation ['kærɪktə ,reprɪzen'teɪʃən] представление символов. @ Отображение знаков в виде битовых цепочек, определяемое выбранным методом кодирования.

character set ['kærɪktə set] набор символов; алфавит. @ 1. Множество символов (литер), которые способны обрабатывать и отображать печатающее устройство или видеотерминал. 2. Множество символов, используемых в языках программирования.

characteristic [kærɪktə'rɪstɪk] *n.* 1. характеристика, смещенный порядок. 2. характерная черта, особенность. @ 1. характеристика (различие между двумя открытыми текстами, которое с большой вероятностью приводит к появлению определенного различия в соответствующих им шифрованных текстах); 2. характеристика (поля); 3. (рабочая) характеристика (параметр, характеризующий

объем работ, который требуется выполнить для достижения требуемого результата); **4.** отличительный признак. *adj.* характерный; типичный. @ **characteristic frequency (CHF)** характеристическая частота. @ **characteristic function** характеристическая функция. @ **characteristic vector** 1. характеристический вектор; 2. собственный вектор. # **of characteristic** характерный для.

characteristical [kærɪktə'ristɪkəl] *adj.* характеристический. @ **characteristical polynomial** характеристический многочлен.

charge [tʃɑːdʒə] *n.* 1. заряд; 2. нагрузка; 3. ответственность; 4. цена; 5. *pl.* расходы, издержки; *v.* 1. нагружать; 2. заряжать. # **free of charge** бесплатный; бесплатно. # **to be in charge of** быть ответственным, возглавлять. # **to take charge of** возглавлять.

cheater [tʃi:tə] *n.* нарушитель, обманщик.

cheating [tʃi:tɪŋ] *n.* нарушение, обман.

check [tʃek] *n.* 1. контроль, проверка; 2. ошибка (*обнаруженная автоматической проверкой*); *adj.* контрольный, проверочный; *v.* 1. контролировать, проверять; 2. сверять (**up**); 3. задерживать; 4. соответствовать, совпадать (**with**). @ **check character** контрольный знак. @ **check decryption** контрольное (проверочное) расшифрование. @ **check digit** контрольный разряд. @ **check list** 1. контрольная таблица; 2. схема контрольных испытаний. @ **check position** 1. контрольный разряд; 2. контрольная позиция. @ **check problem** проблема (задача) контроля правильности работы вычислительного комплекса (вычислительной машины). @ **check register** контрольный регистр. @ **check sum error-detecting system** система обнаружения ошибок по контрольной сумме. @ **check sum failure** сбой по контрольной сумме. @ **check summing** вычисление контрольной суммы. @ **check symbol** контрольный знак (символ). @ **check total** контрольная сумма. @ **check word** проверочное слово (шифртекст, генерируемый шифровальным оборудованием в целях обнаружения и исправления погрешностей в процессе шифрования). # **to hold (keep) in check** сдерживать; контролировать.

check bits [tʃek bɪts] контрольные разряды. @ Разряды слова или сообщения, являющиеся функцией от информационных разрядов и используемых для обнаружения при передаче или хранении данных.

check read [tʃek riːd] контрольное считывание. @ Считывание, выполняемое непосредственно после записи для проверки.

checking ['tʃekɪŋ] *n.* проверка, профилактический контроль. @ **check(ing) circuit** контролирующая схема, контролирующая цепь. @ **check(ing) program (routine)** программа контроля. @ **check(ing) subroutine** подпрограмма контроля. @ **checking calculation** проверочный расчет, контрольное вычисление. @ **checking information** контрольная информация. @ **checking table** 1. проверочная таблица; 2. проверочный стенд.

checkout ['tʃekaut] 1. отладка; 2. проверка.

checkpoint ['tʃekpɔɪnt] *n.* 1. контрольная точка. @ Точка выполнения процесса, в которой сохраняется информация, необходимая для его повторного

запуска с этой точки. 2. выгружать, откачивать.@ Сохранять состояние процесса во внешней памяти.

checkpoint data set [ˈtʃekpɔɪnt ˈdeɪtə set] набор данных контрольной точки.@ Набор данных (файл), содержащий состояние системы или задачи, сохраненное в контрольной точке.

checkpoint restart [ˈtʃekpɔɪnt ˈriːstaɪt] перезапуск с контрольной точки, рестарт с контрольной точки.@ Возобновления выполнения сохраненного процесса или задачи после сбоя.

checkpoint space [ˈtʃekpɔɪnt speɪs] область сохранения.@ Область диска для сохранения состояния выгруженных задач.

checkpointable task [ˈtʃekˈpɔɪntˈteɪbl taːsk] выгружаемая задача.

checkpointing [ˈtʃekpɔɪntɪŋ] *n.* 1. сохранение состояние процесса в контрольной точке (для возобновления в случае сбоя); 2. подкачка.@ В мультипрограммных системах – сохранение состояния менее приоритетной или ждущей задачи для освобождения места для более приоритетной задачи.

checksum [ˈtʃeksʌm] *n.* контрольная сумма.@ Сумма всех слов или байтов порции данных (файла, блока, записи).@ **checksum generator** генератор контрольной суммы.

checkvalue [ˈtʃekˈvæljuː] контрольная величина, контрольное значение (напр, контрольная сумма)

chief [tʃiːf] *adj.* главный.@ **chief programmer team** бригада главного программиста.@ **chief cryptanalyst** главный криптоаналитик (название одной из руководящих должностей в военном министерстве USA во время второй мировой войны).

chief programmer [tʃiːf ˈprɒɡræmə] главный программист.@ Руководитель работ при разработке программ методом «бригады главного программиста».

chiefly [tʃiːfli] *adv.* главным образом.

children [ˈtʃɪldrən] *n. pl* потомки.@ **children key** производный (вторичный) ключ.

chip [tʃɪp] *n.* микросхема; интегральная схема, ИС.@ Пластмассовая карточка типа кредитной, но имеющая встроенные ЗУ и микропроцессор или логическую схему.

chosen- [ˈtʃuːzən] в сложных и сложносоставных словах имеет значение на основе выбранного.

chosen-ciphertext [ˈtʃuːzənˈsaɪfəˈtekst] *adj.* на основе выбранного шифртекста.@ **chosen-ciphertext attack** атака на основе выбранного шифртекста.@ **chosen-ciphertext attack secure** защищённый от атаки на основе выбранного шифртекста.

chosen-content [ˈtʃuːzənˈkɒntent] *adj.* на основе выбранного содержимого.@ **chosen-content attack** атака на основе выбранного содержимого (противник составляет ложную криптограмму, определяя ее содержание по своему усмотрению).

рению).@ **chosen-content attack secure** защищенный от атаки на основе выбранного содержимого.

chosen-cryptogram *adj.* = **chosen-ciphertext**

chosen-key ['tʃu:zən'ki:] *adj.* на основе выбранного ключа.@ **chosen-key attack** атака на основе выбранного ключа.@ **chosen-key attack secure** защищенный от атаки на основе выбранного ключа.

chosen-plaintext ['tʃu:zən'plain'tekst] *adj.* на основе выбранного открытого текста.@ **chosen-plaintext attack** атака на основе выбранного открытого текста.@ **chosen-plaintext attack secure** защищенный от атаки на основе выбранного открытого текста.

chosen-signature ['tʃu:zən'signətʃə] *adj.* на основе выбранных подписей.@ **chosen-signature attack** атака на основе выбранных подписей.@ **chosen-signature attack secure** защищенный от атаки на основе выбранных подписей

chosen-text ['tʃu:zən'tekst] *adj.* на основе выбранного (открытого и шифрованного) текста.@ **chosen-text attack** атака на основе выбранного текста.@ **chosen-text attack secure** защищённый от атаки на основе выбранного (открытого и шифрованного) текста.

cipher ['saɪfə] *n.* шифр.@ Преобразование текста для сокрытия его семантического содержания. Шифром называется семейство E криптографических отображений информации, где с каждым отображением шифра связано значение k некоторого параметра, называемого ключом. *v.* шифровать, зашифровывать.@ **cipher analysis (cryptanalysis)** криптоанализ – наука о методах анализа криптографических отображений информации с целью раскрытия защищаемой информации.@ **cipher alphabet** шифралфавит.@ **cipher attachment** приставка-шифратор.@ **cipher block chaining (CBC)** сцепление блоков шифра (один из режимов использования DES-алгоритма).@ **cipher block** блок шифра (шифрблок).@ **cipher busting machine** машина для вскрытия шифра.@ **cipher center** шифровальный центр.@ **cipher clerk** шифровальщик.@ **cipher clock** шифровальный циферблат (графическое представление шифра простой замены с помощью окружности, внутренней стороны которой выписываются буквы алфавита открытого текста, а с внешней — шифрованного).@ **cipher code** шифровальный код.@ **cipher construction** конструирование шифров.@ **cipher control byte** байт контроля шифра.@ **cipher designer** разработчик шифров.@ **cipher device** шифровальная машина.@ **cipher feedback** обратная связь по шифртексту (один из режимов использования DES-алгоритма).@ **cipher feedback mode (CFM)** режим шифрования с обратной связью по шифртексту.@ **cipher function** шифрфункция.@ **cipher group** шифргруппа (шифруемая группа знаков).@ **cipher key** ключ к шифру (ключ шифрования).@ **cipher machine** шифровальная машина.@ **cipher material** шифрматериал.@ **cipher message** шифрованное сообщение, шифровка.@ **cipher punk** шифрпанк (человек, который придерживается мнения о том, что любая информация частного характера неприкосновенна и должна быть надежно защищена с помощью стойких криптографических алгоритмов).@ **cipher security** меры безопасности при работе с шифрами.@ **cipher speak** шифртерминология, шифржаргон.@ **cipher suit**

шифрованный комплект (набор алгоритмов шифрования, реализованных в данной системе передачи сообщений).@ **cipher system identification** определение шифрсистемы.@ **cipher system** шифрсистема.@ **cipher taxonomy** таксономия шифром.@ **cipher-breaking device** устройство для вскрытия (взлома) шифров.@ **cipherfunction** шифрфункция.@ **cipher's performance** скорость шифрования.

cipher adventure = **cryptothriller**

cipher algorithm = **ciphering algorithm**

cipher officer = **cipher clerk**

cipher-analyst = **cryptanalyst**

ciphered code = **cipher code**

ciphered ['saɪfəd] *adj.* шифрованный, зашифрованный.@ **ciphered facsimile communication (cifax)** 1. криптографическая защита факсимильной связи; 2. шифрованное факсимильное сообщение.

cipherer ['saɪfər] *n.* 1. кодирующее устройство, шифратор; 2. шифровальщик

ciphering ['saɪfərɪŋ] *n.* шифрование.@ **ciphering algorithm** алгоритм шифрования.@ **ciphering generator** генератор шифрующих (ключевых) последовательностей.@ **ciphering method** метод шифрования.@ **ciphering mode** режим шифрования.

ciphertext ['saɪfə'tekst] *n.* шифртекст (полученный в результате шифрования текста).@ **ciphertext asso-ciated with a given key** шифртекст, полученный на данном ключе.@ **ciphertext associated with a given key** шифртекст, полученный на данном ключе.@ **ciphertext autokey cipher** шифр с автоключом, зависящим от шифртекста.@ **ciphertext autokey (СТАК)** автоключ, зависящий от шифртекста.@ **ciphertext character** знак шифртекста.@ **ciphertext expansion** экспансия шифртекста (полученный в результате шифрования текст имеет большую длину по сравнению с исходным открытым текстом).@ **ciphertext file** файл с шифртекстом.@ **ciphertext generator** генератор шифртекста.@ **ciphertext letter** буква (буквенный знак) шифртекста.@ **ciphertext message** шифрованное сообщение (шифрованный текст сообщения).@ **ciphertext-only attack secure** защищённый от атаки на основе знания одного только шифртекста.@ **ciphertext-only attack** атака на основе знания одного только шифртекста.

ciphertext feedback = **cipher feedback (CFB)**

ciphony ['saɪfounɪ] *n.* 1. криптографическая защита телефонной связи; 2. шифрованное речевое сообщение

circuit ['sə:kɪt] *n.* 1. линия связи; 2. (двухсторонний) канал связи. *Ср. channel*; 3.(электронная) схема; 4. контур; 5. простой цикл; 6. контур (в графе); 2. длина окружности.# **circuit of action** район действия; сфера действия.# **to clear the circuit** выключить линию.

circuit switching ['sə:kɪt 'swɪtʃɪŋ] коммутация каналов.@ Коммутация в сети передачи данных, при которой для связи абонентов устанавливается физическое соединение на все время сеанса связи.

circuit technique ['sə:kɪt tek'ni:k] схемотехника.

circuitry ['sə:kɪtrɪ] *n.* схемы.

circular ['sə:kjulə] *adj.* 1. круглый; 2. круговой; 3. дуговой; 4. циркулярный. @ **circular reference** циклическая зависимость.

circular buffer ['sə:kjulə 'bʌfə] циклический буфер. @ Организация буфера в виде массива с указателями начала и конца свободного пространства, перемещаемыми, соответственно, при записи и считывании; при достижении конца массива указатель перескакивает на начало.

circular list ['sə:kjulə list] кольцевой список. @ Связанный список, в котором последний элемент содержит ссылку на первый.

circular shift ['sə:kjulə ʃɪft] циклический сдвиг. @ Операция сдвига, при которой разряды, выдвигаемые из одного конца регистра, поступают в другой.

circulate ['sə:kju:leɪt] *v.* 1. циркулировать; 2. распространять(ся).

circulating [ˌsə:kju:'leɪtɪŋ] *adj.* циркулирующий. @ **circulating code register** 1. динамический регистр; 2. регистр с циркуляцией кода. @ **circulating memory** динамическая память, запоминающее устройство динамического типа. @ **circulating register** сдвиговый регистр. @ **circulating storage** динамическая память, запоминающее устройство динамического типа.

circulation [ˌsə:kju:'leɪʃən] *n.* циркуляция.

circulator [ˌsə:kju:'leɪtə] *n.* циркулятор.

circumstance ['sə:kəmstəns] *n.* 1. обстоятельство, случай; 2. *pl.* обстоятельства, условия. # **under the circumstance** при данных обстоятельствах.

civil *adj.* = **civilian**

civilian [sɪ'vɪljən] *adj.* гражданский. @ **civilian (class)** **P** класс **P** (класс математических задач, которые могут быть решены за полиномиальное время). @ **civilian (class)** **NP** класс **NP** (класс математических задач, которые могут быть решены за полиномиальное время на недетерминированной машине Тьюринга). @ **civilian cryptography** криптография для гражданских нужд (в отличие от криптографии для военных и дипломатов).

civision [sɪ'vɪʃən] *n.* 1. криптографическая защита телевизионных передач; 2. шифрованная телевизионная передача

class [kla:s] *n.* класс; *v.* 1. классифицировать, оценивать; 2. ставить наряду, относить к (**with**)

classic ['kla:sɪk] *adj.* классический, образцовый

classical ['kla:sɪkəl] *adj.* классический. @ **classical cipher** классический шифр (использующий перестановку и замену букв алфавита естественного языка). @ **classical cryptography** классическая (одноключевая) криптография.

classification [ˌklæsɪfɪ'keɪʃən] *n.* классификация. @ 1. Операция отнесения заданного объекта к одному из классов, внутри которых объекты считаются неразличимыми; результат этой операции. 2. Простейший вид моделирования; в частности, самый слабый вид измерения

classificatory model [klæsɪfi-'keɪtəri 'mɒdl] модель классификационная.@ Простейший вид модели, в которой фиксируются только отношения тождественности или различия.

classified ['klæsɪfaɪd] *adj.* 1. классифицированный; 2. секретный; засекреченный.@ **classified cryptoalgorithm** секретный криптоалгоритм.@ **classified key** секретный ключ.@ **classified message** секретное сообщение.@ **classified network** сеть засекреченной связи.@ **classified work in cryptography** закрытые работы по криптографии.

classify ['klæsɪfaɪ] *v.* классифицировать; подразделять на (**into**).

clear (CLR) [kliə] *v.* заносить нуль, очищать (*регистр, ячейку памяти*); сбрасывать (*счетчик*); *adj.* 1. ясный, светлый; прозрачный; 2. чистый; 3. понятный; открытый, незашифрованный; открытый текст.@ **clear character** знак открытого текста.@ **clear communication** открытая связь.@ **clear message** открытое (незашифрованное) сообщение.@ **clear mode** режим открытой связи.@ **clear operation** работа (шифратора) в режиме приёма-передачи открытого текста (работа в открытом режиме).@ **clear override** переключение (шифратора) с открытой на шифрованную связь (при поступлении на его вход шифртекста).@ **clear to send** разрешённый к передаче.@ **clear key** незашифрованный ключ.@ **clear crypto mode** режим работы (шифратора) с переходом с открытой на шифрованную связь и обратно.@ **clear and add instruction** команда очистки и сложения.

clearance ['kliərəns] *n.* допуск, право доступа.

clear-cut ['kliə'kʌt] *adj.* четко выраженный, четкий.

cleartext ['kliə'tekst] *n.* открытый (исходный) текст (данные с доступным семантическим содержанием, передаваемые с использованием криптографии).@ **cleartext-chiphertext expansion** расширение шифртекста относительно открытого (исходного) текста.

cleartext message = **clear message**

cleartext operation = **clear operation**

cloak [klaʊk] *n.* 1. тактирование; синхронизация; 2. генератор "белого шума" (прибор для шумовой маскировки).@ **clock-controlled shift register** регистр сдвига с тактированием.

close [klaʊz] *n.* 1. конец, окончание; 2. закрытие; *v.* 1. закрывать(ся); 2. заканчивать(ся); 3. замкнуть; замыкать.# **at the close** в конце.

close [klaʊs] *adj.* 1. близкий; 2. тщательный, подробный; 3. закрытый; скрытый; 4. точный; *adv.* близко (**to**)

close a file [klaʊz ə faɪl] закрывать файл.@ Операция завершения работы программы с файлом. При ее выполнении все связанные с файлом буфера сбрасываются, и информация о произведенных изменениях заносится на диск.

closed [klaʊzd] *adj.* 1. замкнутый; 2. замкнутое (множество).@ **closed cycle** замкнутый цикл.@ **closed cycle control** управление по замкнутому циклу.@ **closed function** функция, вычисляемая по закрытой (замкнутой) подпрограмме.@ **closed loop** замкнутая петля, замкнутый контур, замкнутый цикл.@

closed loop control управление по замкнутому циклу. @ **closed routine** (замкнутая) подпрограмма. @ **closed semiring** замкнутое полукольцо. @ **closed subroutine** (замкнутая) подпрограмма.

closed shop [klouzd ʃɒp] вычислительный центр без доступа пользователей. @ Организация работы вычислительного центра, при которой программы разрабатываются штатными программистами, а не заказчиками. ЭВМ обслуживается операторами и пользователи не имеют доступа к ней.

closed system [klouzd 'sistim] замкнутая система. @ Система, не допускающая расширений.

closed user group [klouzd 'ju:zə gru:p] замкнутая группа пользователей. @ Группа пользователей сети передачи данных, которые не могут быть вызваны извне этой группы.

close(-)down [klous 'daun] завершение работы (*вычислительной системы*).

close(-)loop gain [klouz 'lu:p geɪn] коэффициент усиления замкнутой цепи регулирования.

closely ['kləʊslɪ] *adv.* 1. близко; плотно; 2. поблизости; 3. внимательно; тщательно; подробно.

closely(-)coupled interface ['kləʊslɪ 'kʌpld ɪntə'feɪs] сильная связь. @ Способ связи между компонентами системы, при котором изменения в устройстве и функционировании одного компонента влекут соответствующее изменения в другом.

clustering ['klʌstərɪŋ] *n.* кластеризация, группировка. @ Размещение записей с близкими значениями ключа в смежных блоках внешнего запоминающего устройства.

clusterization ['klʌstəraɪzɪʃən] *n.* кластеризация. @ Выделение групп объектов с общими признаками.

clusters topology ['klʌstəs tə'pɒlədʒɪ] иерархическая топология (кластерная топология). @ Архитектура ЭВМ, при которой узлы объединяются в группы (кластеры), причем правила взаимодействия между узлами внутри одного кластера и между узлами разных кластеров различны.

code [kəʊd] *n.* 1. код, система кодирования. @ Способ преобразования информации, записанной в некотором алфавите (например, русском алфавите), в другой (например, двоичный). 2. код, кодировка. @ Набор символов, используемый для кодирования. 3. программа, текст программы, код; 4. код. @ Число, которому переписан некоторый смысл. 5. код, шифр. @ **code alphabet** алфавит кода. @ **code audit** ревизия программы, проверка соответствия программы спецификациям. @ **code book** книга шифров, кодовая книга. @ **code breaker** криптоаналитик, дешифровальщик, взломщик кодов — человек, создающий и применяющий методы криптоанализа. @ **code breaking algorithm** алгоритм вскрытия кода. @ **code breaking exploits** криптоаналитические подвиги. @ **code breaking organization** криптоаналитическая организация. @ **code builder** разработчик кодов. @ **code capacity** пропускная способность (*канала связи*). @ **code change** смена кода. @ **code character** символ кода. @ **code check** контроль

кода. **@ code converter** преобразователь кода. **@ code element** элемент кода. **@ code generation** генерация команд, генерация объектного кода. **@ code generator** генератор кода. **@ code group** кодовая группа. **@ code length** длина (разрядность) блока. **@ code letter** буква (буквенный знак) кода. **@ code like** кодоподобный. **@ code line** строка (текста) программы. **@ code inspection** коллективный формальный анализ программы без участия автора (*прием технологии разработки программного обеспечения*). **@ code machine** кодирующая машина. **@ code maker** составитель (разработчик) кодов. **@ code making** составление (разработка) кодов. **@ code material** закодированный материал. **@ code name of an intercept station** кодовое имя станции перехвата. **@ code number** кодовое число. **@ code operated switch (COS)** переключатель с кодовым управлением. **@ code phrase** кодовая фраза. **@ code position** кодовая позиция. **@ code recovery** восстановление кода. **@ code register** кодовый регистр. **@ code row** правило кодирования. **@ code sing** кодовый знак. **@ code storage circuit** схема хранения кода. **@ code system** система кодирования; кодовая система. **@ code text** закодированный текст. **@ code translation** перекодирование (повторное кодирование в другом коде). **@ code vocabulary** кодовый словарь (слова и фразы открытого текста, для которых в данном коде имеются соответствующие кодовые обозначения). **@ code word** кодовая группа. *v.* кодировать, программировать, составлять программы. **@ codename** давать кодовое имя.

code extension character [koud ɪks'tenʃən 'kærɪktə] символ расширения кода. **@** Управляющий символ, указывающий переход к другой схеме кодирования, например, к другому алфавиту.

code generator [koud 'dʒenəreɪtə] генерация команд, генерация объектного кода. **@** Часть транслятора, порождающая последовательность машинных команд, соответствующих транслируемой программе.

code image [koud 'ɪmɪdʒ] закодированное изображение. **@** Представление изображения в форме, удобной для хранения и обработки.

code removal [koud rɪ'mu:vəl] удаление кода. **@** При оптимизации программы – удаление фрагментов программы, которые не выполняют никаких действий или не могут получить управление.

code walkthrough [koud 'wɔk'θru:] разбор программы. **@** При коллективной разработке программ – анализ текста программы группой программистов для проверки ее правильности.

code(-)breaking [koud'breɪkɪŋ] вскрытие (взлом) шифра.

codebreaker [koud'breɪkə] криптоаналитик, дешифровальщик, взломщик кодов.

codebreaking algorithm [koud'breɪkɪŋ 'ælɡə,rɪdʒəm] алгоритм вскрытия кода.

codec [koudek] *n.* шифратор-дешифратор, кодер-декодер (кодэк).

codecracker = codebreaker

code-cracking = code-breaking

coded ['koudɪd] *adj.* закодированный. **@ coded area** участок, занятый кодом. **@ coded communication** закодированная связь. **@ coded message** закодирован-

ное (шифрованное) сообщение. @ **coded sequence** закодированная последовательность. @ **coded text** кодированный текст. @ **coded transaction** кодированная транзакция. @ **coded word** кодированное слово.

coded-pattern method ['koudɪd 'pætən 'meθəd] метод поля кодовых комбинаций.

codemaker [koud'meɪkə] криптограф, составитель кода.

coder [koudə] *n.* 1. программист, кодировщик. @ Программист, составляющий программы по детальным готовым спецификациям. 2. шифратор; 3. кодировщик, шифровальщик.

coder-decoder ['koudə'dɪkoudə] кодер-декодер.

coding (code) device ['koudɪŋ ('koud) dɪ'vaɪs] кодирующее устройство.

coding (code) relay ['koudɪŋ ('koud) 'ri:'leɪ] кодирующее реле.

coding ['koudɪŋ] *n.* 1. кодирование. @ Запись информации с использованием некоторого кода. 2. программирование, составление программ, кодирование. @ Запись (ранее спроектированной) программы на языке программирования. @ **coding algorithm** кодирующий алгоритм. @ **coding check** контроль программы. @ **coding scheme** система кодирования, код; схема кодирования. @ **coding sheet** бланк для записи программ. @ **coding standards** стандарты кодирования. @ **coding theorems** теоремы кодирования. @ **coding theory** теория кодирования.

coding bounds ['koudɪŋ baʊnds] границы кодирования. @ Пределы производительности кода, выраженные такими параметрами, как число кодовых слов, минимальное кодовое расстояние, длина кодового слова и эффективность.

coefficient [ˌkɔɪ'fɪʃənt] *n.* коэффициент. @ **coefficient matrix of a system of linear equations** матрица коэффициентов системы линейных уравнений.

coin [kɔɪn] *adj.* монетный. @ **coin sequence** "монетная" последовательность (двоичная последовательность, каждый компонент которой рассматривается как результат статистического испытания с двумя равновероятными исходами).

coincide [ˌkɔɪn'saɪd] *v.* 1. совпадать; 2. соответствовать.

coincidence [kɔɪ'nsɪdəns] *n.* 1. совпадение; 2. случайное стечение обстоятельств. @ **coincidence register** регистр совпадения. @ **coincidence test** тест на совпадения. @ **coincidences between two cryptograms** совпадения между двумя криптограммами.

coincidence-type adder [kɔɪ'nsɪdəns'taɪp 'ædə] сумматор совпадений, комбинационный сумматор

coincident [kɔɪ'nsɪdənt] *adj.* 1. совпадающий; 2. соответствующий

coincident selection system [kɔɪ'nsɪdənt sɪ'leɪʃən 'sɪstɪm] селективная система выборки. @ Система выборки, работающая по принципу совпадения токов

cold [kould] *adj.* холодный. @ **cold start-up** "холодный" запуск (процедура первоначальной загрузки ключей в криптографическое оборудование). @ **cold standby** «холодное» резервирование.

cold backup [kould 'bæk'ʌp] «холодное» резервирование.@ Способ резервирования, при котором резервная система должна быть приведена в готовность и запущена вручную.

cold restart (boot) [kould 'ri:stɑ:t (bu:t)] «холодный» перезапуск.@ 1. Перезапуск системы, требующий перезапуска всех подключенных устройств и выполнения процедур начальной загрузки. 2. Для микроЭВМ – перезапуск системы, при котором отключается (электро)питание и содержимое оперативной памяти теряется.

collaborate [kə'leɪəreɪt] v. сотрудничать, работать совместно.# **in collaboration with** совместно с.

collect [kə'lekt] v. 1. собирать; коллекционировать; 2. комплектовать.@ **collect a large amount of plaintext and ciphertext** получить большое количество шифрованного и открытого текста.@ **collect COMINT from satellite** собирать информацию радиоэлектронной разведки со спутника.

collection [kə'leɪʃən] n. сбор, получение (перехват и накопление сообщений для их дальнейшей обработки с целью получения разведывательной информации).

column (col) ['kɒləm] n. столбец (*матрицы, таблицы, экрана*).

column vector ['kɒləm 'vektə] вектор-столбец.

column-major order ['kɒləm'meɪdʒə ɔ:'də] развертывание по столбцам.@ Один из способов отображения элементов двумерного массива на вектор, например для представления в памяти.

column-ragged ['kɒləm'ræɡɪd] не выровненная по столбцам (*о матрице*).

columnar ['kɒləmnə] adj. колонный.@ **columnar generator** комбинационный генератор (порождает псевдослучайную последовательность путем объединения нескольких выходных последовательностей, полученных с помощью набора регистров сдвига, работающих параллельно).@ **columnar of linear feedback shift registers** комбинация регистров сдвига с линейной обратной связью.@ **columnar transposition** шифр колонной перестановки.

combination [kəm'bɪneɪʃən] n. 1. комбинация.@ Метод параллельного объединения функций. 2. сочетание.@ **combination of linear feedback shift registers** комбинация регистров сдвига с линейной обратной связью.

combinational logic [kəm'bɪneɪʃənəl 'lɒdʒɪk] комбинационная логика. @ Цифровая логика, ограниченная описанием комбинационных схем.

combinational circuit [kəm'bɪneɪʃənəl 'sə:kɪt] комбинационная схема.@ Логическая схема, выходные сигналы которой в каждый момент времени определяются входными сигналами в этот момент времени.

combinational logic element [kəm'bɪneɪʃənəl 'lɒdʒɪk 'elɪmənt] элемент комбинационной логической схемы.

combine [kəm'baɪn] v. 1. объединять(ся); соединять(ся); 2. комбинировать, сочетать(ся).

combined [kəm'baɪnd] *adj.* 1. объединенный; общий; 2. комбинированный; смешанный. @ **combined encryption** комбинированное шифрование (межконцевое и канальное).

combined station [kəm'baɪnd 'steɪʃən] комбинационная станция. @ Узел сети, реализующий сбалансированную процедуру HDLC, т.е. способность принимать и передавать команды и ответы.

combiner [kəm'baɪnə] *n.* смеситель (функция или устройство для объединения нескольких числовых последовательностей в одну).

combining function *n.* = **combiner**

come [kʌm] *v.* (**came, come**) 1. приходить, приезжать; 2. случаться, происходить; 3. доходить, достигать; сводиться к (**to**). # **in years to come** в ближайшие годы, в будущем. # **to come** + *inf.* стать + *инф.*; начинать + *инф.* # **to come into account** учитываться. # **to come into being** возникать, появляться. # **to come into existence** возникать, появляться. # **to come into service** возникать, появляться. # **to come into effect** вступать в силу. # **to come into force** вступать в силу. # **to come into one's own (right)** вступать в свои права. # **to come into play** начинать действовать. # **to come to grips** подходить вплотную. # **to come to hand** появиться. # **to come to know** познакомиться, узнать

commercial [kə'mɜːʃəl] *adj.* 1. торговый, коммерческий; 2. промышленный; выпускаемый промышленностью. @ **commercial channel** коммерческий канал (связи). @ **commercial code** коммерческий код. @ **commercial Communications Security Endorsement program (CCCEP)** Программа аттестации коммерческих средств защиты связи (USA). @ **commercial Computer Security Center (CCSC)** Центр безопасности коммерческих вычислительных систем (Англии). @ **commercial encryption** коммерческие криптосистемы.

common ['kɒmən] *adj.* 1. общий; 2. обычный; 3. свойственный (**to**). @ **common key** общий ключ (одноключевой криптосистемы). @ **common multiple** общий делитель. # **in common** общий; сообща. # **in common with** подобно, так же как и. # **it is common knowledge** это общеизвестно.

common carrier ['kɒmən 'kæriə] 1. общественная (общедоступная) линия связи; 2. коммерческая (частная) сеть связи; 3. зарегистрированная частная кампания-владелец сети связи.

common-key cryptography = **single-key cryptography**

communicant [kə'mjuːnikənt] *n.* абонент (сети связи). @ **communicate privately** обмениваться секретными сообщениями.

communicate [kə'mjuːniket] *v.* 1. сообщать; передавать (**to**); 2. общаться(ся) с (**with**).

communication (com, comm) [kə'mjuːnɪ'keɪʃən] *n.* 1. (обычно *pl*) связь; передача данных; 2. взаимодействие; общение. @ **communication channel** канал связи, информационный канал. @ **communication chart** таблица соединений, схема соединений. @ **communication device** устройство связи. @ **communication engineering** техника связи. @ **communication facility** средства связи. @ **Communication I/O Control System (CIOCP)** система управления каналами

связи.@ **communication light** пультовая индикаторная (сигнальная) лампа.@ **communication network** сеть связи.@ **communication server** коммутационный узел обслуживания.@ **communication theory** теория связи.@ **communication vector table (CVT)**.@ **communication(s) link** канал (линия) связи.@ **communications electronics (CE)**.@ **communication complexity** коммуникационная сложность (алгоритма или математической задачи).@ **communication network** сеть связи.@ **communications cryptograph** криптография для защиты связи.@ **communications intelligence material** материалы радиоэлектронной разведки.@ **communications intercepts** перехваченные сообщения.@ **communication(s) link** канал (линия) связи.@ **communication complexity** коммуникационная сложность (алгоритма или математической задачи).@ **communication network** сеть связи.@ **communications cryptograph** криптография для защиты связи.@ **communications intelligence material** материалы радиоэлектронной разведки.@ **communications intercepts** перехваченные сообщения.

communication port [kə'mju:ni'keɪʃən pɔ:t] коммуникационный порт.@ Порт, к которому подключен адаптер связи.

communication processor [kə'mju:ni'keɪʃən 'prəʊsesə] связной процессор.@ Специализированный процессор ввода-вывода, используемый для управления определенным количеством линий или устройств связи.

communication subnetwork (subnet) [kə'mju:ni'keɪʃən 'sləb'netwɜ:k] коммуникационная подсеть.@ Совокупность выделенных процессоров и магистральных линий, реализующих функции передачи данных в распределенной сети.

communication system [kə'mju:ni'keɪʃən 'sɪstɪm] система связи.@ Система, посредством которой источник информации может достаточно эффективно и надежно передавать эту информацию в пункт назначения.

communications intelligence (COMINT) [kə'mju:ni'keɪʃəns ɪn'telɪdʒəns] радиоэлектронная разведка (радиоэлектронной разведки).@ **COMINT agency** агентство радиоэлектронной разведки.@ **COMINT data** данные радиоэлектронной разведки.@ **COMINT equipment** оборудование радиоэлектронной разведки.@ **COMINT friendly** дружественный для радиоэлектронной разведки (не требует применения нетрадиционных, дорогостоящих или чреватых непредсказуемыми последствиями методов радиоэлектронной разведки).@ **COMINT organization** организация радиоэлектронной разведки.@ **COMINT processing** обработка данных радиоэлектронной разведки.@ **COMINT purposes** цели радиоэлектронной разведки.@ **COMINT reports** сводки радиоэлектронной разведки.@ **COMINT satellite** спутник радиоэлектронной разведки.

communications [kə'mju:ni'keɪʃəns] коммуникации.@ **communications Intelligence Board (CIB)** Совет по радиоэлектронной разведке.@ **communications network** сеть связи.@ **communications satellite (COMSAT)** спутник связи.@ **communications Security (COMSEC)** 1. Безопасность связи (подразделения NSA USA, занимающиеся вопросами обеспечения безопасности связи); 2. обеспечение безопасности связи.@ **communications security device**

(CSD) устройство для обеспечения безопасности связи. @ **communications Security Establishment (CSE)** Служба безопасности связи (канадское правительственное ведомство, занимающееся перехватом и дешифрованием сообщений). @ **communications Security Establishment** Служба безопасности связи; (канадское правительственное ведомство, занимающееся перехватом и дешифрованием сообщений).

communicator *n.* = **communicant**

commutative [ˌkɒmjʊːˈteɪtɪv] *adj.* коммутативный. @ **commutative property of encrypting function** коммутативность шифрующей функции. @ **commutative ring** коммутативное кольцо.

compact [kəmˈpækt] *v.* сжимать; уплотнять; *adj.* компактный. @ **compact knapsack** компактный вектор ранца.

compare [kəmˈpreə] *v.* 1. сравнивать; сличать (**with**); 2. ставить наравне; 3. сравниваться; выдерживать сравнение; 5. уподоблять (**to**). # **to compare favourably with** выгодно отличаться от.

comparison [kəmˈpærɪsn] *n.* сравнение. # **as compared to (with)** по сравнению с. # **in comparison with** по сравнению с. # **beyond comparison** вне сравнения. # **to make comparisons** проводить аналогию.

compass [kəmˈpɑːs] *adj.* компасный. @ **compass cipher** компасный шифр (разновидность шифра простой замены). @ **compass key** ключ к компасному шифру.

compatibility [kəmˈpætəˈbɪlɪti] *n.* совместимость. @ **1.** Совместимость аппаратных средств – способность подсистемы (например, памяти) или внешнего устройства одной модели заменять подсистему или внешнее устройство другой модели. **2.** Совместимость программного обеспечения – способность ЭВМ непосредственно выполнять программу, которая была скомпилирована, скомпонована на машинном языке для другой ЭВМ. **3.** Совместимость новой программы – способность воспроизводить поведение своего предшественника, в частности принимать данные в том же входном формате.

compatibility mode [kəmˈpætəˈbɪlɪti mɔːd] режим эмуляции. @ Режим работы процессора, при котором он выполняет команды другой модели ЭВМ. Архитектура с режимом эмуляции обеспечивает частичную совместимость новой ЭВМ со старыми моделями.

complement [ˈkɒmplɪment] *n.* дополнение; *v.* 1. дополнять; 2. укомплектовывать. @ **complement key** ключ дополнение (получается путём выполнения операции логического отрицания над битами ключа, представленного в двоичном виде).

complement number [ˈkɒmplɪˈment ˈnʌmbə] система дополнений. @ Альтернативный способ представления чисел в системе счисления с фиксированным основанием.

complement number [ˈkɒmplɪˈment ˈnʌmbə] система дополнений. @ Альтернативный способ представления чисел в системе счисления с фиксированным основанием.

complementary ['kɒmplɪ'mentəri] *adj.* дополнительный, дополняющий, комплементарный. @ **complementary key** дополняющий (комплементарный) ключ (открытый или секретный ключ в криптосистеме с открытым ключом).

complete [kəm'pli:t] *adj.* полный; законченный; совершенный; *v.* заканчивать. @ **complete automatic check** полностью автоматический контроль. @ **complete graph** полный граф. @ **complete information** полная информация. @ **complete instruction** полная команда. @ **complete lattice** полная решетка. @ **complete operation** завершенная (*полная*) операция. @ **complete tree** завершенное дерево. @ **complete unit** составной элемент. @ **complete protection against impersonation attack** полная защита от попытки имитации. @ **complete set of residues modulo n** полное множество вычетов по модулю n . @ **complete spread function** полнораспределенная функция (значение функции существенно зависит от каждого её аргумента).

complete carry [kəm'pli:t 'kæri] полный перенос. @ При параллельном сложении – обработка переноса, при которой перенос распространяется в старшие разряды.

completely [kəm'pli:tli] *adv* полностью. @ **completely random source of messages** полностью случайный источник сообщений.

completeness [kəm'pli:tni:s] *n.* полнота, завершенность. @ **completeness property** свойство полноты шифрования (каждый выходной бит шифра является функцией всех входных битов).

complex ['kɒmpleks] *adj.* 1. сложный, комплексный, составной; 2. трудный; *n.* комплекс; совокупность. @ **complex key** сложный (комбинированный) ключ. @ **complex arithmetic** 1. арифметика с комплексными числами, арифметические операции с комплексными числами; 2. арифметическое устройство для работы с комплексными числами. @ **complex field amplitude (CFA)** комплексная амплитуда поля. @ **complex integer** комплексное число. @ **complex operation** 1. сложная операция; 2. действие с комплексными числами. @ **complex plane** комплексная плоскость. @ **complex variable** комплексная переменная.

complex system ['kɒmpleks 'sɪstɪm] сложная система. @ Система, модель которой, используемая для управления системой, неадекватна заданной цели.

complexity ['kɒmpleksɪti] *n.* 1. сложность. @ 1. Свойство некоторого явления (объекта, процесса, системы) выражающееся в неожиданности, непредсказуемости, необъяснимости, случайности, «антиинтуитивности» его поведения. 2. «Трудность» решения вычислительных проблем, измеренная в терминах некоторого ресурса, потребляемого в процессе вычисления. 2. запутанность. @ **complexity factor** коэффициент сложности. @ **complexity function (work function)** функция сложности (работы).

complexity classes ['kɒmpleksɪti kla:sɪs] классы сложности. @ Способ группировки алгоритмов или вычислительных функций в соответствии с их сложностью.

complexity measure ['kɒmpleksɪtɪ 'meɪʒə] критерий сложности.@ Средство измерения объема ресурсов, используемых в процессе вычисления.

component [kəm'pounənt] *n.* 1. компонент, элемент (часть системы, выполняющая определенные функции); 2. деталь, узел, блок, компонента, составляющая; *adj.* составной; сложный; составляющий, входящий в состав.@

component by component addition покомпонентное сложение (попарное сложение соответствующих элементов двух последовательностей).@ **component values** значение параметров, включая допуски элементов схемы.@ **component cipher** составляющий шифр (шифр, входящий в состав суперпозиции шифров).

component-wise addition = component by component addition

composite ['kɒmpəzɪt] *adj.* 1. *adj.* составной (о числе), смешанный, сложный; 2. *n.* составное число.@ **composite function** сложная функция.

composite attribute ['kɒmpəzɪt 'ætrɪbjʊ:t] составной атрибут.@ Атрибут, состоящий из нескольких простых атрибутов.

composition *n.* = **product**

compound (cpd) ['kɒmpaʊnd] *n.* соединение; смесь; состав; *adj.* составной, смешанный, сложный.@ **compound density** плотность размещения компонентов (компьютеров).@ **compound disturbance** сложное возмущение, сложное возбуждение.@ **compound domain** составной домен.

compound statement ['kɒmpaʊnd 'steɪtmənt] составной оператор. @ Оператор, в состав которого входят другие операторы.

compression function = hash function

compression [kəm'preʃən] *n.* сжатие (данных).@ **compression coding** кодирование для сжатия, сжимающее кодирование.

compromise ['kɒmprəmaɪz] 1. *v.* компрометировать; 2. *n.* компрометация.@ **compromise a secret key** компрометировать секретный ключ.@ **compromise of a key** компрометация ключа.

compromised ['kɒmprəmaɪzd] *adj.* скомпрометированный.@ **compromised cryptosystem** скомпрометированная криптосистема (потерявшая секретность в результате того, что её секретные криптопеременные стали известны противнику).@ **compromised key** скомпрометированный (потерявший секретность - вскрытый противником или ставший ему известным в силу каких-либо других обстоятельств) ключ.

computable [kəm'pjʊ:təbl] *adj.* вычислимый.@ **computable function** вычислимая функция.

computational [kəm'pjʊ:'teɪʃənl] *adj.* вычислительный.@ **computational complexity** вычислительная сложность.@ **computational complexity-based cryptography** вычислительная криптография (криптография на основе вычислительной сложности).@ **computational feasible** вычислительно осуществимый.@ **computational hard problem** труднорешаемая задача (задача, решение которой требует больших вычислительных затрат).@ **computational infeasible** вычислительно неосуществимый.@ **computational problem** вычислительная задача (проблема).@ **computational scheme** вычислительная схема, схема вы-

числений. @ **computational secure scheme** вычислительно стойкая схема (схема шифрования или аутентификации является вычислительно стойкой, если её стойкость зависит от вычислительного алгоритма, сложность которого такова, что он не может быть реализован на практике, поскольку требует выполнения слишком большого числа операций).

computational cryptography = computational complexity based cryptography

computational linguistics [kəmpju:'teɪʃənl 'lɪŋgwɪstɪks] вычислительная лингвистика. @ Дисциплина на стыке лингвистики и искусственного интеллекта, занимающаяся изучением формальных свойств естественных языков с помощью ЭВМ и моделированием процессов анализа, синтеза естественных языковых текстов на ЭВМ.

computational psychology [kəmpju:'teɪʃənl saɪ'kɒlədʒɪ] вычислительная психология. @ Дисциплина на стыке искусственного интеллекта и психологии. Занимается построением машинных моделей процессов естественного познания, присущих человеку.

computationally [kəmpju:'teɪʃənlɪ] *adv.* вычислительно

compute [kəm'pjʊ:t] *v.* вычислять, рассчитывать, считать. @ **compute a key** вычислять ключ

computer [kəm'pjʊ:tə] 1. *n.* компьютер; 2. *adj.* компьютерный. @ **computer cryptography** 1. компьютерная криптография; 2. применение криптографии для защиты данных в компьютере и компьютерных сетях. @ **computer eavesdropping** перехват электромагнитного излучения работающих компьютеров. @ **computer key** ключ шифрования-расшифрования для компьютера. @ **computer Security (COMPUSEC)** Компьютерная безопасность (подразделения NSA USA, занимающиеся вопросами обеспечения компьютерной безопасности). @ **computer-based message system (CBMS)** компьютерная система передачи сообщений. @ **computer cryptanalysis** машинный криптоанализ (криптоанализ с использованием компьютера). @ **computer architecture** архитектура вычислительной системы. @ **computer calculation** расчет на вычислительной машине. @ **computer center (centre)** вычислительный центр. @ **computer circuit** схема вычислительной машины. @ **computer conference** телеконференция. @ **computer cycle** машинный цикл. @ **computer dead time** время простоя вычислительной машины. @ **Computer Description Language (CDL)** язык описания архитектуры ЭВМ на уровне межрегистровых пересылок. @ **computer design** конструирование (проектирование) вычислительной машины. @ **computer display** дисплей вычислительной машины. @ **computer efficiency** эффективность использования вычислительной машины. @ **computer facility** вычислительный центр (*внутри организации*). @ **computer function** функция вычислительной машины. @ **computer game** машинная игра, игровая программа. @ **computer generation** поколение ЭВМ. @ **computer graphics** машинная графика. @ **computer hardware** аппаратные средства вычислительной системы. @ **computer instruction** машинная команда. @ **computer intelligence access (CIA)** обращение к машинному интеллекту. @ **computer interface (CI)** интер-

фейс ЭВМ. @ **computer mail** электронная почта. @ **computer manager** администратор вычислительной системы. @ **computer memory** память вычислительной машины. @ **computer operation** 1. машинная операция; 2. работа вычислительной машины. @ **computer operator** оператор ЭВМ, техник-вычислитель. @ **computer program** программа для вычислительной машины. @ **computer programming** программирование для вычислительной машины. @ **computer run** запуск программы на ЭВМ; выполнение программы на ЭВМ; счет, работа ЭВМ. @ **computer services manager** администратор вычислительных услуг. @ **computer storage** запоминающее устройство ЭВМ. @ **computer test circuit** схема контроля вычислительной машины. @ **computer useful time** полезное машинное время. @ **computer user** пользователь вычислительной системы. @ **computer word** машинное слово. @ **computer zero** машинный ноль.

computer-aided cryptanalysis = **computer cryptanalysis**

computer-assisted cryptanalysis = **computer cryptanalysis**

computer-backed cryptanalysis = **computer cryptanalysis**

computer-performing cryptanalysis = **computer cryptanalysis**

computer control system [kəm'pjʊ:tə kən'trəʊl 'sɪstɪm] компьютерная система управления. @ Система управления с ЭВМ.

computer family [kəm'pjʊ:tə 'fæmɪli] семейство ЭВМ. @ Группа типов ЭВМ с одинаковой или близкой архитектурой, но с различным техническим исполнением и различной производительностью.

computer fraud [kəm'pjʊ:tə frɔ:d] злоумышленное использование вычислительной машины. @ Любая деятельность, направленная на манипулирование информацией внутри вычислительной системы с целью личной выгоды.

computer graphics metafile (CGM) [kəm'pjʊ:tə g'ræfɪks ,metə'faɪl] метафайл машинной графики. @ Стандарт на формат хранения и передачи изображений.

computer language [kəm'pjʊ:tə 'læŋgwɪdʒ] машинный язык, язык машины. @ Система команд ЭВМ.

computer literacy [kəm'pjʊ:tə 'lɪtərəsi] компьютерная грамотность, вторая грамотность. @ Комплекс знаний и навыков, необходимый для повседневного применения ЭВМ в профессиональной деятельности.

computer logic [kəm'pjʊ:tə 'lɒdʒɪk] логика вычислительной машины. @ Базовая организация, конструкция и монтаж, используемые для реализации конкретной архитектуры ЭВМ.

computer micrographics [kəm'pjʊ:tə 'maɪkrəʊ,g'ræfɪks] машинная микрографика. @ Совокупность методов и технических приемов для отображения графических данных на микрофильм или микрофиши с помощью ЭВМ.

computer network [kəm'pjʊ:tə 'netwɜ:k] сеть ЭВМ, вычислительная сеть. @ Совокупность связанного и коммутационного оборудования, протоколов и программных средств, объединяющих несколько вычислительных машин в единую вычислительную систему.

computer power [kəm'pjʊ:tə 'paʊə] производительность ЭВМ. @ Параметры оценки производительности ЭВМ включают тактовую частоту процессора,

время выполнения операции типа сложения, время выполнения регистровой операции, время обработки эталонных тестов.

computer science [kəm'pjʊ:tə 'saɪəns] информатика.@ Общее название для группы дисциплин, занимающихся различными аспектами применения и разработки ЭВМ; программирование, прикладная математика, языки программирования и операционные системы, искусственный интеллект, архитектура ЭВМ.

computer system [kəm'pjʊ:tə 'sɪstɪm] вычислительная система, ЭВМ.@ Собственно вычислительная машина с подключенными к ней внешними устройствами и системным программным обеспечением.

computer time [kəm'pjʊ:tə taɪm] машинное время.@ Полезное время работы вычислительной машины.

computer vision [kəm'pjʊ:tə 'vɪʒən] машинное зрение.@ Средства ввода и распознавания изображений.

concatenated [kən,kæti'neɪtɪd] *adj.* 1. составной; 2. = **chained**.@ **concatenated encryption** составное шифрование (последовательно двумя или более различными криптографическими методами).@ **concatenated code** составной код в системах каскадного кодирования.

concatenated coding systems [kən,kæti'neɪtɪd kəʊdɪŋ 'sɪstɪms] системы каскадного кодирования.@ Системы связи, в которых сообщения перед передачей по каналу кодируются посредством внутреннего кода, а затем декодируются в соответствии с ним; вся эта система «кодер – канал – декодер» сама рассматривается как канал (возможно менее зашумленный, чем исходный канал) и поэтому имеет еще один кодер и декодер, расположенные перед и после нее; эти дополнительные устройства реализуют внешний код.

concatenation [kən,kæti'neɪʃən] *n.* сцепление, конкатенация.@ Операция объединения двух последовательностей (строк, файлов) в одну, при которой первая последовательность становится началом результирующей, а вторая – хвостом.@ **concatenation of a message and an appended authenticator** сцепление сообщения и добавляемого (к этому сообщению) аутентификатора.@ **concatenation closure** конкатенационное замыкание.

conceal [kən'si:l] *v.* прятать, скрывать.@ **conceal the contents of a message** прятать содержание сообщения.

concealment [kən'si:lment] *n.* сокрытие, утаивание.@ **concealment message methodology** методология сокрытия сообщения.

concern [kən'sə:n] *v.* 1. касаться, иметь отношение; иметь дело; 2. интересоваться; *n.* 1. дело, отношение; 2. участие, интерес; 3. забота, внимание; 4. значение, важность; 5. цель, задача; 6. концерт.# **as far as ... is concerned** что касается, когда речь идет о.# **(in) so far as ... is concerned** что касается, когда речь идет о.# **(sofar) as concerns** что касается, когда речь идет о.# **of concern** представляющий интерес.# **to concern oneself with** иметь дело с, заниматься чем-л.; быть связанным с чем-л..# **to be concerned with** иметь дело (с), зани-

маться чем-л.; быть связанным с чем-л..# **to have no concern with** не иметь отношения к.

conclusion [kən'klu:ʒn] *n.* 1. заключение; вывод; 2. окончание.# **to bring to a conclusion** завершать, заканчивать.# **to arrive at a conclusion** прийти к заключению.# **to reach a conclusion** прийти к заключению.# **to draw a conclusion** делать вывод, заключение.

condition (COND) [kən'dɪʃən] *n.* 1. условие.@ Логическое выражение, от истинности которого зависит выполнение или невыполнение некоторых действий. 2. состояние, ситуация; положение; 3. режим; 4. *pl.* обстоятельства; *v.* 1. обуславливать; 2. улучшать; кондиционировать.# **in condition** в хорошем состоянии.# **out of condition** в плохом состоянии.# **on (upon) condition** при условии.# **under such conditions** при таких обстоятельствах.

conditional [kən'dɪʃənl] *n.* условное выражение.@ Логическое выражение вида «если А то В». *adj.* условный.@ **conditional branch** условный переход.@ **conditional branch instruction** команда условного перехода (ветвления).@ **conditional breakpoint instruction** команда условного контрольного перехода или останова.@ **conditional convergence** условная сходимость.@ **conditional distribution** условное распределение.@ **conditional implication** условная импликация.@ **conditional inequality** условное неравенство.@ **conditional instruction** условная команда, команда условного перехода.@ **conditional jump instruction** команда условного перехода.@ **conditional maximum likelihood estimate (CMLE)** условная оценка методом максимального правдоподобия.@ **conditional operation** условная операция.@ **conditional probability** условная вероятность.@ **conditional stop instruction** команда условной остановки.@ **conditional transfer (instruction)** 1. передача управления по команде условного перехода; 2. условная передача управления; 3. команда условного перехода; 4. команда условной передачи управления.

conditional compilation [kən'dɪʃənl ˌkɒmpɪˈleɪʃən] условная трансляция.@ Средство языка программирования, позволяющее включать или выключать трансляцию части текста программы в зависимости от значения некоторой константы.

conditional jump [kən'dɪʃənl ɔʒʌmp] условный переход, операция условного перехода.@ Передача управления по указанному адресу в зависимости от результата выполнения предыдущей команды или значений управляющих регистров процессора.

conditional statement [kən'dɪʃənl 'steɪtmənt] условный оператор.@ Управляющая конструкция, описывающая условие и действия, выполняемые от истинности условия.

conference ['kɒnfəʁəns] *n.* конференц-связь.@ **conference cryptosystem** криптосистема для конференц-связи.@ **conference key** конференц-ключ (общий для всех участников конференции).@ **conference key distribution system** система распределения конференц-ключей.

confidence ['kɒnfɪdəns] *n.* 1. доверие, степень доверия; 2. уверенность. @ **confidence estimation** оценка по доверительному интервалу. @ **confidence level** граница достоверности, степень уверенности. @ **confidence limits** доверительные границы.

confidence interval ['kɒnfɪdəns 'ɪntəvəl] доверительный интервал. @ Числовой диапазон, вероятность принадлежности к которому истинного значения переменной величины больше заданной величины.

confident ['kɒnfɪdənt] *adj.* уверенный

confidential (C) ['kɒnfɪdənsjəl] *adj.* конфиденциальный. @ **confidential means of communication** средства конфиденциальной связи. @ **confidential message** конфиденциальное сообщение.

confidentiality ['kɒnfɪdənsəlɪtɪ] *n.* конфиденциальность (защищённость информации от несанкционированного доступа со стороны пользователей, не имеющих соответствующих полномочий). @ **confidentiality provided by encryption** конфиденциальность, обеспечиваемая с помощью средств шифрования.

confusion [kən'fju:ʒn] *n.* 1. смущение; 2. путаница; недоразумение; 3. перемешивание (использование шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов). @ **confusion of goals** смещение целей.

congruence ['kɒŋgruəns] *n.* 1. конгруэнтность (числа a и b связаны отношением конгруэнтности по модулю m , если $a-b$ делится на m); 2. согласованность; 3. соответствие; 4. совпадение. @ **congruence relation** отношение конгруэнтности.

congruent ['kɒŋgruənt] *adj.* конгруэнтный.

congruential ['kɒŋgruənʃəl] *adj.* конгруэнтный @ в криптологии – генератор. @ **congruential generator** конгруэнтный генератор (генератор конгруэнтных чисел).

consecutive [kən'sekjʊtɪv] *adj.* последовательный, идущий подряд. @ **consecutive bits of linear feedback shift register sequence** подряд идущие биты последовательности, полученной с помощью регистра сдвига с линейной обратной связью.

consequence ['kɒnsɪkwəns] *n.* следствие; последствие, результат. # **as a consequence** в результате. # **in consequence of** вследствие; в результате. # **in consequence of which** вследствие чего. # **of consequence** имеющий значение. # **of no consequence to** несущественный, неважный (для).

conservative [kən'sə:vətɪv] *adj.* 1. консервативный; 2. умеренный; осторожный; 3. заниженный; ограниченный. # **as a conservative estimate** по скромному подсчету.

consideration [kən,sɪdə'reɪʃən] *n.* 1. рассмотрение, обсуждение; 2. соображение; размышление; 3. внимание. # **by practical considration** путем эксперимента, опытным путем. # **on (under) no considration** ни под каким видом. # **under considration** рассматриваемый. # **without considration** не учитывая. # **to**

give considration to рассмотреть, обсудить что-л. # **to take into considration** принимать во внимание.

consistent [kən'sistənt] *adj.* 1. непротиворечивый, согласованный; 2. последовательный, логичный; 3. согласующийся, совместимый. # **as consistent with** в соответствии с. # **in a consistent manner** последовательно. # **self consistent** самосогласованный; самосостоятельный. # **to be consistent with** соответствовать чему-л.; согласовываться с чем-л.; быть совместимым с

consonant ['kɒnsənənt] *n.* буква, обозначающая согласный звук. @ **consonant-vowel relationship** взаимосвязь между буквами, обозначающими согласные и гласные звуки.

constant ['kɒnstənt] *n.* константа, постоянная величина, постоянный коэффициент; *adj.* постоянный, независимый. @ **constant angular velocity (CAV)** постоянная скорость вращения диска. @ **constant bias** постоянная (систематическая) ошибка. @ **constant declaration** описание константы. @ **constant factor** постоянный множитель. @ **constant frequency (CF)** неизменная частота. @ **constant list** список констант. @ **constant motion** равномерное прямолинейное движение. @ **constant of integration** постоянная интегрирования. @ **constant of inversion** константа инверсии. @ **constant of proportionality** константа пропорциональности. @ **constant sequence** постоянная последовательность (двоичная последовательность, состоящая из одних нулей или из одних единиц). @ **constant-false-alarm rate (CFAR)** постоянная частота ложных тревог; постоянная вероятность ложных тревог. @ **constant-frequency variable-dot system (CFVD(S))** система передачи полутоновых изображений штриховым способом.

constant area ['kɒnstənt 'ɛəriə] область констант. @ Область памяти, где расположены значения констант программы.

constant expression ['kɒnstənt ɪks'preʃən] константное выражение. @ Выражение, в которое входят только константы.

contemporary [kən'tempərəri] *n.* современник; *adj.* 1. современный; 2. одновременный. @ **contemporary cryptology** современная криптология.

content ['kɒntent] *n.* 1. *pl.* содержание; 2. объем, вместимость; *v.* удовлетворять. # **to content oneself with** удовлетворяться, довольствоваться чем-л. # **table of contents** оглавление.

contents ['kɒntents] *n. pl.* содержание, содержимое. @ **contents of a cryptogram** содержание криптограммы.

contingency [kən'tɪndʒənsi] *n.* непредвиденное обстоятельство, случай. @ **contingency key** ключ для непредвиденных обстоятельств (специальный ключ, предназначенный для использования при возникновении непредвиденных обстоятельств).

contingency table [kən'tɪndʒənsi 'teɪbl] таблица сопряженности признаков. @ В статическом анализе распределение частот выборок, классифицируемое по двум или более признакам, каждый из которых принадлежит двум или более классам.

continous [kən'tɪnjuəs] *adj.* непрерывный.@ **continous encryption** непрерывное шифрование.

continued [kəntɪ'njuːɪd] *adj.* 1. продолжительный; продолжающийся; дальнейший; 2. непрерывный.# **to be continued** продолжение следует.

contrary ['kɒntrəri] *adj.* противоположный.# **contrary to** в противоположность.# **on the contrary** наоборот

contrast ['kɒntræst] *n.* 1. противоположность; 2. контрастность, контраст; *v.* контрастировать.# **as contrasted with** в противоположность чему-л.; по сравнению с чем-л.# **by contrast to (with)** в противоположность чему-л.; по сравнению с чем-л.# **in contrast with** в противоположность чему-л.; по сравнению с чем-л.

control (CTRL) «спец».@ Регистровая клавиша, используемая для ввода управляющих кодов.

control [kən'trɒl] *n.* 1. управление.@ Целевое воздействие на системы (т.е. воздействие, приближающее к целевому состоянию). 2. регулирование, регулировка; 3. устройство (орган) управления. *v.* 1. управлять, регулировать; 2. контролировать, проверять.@ **control action** управляющее (регулирующее) воздействие.@ **control and switching equipment (CSE)** аппаратура управления и коммутации.@ **control bit** управляющий разряд; служебный разряд.@ **control chart** контрольная карта.@ **control circuit** схема управления, цепь управления, цепь регулирования, контрольная цепь.@ **control code** управляющий код.@ **control command** команда управления.@ **control component** элемент системы управления.@ **control computer (CC)** управляющая вычислительная машина.@ **control computer module (CCM)** модуль управляющей ЭВМ.@ **control computer** управляющая ЭВМ.@ **control design** расчет (синтез) системы управления.@ **control desk** пульт (щит) управления.@ **control device** 1. устройство управления; 2. устройство контроля.@ **control flow chart** структурная схема управления.@ **control function** функция управления.@ **control hierarchy** иерархия управления (контроля).@ **control index** контрольный индекс.@ **control input** управляющий вход.@ **control instruction** команда управления, управляющая команда.@ **control list** управляющая таблица.@ **control logic** 1. логика управления; 2. логическая схема устройства управления.@ **control mark** служебная метка, служебный маркер.@ **control of electromagnetic radiation (CONELRAD)** контроль за электромагнитным излучением.@ **control of electromagnetic radiation (conelrad)** контроль электромагнитного излучения.@ **control operation** операция управления (регулирования).@ **control panel** панель управления.@ **control pen** световое перо.@ **control register** 1. регистр управления; 2. регистр команд; 3. счетчик команд.@ **control response** управляющее воздействие.@ **control sequence** управляющая последовательность, нисходящая последовательность.@ **control statement** оператор управления, управляющий оператор.@ **control storage load (CSL)** загрузка управляющего ЗУ.@ **control system** 1. система управления (регулирования); 2. система контроля.@ **control terminal** операторский терминал.@ **control total** кон-

трольная сумма. @ **control transfer instruction** команда передачи управления. @ **control transfer** передача управления, переход. @ **control unit** 1. устройство управления; 2. центральный процессор. @ **control value** контрольное значение. @ **control word** управляющее слово.

control block [kən'troul blɒk] управляющий блок. @ Структура данных, содержащая параметры некоторого устройства или объекта.

control bus [kən'troul blʌs] шина управления. @ Часть шины, по которой передаются управляющие сигналы.

control character [kən'troul 'kæɪɪktə] управляющий символ (знак), знак управления. @ Знак, который при вводе с клавиатуры или передаче перефигурному устройству вызывает выполнение определенной функции.

control flow [kən'troul fləʊ] поток управления. @ Последовательность выполняемых команд.

control heading [kən'troul 'hedɪŋ] служебная (управляющая) программа. @ Программа, которая обычно располагается перед массивом или программой.

control line [kən'troul laɪn] управляющая линия. @ Линия многопроводного интерфейса, служащая для передачи управляющих сигналов.

control point [kən'troul pɔɪnt] опорная точка. @ В машинной графике – точка заданной линии или поверхности, на основании которой строится аппроксимирующая линия или поверхность.

control program (CP) [kən'troul 'prəʊgræm] управляющая программа. @ 1. Операционная система. 2. Часть операционной системы, занимающаяся диспетчеризацией.

control record [kən'troul 'rekɔ:d] контрольная запись. @ Запись, которая содержит контрольные суммы, вычисленные путем суммирования значений из других записей файла. Контрольные суммы могут нести дополнительную информацию или использоваться только для проверки правильности данных.

control section (CS, CSECT) [kən'troul 'sekʃən] программная секция. @ В языке ассемблера – группа команд, которые должны быть расположены в непрерывной области памяти.

control stack [kən'troul stæk] управляющий стек. @ Стек, содержащий цепочку выполняемых команд. Является частью устройства управления в вычислительных машинах со стековой архитектурой.

control storage [kən'troul 'stɔ:ɹɪdʒ] управляющая память. @ Запоминающее устройство, содержащее управляющие программы или микропрограммы. Обычно реализуется как постоянное запоминающее устройство.

control structure [kən'troul 'strʌktʃə] управляющая структура, управляющая конструкция. @ Конструкция языка программирования для задания последовательности выполнения действий: операторы цикла, условный оператор.

controlled [kən'trould] *adj.* контролируемый. @ **controlled authority** орган контроля (администрация криптосети). @ **controlled cryptographic item (CCI) assembly** комплект оборудования, являющийся контролируемым криптогра-

фическим изделием. @ **controlled cryptographic item (CCI) component** устройство, являющееся частью контролируемого криптографического изделия. @ **controlled cryptographic item (CCI) equipment** оборудование, в состав которого входит контролируемое криптографическое изделие. @ **controlled cryptographic item** контролируемое криптографическое изделие (несекретное криптографическое оборудование, использование которого осуществляется под строгим контролем со стороны государства). @ **controlled key distribution** контролируемое распределение ключей. @ **controlled member** управляемый элемент. @ **controlled process** управляемый (регулируемый) процесс. @ **controlled sampling** управляемый выбор дискретных данных. @ **controlled variable** управляемая переменная.

controlling [kən'troulɪŋ *adj.* контролирующий. @ **controlling mean** средства управления (регулирования).

controversy ['kɒntɹəvɜ:sɪ] *n.* дискуссия, спор. # **without (beyond) controversy** неоспоримо, бесспорно

convention [kən'venʃən] *n.* 1. собрание, съезд; 2. договор, соглашение; 3. обычай; обыкновение; 4. условие; условное обозначение. # **by convention** принято; обычно

conventional [kən'venʃənəl] *adj.* 1. принятый; 2. обычный; традиционный, стандартный; 3. условный. @ **conventional cipher** традиционный шифр (с секретным ключом). @ **conventional cryptanalysis** традиционный криптоанализ (без использования компьютеров). @ **conventional cryptographic key** ключ традиционной (одноключевой) криптографической системы. @ **conventional cryptographic means** традиционные криптографические средства. @ **conventional signature scheme** стандартная схема цифровой подписи. # **in is conventional** обычно; принято.

conventional cryptosystem = symmetric cryptosystem

conversational [kən'vɜ:ʃənəl] *adj.* переговорный, диалоговый. @ **conversational key** переговорный ключ (используемый для переговоров при согласовании общего ключа). @ **conversational compiler** диалоговый транслятор. @ **conversational mode** диалоговый режим.

conversational (linguistic) model [kən'vɜ:ʃənəl ('lɪŋgwɪstɪk) 'mɒdl] модель языковая. @ Любая конструкция на естественном языке, рассматриваемая как описание чего-л. (например, определение как модель определяемого; имя, как обозначение называемого и т. д.).

conversational processing [kən'vɜ:ʃənəl 'prəʊsesɪŋ] диалоговая обработка. @ Обработка данных в режиме человек – машина.

conversational program [kən'vɜ:ʃənəl 'prəʊgræm] диалоговая программа. @ Программа обработка данных в режиме человек – машина.

convey ['kɒn'veɪ] *v.* перевозить, транспортировать; 2. передавать; 3. сообщать. # **to convey the impression** создавать впечатление.

coprime ['kɒpraɪm] *adj.* взаимно простой.

corner ['kɔ:nə] *n.* 1. угол; 2. часть, район. # **corner stone** краеугольный камень. # **the four corners of the earth** четыре страны света.

correct [kə'rekt] *adj.* правильный; истинный; *v.* исправлять, поправлять, корректировать. @ **correct decryption** правильное расшифрование. @ **correct key** правильный ключ. # **correct to** с точностью до. # **corrected to (for)** с поправкой на.

correlation [kɔrɪ'leɪʃən] 1. корреляция. @ Мера согласованности двух или более случайных переменных. 2. связь, соотношение. @ **correlation attack** корреляционная атака (криптоанализ на основе выявления статистической зависимости между элементами входной и выходной последовательностями шифратора). @ **correlation attack secure** защищённый от корреляционной атаки. @ **correlation immunity** корреляционная стойкость (степень статистической зависимости между элементами входной и выходной последовательности шифратора). @ **correlation device** корреляционное устройство. @ **correlation difference** корреляционная разность. @ **correlation function (CF)** функция корреляции (корреляционная функция). @ **correlation matrix** матрица коэффициентов корреляции, корреляционная матрица. @ **correlation-immune** корреляционно-стойкий (характеризующийся отсутствием статистической зависимости между элементами входной и выходной последовательностями шифратора).

correspond [kɔrɪ'spɒnd] *v.* 1. соответствовать (**with, to**); согласовываться; 2. быть аналогичным (**to**); 3. переписываться (**with**). # **to bring correspond** приводить в соответствие.

corrupt [kə'rʌpt] *n.* компрометировать. @ **corrupt KDC** компрометировать KDC.

corrupted [kə'rʌptɪd] *adj.* скомпрометированный. @ **corrupted key** скомпрометированный (потерявший секретность – вскрытый противником или ставший ему известным каким-либо другим способом) ключ.

cost [kɒst] *n.* 1. цена, стоимость; 2. расходы; издержки. # **at any cost** любой ценой; во что бы то ни стало. # **at all cost** любой ценой; во что бы то ни стало. # **at the cost of** ценой чего-л.; за счет. # **at one's cost** за чей-л. счет.

count [kaunt] *n.* 1. счет, подсчёт, маркировка; 2. единица счета, одиночный импульс счета; *v.* 1. считать, подсчитывать, отсчитывать; 2. полагать; 3. полагаться на (**on, upon**).

count of character frequencies = character frequency

counter mode счётный режим (один из режимов работы синхронного точного шифра)

counter ['kauntə] *n.* счетчик, пересчетное устройство, пересчетная схема; *adj.* противоположный. @ **counter body** корпус счетчика. @ **counter capacity** емкость счетчика, коэффициент передачи счетчика. @ **counter circuit** счетная схема, схема счетчика. @ **counter register** 1. счетчик; 2. регистр счетчика. @ **counter tipe adder** сумматор накапливающего типа, накапливающий сумматор.

counter- ['kauntə] *pref.* придает значение против-, контр-, например: **counter-clockwise** против часовой стрелки.

counterfeit ['kauntə'feit] *adj.* поддельный. @ **counterfeit cipher** поддельный шифр.

counting *n.* = **count**

country ['kʌntri] *n.* 1. страна; 2. родина, отечество; 3. сельская местность; 4. местность, территория. # **country at large** вся страна. # **in this country** *переводится названием той страны, в которой была написана данная статья (книга)*

couple ['kʌpl.] *n.* пара; *v.* соединять; сочетать. # **coupled with** в сочетании с, вместе с

coupling ['kʌplɪŋ] *n.* 1. связь; соединение; 2. взаимодействие. # **cross coupling** перекрестные связи

courier ['kʊriə] *n.* курьер, посыльный. @ **courier time** время защиты (промежуток времени, в течение которого шифрсистема противостоит попыткам её вскрытия). @ **courier-based key distribution** распределение ключей с помощью курьеров (посыльных). @ **courier-based key management** управление ключами с помощью курьеров (посыльных). @ **courier-delivered key** доставленный курьером (посыльным) ключ.

course [kɔ:s] *n.* ход, течение, курс. @ **course in cryptanalysis** курс криптоанализа. # **as a matter of course** как нечто само собой разумеющееся. @ **course calculator** 1. вычислитель курса; 2. навигационный вычислитель. @ **course-of-value function** производящая функция. # **during (in) the course of** в течение, во время. # **in due course (time)** со временем, в свое время. # **in the course of time** с течением времени. # **of course** конечно.

cover ['kʌvə] *v.* 1. покрывать; 2. занимать, простираться; 3. охватывать, включать; 4. рассматривать; *n.* защита. @ **cover time** время защиты (промежуток времени, в течение которого шифрсистема противостоит попыткам её вскрытия).

crack [kræk] *n.* трещина; *v.* вскрывать. @ **crack a cipher** вскрывать шифр. @ **crack a cipher machine** вскрываемая шифр машина.

crackable [kræk'eɪbl] *adj.* вскрываемый. @ **crackable cipher** вскрываемый шифр.

cracker [krækə] *n.* взломщик, "крэкер" (человек, взламывающий средства контроля доступа к компьютерным системам как для незаконного обогащения, так и ради удовольствия лишний раз воспользоваться своими навыками).

cracking [krækiŋ] *n.* вскрытие. @ **cracking a cryptosystem** вскрытие криптосистемы. @ **cracking contest** состязания по вскрытию (криптосистем). @ **cracking program** программа вскрытия.

credit ['kredit] *v.* 1. доверять; 2. отдавать должное; 3. приписывать кому-л., что-л. (with). # **to give credit for** отдавать должное.

crib [krib] *n.* криб, подстрочник (наиболее вероятный вариант открытого текста для некоторого отрезка шифрованного текста). @ **crib dragging** метод протягивания криба (подстрочника).

cribster [kɹɪbstə] *n.* кривстер (криптоаналитик, который вскрывает шифры исключительно с помощью подстроичника).

criteria ['kraɪ'tɪəriə] *n.* критерий.

crux [krʌks] *n.* затруднение; трудный вопрос. # **the crux of the matter** суть дела.

cryppee [kɹɪpi:] *n.* жарг. криптограф.

cryppie *n.* = **cryppee**

cryptoengineer [kɹɪptɔ, en'ʤɪniə] *n.* инженер-криптограф.

cryptophonic [kɹɪptɔ, founɪk] *adj.* криптотелефонный, криптофонический (относящийся к засекречиванию телефонной связи путем шифрования речи). @

cryptophonic device криптотелефонное (криптофоническое) устройство. @

cryptophonic module криптотелефонный (криптофонический) модуль.

crypt- [kɹɪpt] = **crypto-** [kɹɪptɔ]

crypt *n.* (разг.) = **cryptogram**

crypt *n.* 1. разг. = **cryptogram**; 2. "Крипт" (программа шифрования по DES-алгоритму в операционной системе UNIX). @ **crypt bit** бит криптограммы (шифртекста).

cryptalgorithm *n.* = **cryptoalgorithm**

cryptanalyse an algorithm подвергать алгоритм (шифрования) криптоанализу.

cryptanalyse [kɹɪptə'næləs] *v.* подвергать криптоанализу, проводить криптоанализ.

cryptanalysing [kɹɪptə'næləsɪŋ] *n.* проведение криптоанализа.

cryptanalysis [kɹɪptə'næləsɪz] *n.* криптоанализ (анализ криптосистемы с целью определения засекреченных переменных и другой значимой информации об этой криптосистеме, включая открытый текст, шифруемый с её помощью). @ **cryptanalysis by frequency counts** криптоанализ на основе маркировок. @ **cryptanalysis results** результаты криптоанализа. @ **cryptanalysis techniques** методы криптоанализа.

cryptanalyst [kɹɪptə'nælist] *n.* криптоаналитик, дешифровальщик. @ **cryptanalyst hours** время, требуемое криптоаналитику для вскрытия шифра.

cryptanalytic [kɹɪptə'nælitɪk] *adj.* криптоаналитический. @ **cryptanalytic community** криптоаналитическое сообщество. @ **cryptanalytic defence** защита от криптоанализа. @ **cryptanalytic information** информация, существенная для криптоанализа. @ **cryptanalytic machine** (вычислительная) машина, используемая для криптоанализа. @ **cryptanalytic use of high-speed computers** использование высокоскоростных компьютеров для криптоанализа.

cryptanalytically [kɹɪptə'nælitɪklɪ] *adv.* криптоаналитически. @ **cryptanalytically equivalent ciphers** криптоаналитически эквивалентные шифры (если удаётся вскрыть один из криптоаналитически эквивалентных шифров, то вскрывается и другой). @ **cryptanalytically secure key** стойкий к криптоанализу ключ.

cryptanalytics [kriptə'nælɪtiks] *n.* методика криптоанализа, теория и техника вскрытия шифров.

cryptanalyze [kriptə'nælaɪz] *v.* = **cryptanalyse**

cryptanalyzed [kriptə'nælaɪzɪd] *adj.* подвергнутый криптоанализу. @ **crypt-analyzed intercept** перехваченное сообщение, подвергнутое криптоанализу.

cryptarithm [kriptə'riθm] *n.* криптоарифметика. @ Арифметическая задача, в которой вместо цифр используются буквы, причем: (а) каждая цифра заменяется ровно на одну букву и встречается хотя бы раз; (б) самая старшая значащая цифра любого числа не может быть нулем; (в) если основание системы счисления отлично от 10, этот факт оговаривается особо.

cryptic [krip'tɪk] *adj.* 1. записанный в зашифрованном виде (в форме криптограммы) криптографически закрытый; 2. криптологический.

cryptically-written [kript'ɪrɪtn] *adj.* записанный в зашифрованном виде (в виде криптограммы).

cryption *n.* = **encryption**

cryptkeyer [kript,kiə] *n.* сотрудник службы безопасности, отвечающий за работу криптографических средств.

CRYPTO *n.* гриф на документах, имеющих отношение к криптографической защите информации; категория секретности "КРИПТО".

crypto- [kriptɔ] в сложных и сложносоставных словах имеет значение крипто- .

cryptoaccount [kriptou,ə'kaunt] *n.* учет работы криптографических средств.

crypto-administration [kriptou, *n.* администрация криптографической службы.

cryptoalarm (cryptographic alarm) [kriptɔ, *adj.* криптосигнализация.

cryptoalgorithm [kriptou'ælgɔ,ɾɪdʒəm] *n.* 1. криптоалгоритм, алгоритм шифрования; 2. суженный криптоалгоритм (стойкость определяется секретностью самого алгоритма).

cryptoanalysis *n.* = **cryptanalysis**

cryptoanarchist [kriptou'ænəkɪst] *n.* криптоанархист. @ **cryptoanarchist manifesto** манифест криптоанархистов.

cryptoanarchy [kriptou'ænəkɪ] *n.* криптоанархизм (бесконтрольное, нерегулируемое законом распространение криптотехнологий).

cryptoancillary [kriptou,æn'sɪləɾɪ] *adj.* криптовспомогательный. @ **crypto-ancillary equipment** вспомогательное криптографическое оборудование (предназначено для выполнения функций, которые способствуют более эффективной и надежной работе криптографических устройств).

cryptoanonymity [kriptou,ænənɪmɪtɪ] *n.* криптоанонимность.

cryptoboard [kriptou,bɔ:d] *n.* криптоплата.

cryptobully [kriptou'bulɪ] *n.* криптогромила, криптобандит.

cryptocard [kriptou,ka:d] *n.* криптокарта.

cryptocenter [kriptou,sentə] *n.* криптоцентр, шифрцентр.

cryptochannel [kriptou'tʃænɪ] *n.* криптоканал (канал криптографически защищенной связи).

cryptochip [kriptou,tʃɪp] *n.* крипточип, криптомикросхема.

cryptocommunications [kriptou,kə'mjuːnɪ'keɪʃəns] *n.* криптографически защищенная связь.

cryptocommunity [kriptou,kə'mjuːnɪtɪ] *n.* криптосообщество.

cryptocompany [kriptou'kʌmpəni] *n.* криптокомпания.

cryptocompatibility [kriptou,kəm,pætə'bɪlɪtɪ] *n.* криптосовместимость.

cryptocomplexity [kriptou'kɒmpleksɪtɪ] *n.* криптографическая сложность (стойкость).

cryptoconference [kriptou'kɒnfəɪəns] *n.* криптоконференция.

crypto-control [kriptou,kən'trəʊl] *n.* криптоконтроль.

cryptocorrespondence [kriptə,kɒrɪs'pɒndəns] *n.* шифрпереписка.

cryptocriminal [kriptou'krɪmɪnəl] *n.* криптопреступник.

cryptocustodian [kriptou,kʌs'təʊdɪən] *n.* ответственный за хранение ключей.

crypto-dedicated chip = cryptochip

cryptodeveloper [kriptou,dɪ'veləpə] *n.* крипторазработчик. @ **cryptodeveloper kit (CDK)** набор средств крипторазработчика.

cryptodevice [kriptou,dɪ'vaɪs] *n.* криптографическое устройство, криптоприбор, шифратор

crypto-engine [kriptou,ɛn'dʒɪn] *n.* 1. криптосредство; 2. криптографический алгоритм.

cryptoequipment [kriptou,ɪ'kwɪpmənt] *n.* криптографическое оборудование, шифраппаратура.

crypto-fill [kriptou,fɪl] *adj.* (предназначенный) для загрузки (ввода) ключей. @ **crypto-fill device** устройство ввода ключей.

cryptogear [kriptou,ɪə] *n.* криптографическое устройство.

cryptogram ['kriptou,ræm] *n.* 1. криптограмма, тайнопись, шифрованное сообщение; 2. "Криптограмма" (журнал Американской криптологической ассоциации, выходящий раз в два месяца). @ **cryptogram residue class** класс вычетов криптограмм. @ **cryptogram space** пространство криптограмм.

cryptograph ['kriptou,ræf] *n.* 1. шифровальная машина; 2. криптография. @ Наука о построении отображений информации, используемых с целью ее защиты, которые называются криптографическими.

cryptographer ['kriptou,ræfə] *n.* криптограф.

cryptographic ['kriptou,ræfɪk] *adj.* криптографический. @ **cryptographic aids** криптографические средства. @ **cryptographic alarm** криптографическая сигнализация (специальное устройство, которое отслеживает сбои или изменения в работе криптографического оборудования и сигнализирует обслуживающему персоналу об их возникновении). @ **cryptographic alarm** сигнализация о нарушении криптографических правил. @ **cryptographic Application**

Programming Interface (CAPI) криптографический прикладной программный интерфейс пользователя (набор криптографических программных средств, разработанных американской корпорацией "Майкрософт" и предоставляемых программистам для разработки собственных приложений, взаимодействующих с этими средствами).@ **cryptographic attack** криптографическая атака (попытка криптоаналитика вызвать отклонения в атакуемой защищенной системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытием).@ **cryptographic authentication** криптографическая аутентификация (с использованием криптографических средств и методов).@ **cryptographic channel** криптографически защищенный канал.@ **cryptographic checksum** криптографическая контрольная сумма.@ **cryptographic checkvalue** криптографическая контрольная величина (получается путем криптографического преобразования блока данных и предназначена для контроля целостности информации, передаваемой по каналам связи).@ **cryptographic clerk** шифровальщик.@ **cryptographic commodities** криптографическое оборудование (криптографические средства).@ **cryptographic community** криптографическое сообщество.@ **cryptographic compatibility** криптографическая совместимость.@ **cryptographic component** криптографический узел (устройство для аппаратной реализации криптографического алгоритма).@ **cryptographic course** курс криптографии.@ **cryptographic design vulnerabilities** слабые места криптографических систем.@ **cryptographic devices** криптографическая аппаратура, криптографические устройства.@ **cryptographic encryption** криптографическое шифрование.@ **cryptographic equipment room (CER)** помещение для криптографического оборудования (охраняемая экранированная комната для размещения в ней криптографического оборудования).@ **cryptographic equipment (cryptoequipment)** криптографическая аппаратура.@ **cryptographic expert** эксперт в области криптографии.@ **cryptographic facilities** криптографическое оборудование (криптографические средства).@ **cryptographic fiction (cryptofiction)** криптографическая художественная литература (литературное произведение одна из главных сюжетных тем которого связана с криптографией).@ **cryptographic hash function** криптографическая хэш-функция.@ **cryptographic information** криптографическая информация (относится к криптографическим системам и средствам).@ **cryptographic initialization** инициирование криптографических процессов (напр., вводом ключа).@ **cryptographic integrity** криптографическая целостность (стойкость).@ **cryptographic interception** перехват шифрованной информации.@ **cryptographic interface** криптоинтерфейс (интерфейс криптографического устройства).@ **cryptographic jargon** криптографический жаргон.@ **cryptographic literature** литература по криптографии.@ **cryptographic logic** криптографическая логика (аппаратная реализация криптографического алгоритма, дополненная криптосигнализацией и другими средствами обеспечения эффективной и надежной работы криптографического оборудования).@ **cryptographic loop-hole** криптографическая слабость.@ **cryptographic materials** криптографические материалы.@ **cryptographic means** криптографические средства.@ **cryptographic mechanism**

криптографический механизм. @ **cryptographic mistake** криптографическая ошибка. @ **cryptographic network** сеть с криптографической защитой. @ **cryptographic option** дополнительное криптографическое оборудование (поставляемое вдобавок к основному). @ **cryptographic parameter** криптографический параметр. @ **cryptographic prime** простое число, используемое в криптосистеме. @ **cryptographic primitive** криптографический примитив (элементарное понятие из области криптографии — блочный шифр, алгоритм цифровой подписи и т.д.). @ **cryptographic procedure** криптографическая процедура. @ **cryptographic protection** криптографическое закрытие информации (криптографическая защита). @ **cryptographic random number generator (CRNG)** криптографический генератор случайных чисел. @ **cryptographic randomization** криптографическая рандомизация (функция, позволяющая случайным образом задавать состояние шифратора). @ **cryptographic research** криптографические исследования (исследования в области криптографии). @ **cryptographic sensitivity** криптографическая уязвимость. @ **cryptographic separation** криптографическое разделение (информации с использованием различных ключей шифрования). @ **cryptographic service message** сообщение криптографической службы. @ **cryptographic Service Provider Developer Kit (CSPDK)** Набор разработчика средств криптографического сервиса. @ **cryptographic Service Provider (CSP)** средство криптографического сервиса (программный модуль для выполнения криптографических операций). @ **cryptographic service** криптографическая служба. @ **cryptographic strength** криптографическая стойкость — способность шифрсистемы противостоять атакам криптоаналитика. @ **cryptographic success** успех (достижение) в области криптографии. @ **cryptographic system (cryptosystem)** криптографическая система. @ **cryptographic transformation** криптографическое преобразование. @ **cryptographic variable (cryptovariable, CV)** криптографическая переменная (напр., ключ). @ **cryptographic** криптографическое приложение.

cryptographic protocol ['kriptou,ɹæfɪk 'proutəkɔl] криптографический протокол. @ Определенный порядок взаимодействия абонентов, использующих секретную связь. Криптографические протоколы являются важной составной частью криптографической системы. Нередки ситуации, когда задачи обеспечения безопасности информации не решаются из-за наличия слабостей в протоколе, несмотря на использование соответствующих хороших криптографических отображений. Главное отличие протокола от алгоритма заключается в том, что реализация алгоритма предполагает активные действия одного субъекта, а протокол реализуется в ходе взаимодействия нескольких субъектов — активных сторон протокола.

cryptographic *n.* = **cryptography**

cryptographically ['kriptou,ɹæfɪkəlɪ] *adv* криптографически. @ **cryptographically compressed form of a message** криптографически сжатая форма сообщения. @ **cryptographically equivalent** эквивалентные по стойкости. @ **cryptographically random** криптографически случайный (псевдослучайная последовательность называется криптографически случайной, если ее следующий

элемент вычислительно невозможно предсказать, даже зная алгоритм генерации этой последовательности и все ее предшествующие элементы).@ **cryptographically secure random number generator (CSRNG)** криптографически стойкий генератор случайных чисел.@ **cryptographically secure** криптографически стойкий.@ **cryptographically token** криптографический маркер.@ **cryptographically voting** криптографическое голосование (разновидность криптографических протоколов для анонимного голосования).@ **cryptographically-protected communication** связь с криптографическим закрытием информации (шифр-связь).

cryptographically strong = **cryptographically secure**

cryptographie *n.* = **cryptography cryptographically strong random number generator** = **cryptographically secure random number generator**

cryptographing ['kriptou,ra:fiŋ] *n.* разработка и применение средств криптографической защиты.

cryptography ['kriptou,ra:fi] *n.* криптография.@ Наука о принципах, средствах и методах преобразования информации для защиты ее от несанкционированного доступа и искажения. Криптография - одна из старейших наук, ее история насчитывает несколько тысяч лет. Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств. Известно более десятка проверенных алгоритмов шифрования, которые при использовании ключа достаточной длины и корректной реализации алгоритма, криптографически стойки. Криптография не занимается: защитой от обрыва, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных. @ Защита сообщения путем превращения его в набор знаков, расшифровать который может только человек, знающий ключ.@ **cryptography textbook** учебник (пособие / руководство) по криптографии.

cryptoguru ['kriptou'guru:] *n.* криптогуру.

cryptohuddle ['kriptou'hʌdl] *n.* криптосговор.

cryptoignition ['kriptou,ig'nɪʃən] *n.* инициирование криптографических операций.@ **cryptoignition key (СК)** ключ инициирования криптографических операций.

cryptoinformation ['kriptou,ɪnfə'meɪʃən] *n.* 1. шифрованная информация; 2. информация, используемая при криптоанализе; 3. информация, имеющая отношение к криптосистеме.

cryptoinsecurity ['kriptou,ɪnsɪ'kjuəriti] *n.* нарушение криптостойкости (вследствие ошибки оператора или сбоя аппаратуры).

cryptointerface ['kriptou,ɪntə'feɪs] *n.* криптоинтерфейс (интерфейс криптографического устройства).

cryptokey ['kriptou,ki:] *n.* криптоключ.@ **cryptokey entry** ввод ключа.@ **cryptokey generator** генератор криптоключей.

crypto-like ['kriptou,laɪk] *adj.* криптоподобный. @ **crypto-like transformation of information** криптоподобное преобразование информации.

crypto-linguist *n.* = **cryptolinguist**

cryptolinguist ['kriptou'liŋgwɪst] *n.* криптолингвист.

cryptolinguistics ['kriptou'liŋgwɪstɪk] *n.* криптолингвистика (применение лингвистики в криптологии).

cryptolock ['kriptou,lɒk] *n.* криптозамок.

cryptologer *n.* = **cryptologist**

cryptologic ['kriptou'lɒdʒɪk] *adj.* = **cryptological**

cryptological ['kriptou'lɒdʒɪkəl] *adj.* криптологический. @ **cryptological** криптологическое агентство. @ **cryptological circles** криптологические круги. @ **cryptological matters** вопросы, имеющие отношение к криптологии. @ **cryptological Readiness Group (CRG)** Группа криптологической готовности. @ **cryptological-technician (CTT)** специалист-криптолог.

cryptologist ['kriptou,lɒdʒɪst] *n.* криптолог (специалист по криптологии)

cryptology ['kriptou,lɒdʒɪ] *n.* криптология (наука о безопасности связи). @ Название науки криптологии составляется из греческих слов: «criptos» – тайный и «logos» – слово. В современном понимании предметом криптологии являются отображения информации, используемые для ее защиты от любых несанкционированных действий злоумышленников (преступников). С самого начала эта наука развивалась как двуединая, состоящая из двух частей – криптографии и криптоанализа.

cryptomachine ['kriptou,mə'ʃi:n] *n.* криптомашина; криптографическая (шифровальная) машина.

cryptomapping ['kriptou'mæpɪŋ] *n.* криптоотображение.

cryptomaterial ['kriptou,mə'tɪəriəl] *n.* документы или аппаратура, содержащие криптографическую информацию.

cryptomathematics ['kriptou,mæθɪ'mætɪks] *n.* криптоматематика (применение математики в криптологии).

cryptomicroprocessor ['kriptou'maɪkrou'prəʊsesə] *n.* 1. криптомикропроцессор (работает по зашифрованной программе); 2. микропроцессор криптографического устройства.

cryptomode ['kriptou,məʊd] *n.* крипторежим (режим работы с криптографической защитой).

cryptomodule ['kriptou'mɒdju:l] *n.* криптомодуль, модуль с криптографическими средствами.

cryptomonopoly ['kriptou,mə'nɒpəlɪ] криптомонополия.

cryptonet ['kriptou,net] *n.* криптосеть (сеть криптографически защищённой связи). @ **cryptonet key (CNK)** ключ криптосети.

crypto-only mode ['kriptou'əʊnlɪ,məʊd] *n.* режим работы только с криптографической защитой.

cryptooperation ['kriptou,ɔpə'reɪʃən] *n.* криптооперация работа в режиме криптографической защиты.

cryptopackage ['kriptou'pækɪdʒ] *n.* 1. пакет программ для криптографической защиты информации; 2. криптографическое устройство (криптографический прибор) в отдельном корпусе.

cryptopager ['kriptou'peɪdʒə] *n.* криптопейджер (средство персонального конфиденциального радиовызова).

cryptoparts ['kriptou,pa:ts] *n.* блоки, на которые разбиваются сообщения (в соответствии с принятым в криптосистеме форматом).

cryptopatent ['kriptou'peɪtənt] *n.* криптопатент.

cryptoperiod ['kriptou'pɪəriəd] *n.* криптопериод (период шифрования текста на одном ключе).@ **cryptoperiod diffusion** размывание криптопериода.

cryptopersonnel ['kriptou'pɜ:snl] *n.* персонал (личный) состав криптографической службы.

cryptophonie ['kriptou,founɪ] *n.* криптотелефония (телефонная связь с криптографической защитой от подслушивания).

cryptopolicy ['kriptou'pɒlɪsɪ] *n.* политика в области криптографии.

cryptoprinciple ['kriptou'prɪnsəpl] *n.* принцип криптографического преобразования информации.

cryptoprocessor ['kriptou'prəʊsesə] *n.* 1. криптопроцессор (работает по зашифрованной программе) ; 2. процессор криптографического устройства.

cryptoproof ['kriptou,pru:f] *adj.* криптостойкий.

cryptopunk ['kriptou,pʌŋk] *n.* криптопанк (человек, который придерживается мнения о том, что любая информация частного характера неприкосновенна и должна быть надёжно защищена с помощью стойких криптографических алгоритмов).

cryptor ['kriptə] *n.* устройство шифрования, шифратор.

cryptoradio ['kriptou'reɪdɪəʊ] *n.* крипторадио (оснащённая шифратором радиостанция).

cryptoresearcher ['kriptou,rɪ'sə:tʃə] *n.* криптоисследователь.

"**cryptosaur**" ['kriptou,sɔ:t] *n.* "криптозавр" (маститый специалист-криптолог, достижения которого стали достоянием истории).

cryptosecure ['kriptou,sɪ'kjuə] *adj.* криптостойкий.

cryptosecurity ['kriptou,sɪ'kjuəritɪ] *n.* 1. обеспечение безопасности криптографическими средствами; криптографическая защита; 2. криптостойкость.@ **cryptosecurity device** прибор для криптографической защиты.

cryptoserver ['kriptou'sɜ:və] *n.* криптосервер.

cryptoservice ['kriptou,] *n.* криптографическая служба.

cryptosoft ['kriptou'sɒft] *n.* криптософт (криптографическое программное обеспечение).

cryptospeak ['kriptou,spi:k] *n.* криптотерминология, криптожаргон.

cryptostrength ['kriptou,strenθ] *n.* криптостойкость.

cryptosynchronization (cryptosync) ['kriptou,sɪŋkrənai'zeɪʃən] *n.* криптосинхронизация (синхронизация криптографических устройств/процессов).

cryptosystem (CS) ['kriptou'sistɪm] *n.* криптосистема, система шифрования (семейство обратимых преобразований открытого текста в зашифрованный).

cryptosystem assessment оценка криптосистемы (процесс определения применимости криптосистемы на практике).

cryptosystem designer разработчик криптосистемы.

cryptosystem evaluation анализ криптосистемы (поиск уязвимостей в криптосистеме).

cryptosystem review проверка криптосистемы (рассмотрение криптосистемы органом контроля на предмет полноты реализуемых ею функций и определения области ее применения).

cryptosystem survey инспектирование криптосистемы (пользователи криптосистемы излагают свое мнение относительно того, насколько полно она удовлетворяет их потребностям, и делятся с разработчиками этой криптосистемы своими соображениями о путях ее усовершенствования).

cryptosystem that would take millions of years to break криптосистема, для вскрытия которой потребуются миллионы лет.

cryptosystem with 56 bit keys криптосистема с 56-битным ключом.

crypto-tape ['kriptou,teɪp] *n.* криптолента (с шифртекстом или ключом).

cryptotechnology ['kriptou,tek'nɒ'lədʒɪ] *n.* криптотехнология (технология проектирования, изготовления и эксплуатации криптографических устройств).

cryptotelephone ['kriptou'telifoun] *n.* криптотелефон (телефонный аппарат с шифратором или скремблером).

cryptoterm ['kriptou,tə:m] *n.* криптотермин.

cryptotext ['kriptou,tekst] *n.* криптотекст, шифртекст.

cryptothriller ['kriptou'θrɪlə] *n.* криптотриллер (роман с захватывающим сюжетом, одной из главных тем которого является криптология).

crypto-to-plain ['kriptou,tu:'pleɪn] *n.* преобразование зашифрованного текста в открытый.

cryptotransaction ['kriptou,træn'zækʃən] *n.* криптооперация.

cryptouser ['kriptou'ju:zə] *n.* криптопользователь.

cryptovector ['kriptou'vektə] *n.* криптовектор (вектор ключа или вектор начального заполнения ключевого генератора).

cubic ['kju:bɪk] *adj.* кубический. **cubic congruential generator** кубический конгруэнтный генератор.

current ['kʌrənt] *adj.* действующий, текущий. **current key** действующий (в течение определённого периода времени) ключ.

custodian [kʌ'stədiən] *n.* хранитель (лицо, владеющее информацией или отвечающее за ее сохранность). **custodian of a public directory** хранитель открытого справочника (ключей или криптоалгоритмов).

custom ['kʌstəm] *adj.* изготовленный, сделанный на заказ. **custom key** заказной ключ (ключ заказчика (шифратора)).

customer ['kʌstəmə] *n.* заказчик. **customer-specific key** ключ со структурой, определяемой пользователем (заказчиком).

customised ['kʌstə,mɪst] *adj.* соответствующий требованиям заказчика.@ **customised cryptography** криптография, соответствующая требованиям заказчика.

cut [kʌt] *v.* 1. удалять, вырезать.@ В экранных редакторах и машинной графике – удалять выделенный фрагмент текста или изображения с запоминанием его в буфере для последующей вставки в другом месте. 2. снижать, сокращать (**doun**); 3. прерывать; разъединять; выключать (**off**).# **cut and dried** трафаретный, шаблонный.# **cut and try method** экспериментальный метод; метод последовательных приближений.# **clear cut** четкий, ясно выраженный.

cycle (index) counter ['saɪkl ('ɪndeks) 'kaʊntə] счетчик циклов.@ Формальный полином, связанный с группой перестановок на множестве. Указывает разложение перестановок на циклы.

cycle ['saɪkl] *n.* 1. цикл; шаг цикла. 2. такт.@ Время выполнения элементарной внутренней операции процессора. 3. круг.@ **cycle body** тело цикла.@ **cycle check** проверка цикла.@ **cycle index** параметр цикла.@ **cycle index polynomial** полином индексов циклов.@ **cycle order** циклический порядок. @ **cycle per minute (cpm)** период в минуту.@ **cycle shift** циклический сдвиг.@ **cycle stealing** занятие цикла памяти.@ **cycle time** время цикла.@ **cycle of length p** цикл длины p.

cyclic(al) ['saɪklɪk(əl)] *adj.* циклический, периодический.@ **cyclic(al) address generator (CAG)** циклический генератор адресов.@ **cyclic(al) binary code** циклический двоичный код.@ **cyclic(al) check** циклический контроль.@ **cyclic(al) graph** циклический граф.@ **cyclic(al) index** 1. параметр цикла; 2. индекс цикла.@ **cyclic(al) memory** циклическая динамическая память.@ **cyclic(al) permuted code** циклический перестановочный код, циклически перемещаемый код.@ **cyclic(al) process** циклический процесс.@ **cyclic(al) shift** циклический сдвиг.@ **cyclic(al) code-shift keying (CCSK)** манипуляция кодовыми последовательностями.@ **cyclic(al) shift** циклический сдвиг.@ **cyclic(al) redundancy code** в криптологии – циклический избыточный код (функция хэширования, используемая для контроля за появлением ошибок при передаче и преобразовании данных).

cyclic(al) access ['saɪklɪk(əl) 'ækses] циклический доступ.@ Режим доступа к записанной информации в определенные моменты времени цикла событий. Устройством с циклическим доступом является магнитный диск.

cyclic(al) code ['saɪklɪk(əl) koud] циклический (рефлексный) код.@ Код, обладающий следующим свойством: если слово A является элементом кода, то все циклические сдвиги A также являются элементами кода.

cyclic(al) redundancy check (CRC) ['saɪklɪk(əl) rɪ'dʌndənsɪ tʃek] контроль циклическим избыточным кодом.@ Способ контроля с использованием разновидности полиномиального кода.

cyclicity ['saɪklɪksɪtɪ] *n.* цикличность; периодичность.

cyclometre ['saɪ'klɒmɪtə] *n.* циклометр (специальное электро-механическое устройство, изобретенное польскими криптоаналитиками в 1934 г. для автоматизации процесса вскрытия немецкой шифровальной машины "Энигма").

D*

16th department of KGB 16-е управление КГБ (подразделение КГБ, занимавшееся перехватом и дешифрованием сообщений).

daily ['deɪlɪ] *adj.* ежедневный; суточный; *adv.* ежедневно. @ **daily key** ежедневный ключ (ключ текущего дня). @ **daily keying element** ежедневно сменяемый элемент (сменяемая часть) ключа.

"Dancing Men" *n.* "Пляшущие человечки" (рассказ английского писателя А. К. Дойля с описанием оригинального криптоаналитического исследования шифрованного текста).

dark-side ['da:ksaɪd] *adj.* темный, порочный.

dark-side hacker = cracker

data ['deɪtə] *n. pl. om datun (лат.)* данные, информация, факты, сведения, характеристики, установки, координатные показатели. @ **data access arrangement (DAA)** средства доступа к данным. @ **data acquisition unit (DAU)** устройство сбора данных. @ **data address** адрес информации. @ **data addressed memory** ассоциативная память. @ **data analysis display** дисплей для анализа данных. @ **data area** область данных. @ **data array** массив данных. @ **Data Base Task Group (DBTG)** рабочая группа по базам данных, РГБД. @ **data block** совокупность данных, набор данных. @ **data break (cycle stealing)** прерывание для обмена данными (занятие цикла памяти). @ **data bus** шина данных. @ **data channel** канал связи, информационный канал, канал передачи данных. @ **data communication equipment (DCE)** аппаратура передачи данных. @ **data communication terminal** терминал (оконечное устройство) обработки данных. @ **data communications (comms)** передача данных. @ **data concentrator** концентратор данных. @ **data contamination** порча данных. @ **data control block (DCB)** блок управления данными. @ **data control** контроль данных. @ **data corruption data** нарушение целостности данных. @ **data cryptography** криптография для защиты данных. @ **data density** плотность записи. @ **data description** описание данных. @ **data dictionary/directory (DD/D)** словарь (базы) данных. @ **data division** раздел данных. @ **data enciphering key (DEK)** ключ шифрования данных. @ **data Encryption Algorithm** Алгоритм шифрования данных (стандарт шифрования данных USA, введенный в действие в 1981 г. и используемый в американской промышленности). @ **data encryption device** устройство шифратора данных. @ **data encryption equipment (DEE)** оборудование шифрования данных. @ **data Encryption Standard (DES)** Стандарт шифрования данных (USA). @ **data error** ошибка в данных. @ **data exchange control** контроль обмена данных. @ **data exchange key (DEK)** ключ для обмена данными. @ **data format** формат данных. @ **data gathering system** система сбора данных. @ **data handling unit** устройство обработки данных. @ **data handling** обработка информации, обработка данных. @ **data input** вход данных. @ **data level** уровень данных. @ **data link** канал связи. @ **data link (D/L)** 1. канал передачи данных; 2. система автоматической передачи данных. @ **data Link**

Enciphering Standard Стандарт шифрования в линиях связи (введенный в действие в 1981 г. стандарт на шифрование, используемый в промышленности USA).@ **data link encryptor (DLE)** шифратор канала (передачи) данных.@ **data list** список с данными.@ **data management system (DMC)** система управления данными.@ **data mark** метка данных.@ **data medium** носитель данных.@ **data module** винчестерский диск.@ **data network** сеть передачи данных.@ **data origin authentication** аутентификация источника данных.@ **data plotter** графопостроитель.@ **data presentation layer** уровень представления данных.@ **data presentation protocol** протокол уровня представления данных.@ **data processing (DP)** обработка данных.@ **data processing machine** вычислительная машина для обработки данных.@ **data processing operation** операция обработки данных.@ **data processor** процессор для обработки данных.@ **data protection** защита данных.@ **data rate (DR)** скорость передачи данных.@ **data reader** устройство считывания данных.@ **data record** запись данных.@ **data recording control (DRC)** устройство управления записью данных.@ **data recording device (DRD)** устройство записи данных.@ **data reduction system** 1. система преобразования данных; 2. устройство для преобразования данных.@ **data register (DR)** регистр данных.@ **data retrieval system** система поиска данных.@ **data scrambling device** скремблер данных.@ **data security device (DSD)** устройство защиты данных.@ **data set (DS)** 1. набор данных, файл; 2. модем.@ **data sheet** техническое описание.@ **data sink** приемник данных.@ **data source** источник данных.@ **data specification** описание данных.@ **data storage** 1. устройство для запоминания данных; 2. запоминание (хранение) данных.@ **Data Storage Description Language (DSDL)** язык описания хранения данных, язык описания физической структуры базы данных.@ **data storage system** система для хранения данных.@ **data structure language** язык описания физической структуры базы данных.@ **data switching exchange (DSE)** устройство коммутации данных.@ **data tablet** (графический) планшет.@ **data take-off (DTO)** разделение данных.@ **data terminal equipment (DTE)** терминальное оборудование пользователя, оконечное оборудование данных.@ **data terminal** терминал (оконечное устройство) обработки данных.@ **data transfer instruction** команда передачи данных.@ **data transfer** пересылка данных.@ **data transmission (DT)** передача данных.@ **data unit** датчик.@ **data-dependent encryption** зависящее от данных шифрование.@ **data-dependent key** зависящий от (шифруемых) данных ключа.

data encryption key = data enciphering key (DEK)

data encryption processor (DEP) = data ciphering processor (DCP)

data abstraction ['deɪtə 'æbstrækʃən] абстракция данных.@ 1. Использование при работе с объектами только определенных над ними операций без учета их внутреннего представления. 2. Методология программирования, при которой программа описывается как совокупность абстрактных типов данных. Абстракция данных обеспечивает большую модульность, чем процедурная абстракция.

data acquisition ['deɪtə ˌækwɪ'zɪʃən] сбор данных, сбор информации. @ Выделение и первичная обработка параметров физического или информационного процесса для последующей обработки на ЭВМ. Обычно подразумевается ввод данных с терминалов.

data administrator ['deɪtə əd'mɪnɪstreɪtə] 1. администратор данных. @ Человек, определяющий, какая информация хранится в базе данных и как она используется. 2. администратор базы данных.

data aggregate ['deɪtə 'ægrɪɡɪt] агрегат данных. @ Поименованная группа логически связанных элементов данных (полей записи базы данных); составной элемент данных.

data attribute ['deɪtə 'ætrɪbjʊ:t] атрибут (элемента) данных. @ В базах данных – длина, формат, значение, ограничения или другая характеристика элемента данных.

data bank ['deɪtə bæŋk] банк данных. @ Совокупность данных (например, файлов, баз данных) об одной предметной области.

data base (DB) ['deɪtə beɪs] база данных. @ Совокупность взаимосвязанных данных, используемых несколькими приложениями под управлением системы управления базой данных.

data capture ['deɪtə 'kæptʃə] сбор данных, сбор информации. @ Выделение и первичная обработка параметров физического или информационного процесса для последующей обработки на ЭВМ. Обычно подразумевается ввод данных измерительных приборов, подключенных к ЭВМ

data chaining ['deɪtə 'tʃeɪnɪŋ] цепочечная организация данных. @ Такая организация файла данными, когда записи являются связанными. Одна и та же запись может принадлежать двум и более цепочкам. Цепочечная организация позволяет осуществлять доступ к данным в различной последовательности.

data cleaning ['deɪtə 'kli:nɪŋ] очистка данных. @ Устранение ошибок форматирования и ошибок ввода – обычно с помощью программы проверки правильности исходных данных.

data collection ['deɪtə kə'leɪʃən] сбор данных, сбор информации. @ Выделение и первичная обработка параметров физического или информационного процесса для последующей обработки на ЭВМ. Обычно подразумевается ввод данных в пакетном режиме с предварительной ручной обработкой.

data authentication ['deɪtə ɔ:'θentɪkeɪʃən] аутентификация данных. @ **data authentication code (DAC)** код аутентификации данных.

data ciphering ['deɪtə 'saɪfərɪŋ] операция шифрования. @ **data ciphering operation** операция шифрования данных. @ **data ciphering processor (DCP)** процессор шифрования данных. @ **data ciphering unit** устройство шифрования данных.

data compression (compaction) ['deɪtə kəm'preʃən ('kɒmpækʃən)] уплотнение данных, сжатие данных. @ Преобразование данных в более компактную форму для эффективного хранения или передачи.

data definition name (ddname) ['deɪtə ,defɪ'nɪʃən neɪm] имя описания данных, имя определения данных. @ В языке управления заданиями JCL – имя предложения описания набора данных, связывающее описанный набор данных (файл) с текстовым именем, используемым в программе.

data description language (DDL) ['deɪtə dɪs'krɪpʃən 'læŋɡwɪdʒ] язык определения данных, язык описания данных. @ Язык описания структуры базы данных.

data dictionary ['deɪtə 'dɪkʃənəri] словарь (базы) данных. @ Информационная система, описывающая структуру и использование базы данных. Словарь базы данных включает имена и атрибуты элементов данных, описание схемы базы данных и определенных на ней подсхем, описание работающих с базой данных прикладных программ. Словарь базы данных может быть организован в виде отдельной базы данных.

data element ['deɪtə 'elɪmənt] элемент данных. @ В базах данных – элементарная единица информации; соответствует понятию атрибут в реляционных базах данных и понятию поле записи в языках программирования.

data entry ['deɪtə 'entri] 1. ввод данных; 2. информационный элемент. @ Элемент каталога, описывающий данные, в отличие от элементов, содержащих управляющую информацию.

data entry screen ['deɪtə 'entri skri:n] трафарет ввода данных. @ Выводимое на экран (текстовое) изображение в виде таблицы или анкеты с позициями для ввода данных.

data field ['deɪtə fi:ld] поле данных. @ Часть записи или заполняемой формы, предназначенной для значения элемента данных.

data file ['deɪtə faɪl] файл данных. @ Файл, не обладающий специальным смыслом для операционной системы или системы программирования, в отличие от командного, объектного, библиотечного файлов.

data independence ['deɪtə ,ɪndɪ'pendəns] независимость (от) данных. @ Обеспечиваемая системой управления базой данных или операционной системой возможность одинаковой работы программ вне зависимости от изменений физического размещения и представления обрабатываемых данных.

data input ['deɪtə 'ɪnpʊt] ввод данных. @ Операция чтения данных с носителя данных или клавиатуры и последующая запись их в основную память.

data integrity ['deɪtə ɪn'tegriːti] целостность данных. @ Отсутствие ошибок и нарушений согласованности.

data item ['deɪtə 'aɪtəm] элемент данных. @ Поименованная группа данных, обрабатываемая как единое целое: запись, поле записи, элемент массива

data link (layer) protocol ['deɪtə lɪŋk ('leɪə) 'prəʊtəkɒl] канальный протокол, протокол канального уровня. @ Уровень протокола сети передачи данных, регламентирующий установку, поддержание и разъединение логического информационного канала.

data link control protocol ['deɪtə lɪŋk kən'troul 'prəʊtəkɒl] протокол управления каналом передачи данных. @ Протокол связи, преобразующий зашум-

ленные (подверженные ошибкам) каналы передачи данных в каналы связи, свободные от ошибок передачи.

data link hierarchy ['deɪtə lɪŋk 'haɪərə:kɪ] иерархия данных.@ Иерархическая структура записей, в которой запись уровня I содержит данные, общие для набора записей уровня I + 1, и в которой, начиная с высокоуровневой записи, можно осуществить доступ к набору низкоуровневых записей.

data link layer ['deɪtə lɪŋk 'leɪə] канальный уровень.@ Уровень взаимодействия в сети передачи данных, формирующий из данных, передаваемых физическим уровнем, кадры или последовательности кадров, а также обеспечивающий управление доступом к среде передачи и обработку ошибок. Кадры используются для передачи пакетов на сетевом уровне.

data logging ['deɪtə 'lɒɡɪŋ] регистрация данных.@ Процедура, включающая запись всех данных и результатов взаимодействий, которые проходят через данную конкретную точку системы.

data management ['deɪtə 'mænɪdʒmənt] управление данными.@ Термин используется применительно к системам, пользователи которых освобождаются от большинства операций по физическому манипулированию файлами и могут сосредоточить внимание главным образом на логических свойствах данных.

data manipulation language ['deɪtə mænɪpjʊ'leɪʃən 'læŋɡwɪdʒ] язык манипулирования данными, ЯМД.@ Язык для доступа, поиска и модификации базы данных. Различаются автономные ЯМД и ЯМД, включаемые в универсальные языки программирования.

data matrix ['deɪtə 'meɪtrɪks] матрица данных.@ Прямоугольный массив переменных, который может быть числовым, классифицированным или алфавитно-цифровым.

data model ['deɪtə 'mɒdl] модель данных.@ Представление о типах объектов и связей, выделяемых в предметной области для хранения и обработки. Модель данных находит выражение в языке определения данных.

data name ['deɪtə neɪm] имя данных.@ Симболическое имя, используемое программистом для обозначения объекта данных в случае, когда программирование ведется на высокоуровневом языке.

data output ['deɪtə 'aʊtpʊt] вывод данных.@ Операция чтения данных из основной памяти и последующая запись на носитель или отображение на экране дисплея.

data packing ['deɪtə 'pækɪŋ] упаковка данных.@ Размещение структуры данных в памяти или при передаче по линии связи, при которой каждому ее элементу выделяется минимально необходимое число разрядов.

data path ['deɪtə pa:θ] путь данных.@ Термин обозначает любое не только физическое, но и логическое соединение между источником и получателем цифровой или аналоговой информации.

data preparation ['deɪtə 'prepə'reɪʃən] подготовка данных.@ Процесс преобразования данных в машиночитаемый вид для последующего ввода в систему с помощью соответствующего устройства.

data processing system (DPS) ['deɪtə 'prəʊsesɪŋ 'sɪstɪm] система обработки данных. @ Обычно подразумеваются операции, связанные с хранением, поиском, сортировкой, переформатированием и воспроизведением текстовых или табличных данных.

data reduction ['deɪtə rɪ'dʌkʃən] сжатие данных. @ Преобразование большого объема данных в меньший объем.

data representation ['deɪtə ,reprɪzen'teɪʃən] представление данных. @ Соответствие между логическими элементами данных и структурой представляющих их ячеек памяти, сигналов или элементов графического изображения.

data retrieval ['deɪtə rɪ'tri:vəl] выборка данных, обращение к данным. @ Процесс поиска и считывания данных из файла, внешнего устройства или базы

data station ['deɪtə 'steɪʃən] станция сети передачи данных. @ Терминальное оборудование пользователя и средства его сопряжения с сетью.

data stream ['deɪtə stri:m] поток данных. @ Последовательность элементов данных, часто упакованная в виде последовательности слов, имеющих размеры, отличные от размеров элементов данных.

data structure ['deɪtə 'strʌktʃə] структура данных. @ Способ объединения нескольких элементов данных в один: массив, файл, список.

data transfer rate ['deɪtə 'trænsfə reɪt] скорость пересылки данных. @ Скорость перемещения данных между устройствами. Средняя скорость определяется быстродействием устройства записи-считывания, а мгновенная скорость – пропускной способностью интерфейса или канала.

data transfer register ['deɪtə 'trænsfə 'redʒɪstə] регистр передачи данных.

data transfer unit (DTU) ['deɪtə 'trænsfə 'ju:nɪt] блок передачи данных.

data translation ['deɪtə træns-'leɪʃən] конвертирование данных. @ преобразование физического (реже логического) представления данных для работы с ними в другой системе управления данными.

data transparency ['deɪtə træns-'preərənsɪ] независимость от данных. @ Способность сети передачи данных передавать сообщения, содержащие любые комбинации символов или любые последовательности битов.

data type ['deɪtə taɪp] тип (данных). @ В языках программирования – множество допустимых значений и применяемых операций. В большинстве языков понятие типа данных включает также определение способа представления данных в памяти.

data validation ['deɪtə ,vælɪ'deɪʃən] проверка (правильности) данных. @ Предварительная обработка входных данных для проверки их соответствия предъявляемым программой требованиям (диапазон значений, формат представления).

data word ['deɪtə wə:d] слово данных. @ Слово, которое содержит только данные.

date [deɪt] *n.* дата, число; *v.* 1. датировать; 2. вести начало от; относиться к (**from**); 3. устареть. # **at an early date** в ближайшем будущем. # **out of date** ус-

тарелый. # **to this date** до сего времени. # **up to date** современный, новейший. # **(up) to date** на сегодняшний день, в настоящее время; до сих пор.

de facto [di:'fæktou] *adj.* лат. фактический. @ **de facto standard for the encryption of electronic mail** фактический стандарт шифрования электронной почты.

dead [ded] *adj.* 1. мертвый; безжизненный; 2. обесточенный; разомкнутый. # **dead load (weight)** собственный вес; вес конструкции.

deceit [di'si:t] *n.* обман, мошенничество.

decentralized [di:'sentrəlaɪzd] *adj.* децентрализованный. @ **decentralized key distribution** децентрализованное распределение ключей. @ **decentralized key management** децентрализованное управление ключами.

decentralized system [di:'sentrəlaɪzd 'sɪstɪm] децентрализованная система. @ Многопроцессорная система или ЭВМ, в которых управление рассредоточено по различным узлам.

decimated ['desimeɪtɪd] *adj.* прореженная. @ **decimated sequence** прореженная последовательность, полученная в результате отбора элементов исходной последовательности.

decipher (D) [di'saɪfə] *v.* 1. расшифровывать; 2. вскрывать; дешифровывать. @ **decipher a code** вскрывать код. @ **decipher key (DECK)** ключ расшифрования. @ **decipher on the fly** расшифровывать на лету (в темпе ввода шифртекста).

decipherable [di'saɪfərəbl] *adj.* поддающийся вскрытию (дешифровке). @ **decipherable in polynomial time (poly-time)** поддающийся вскрытию (дешифровке) с полиномиальной сложностью.

deciphered [di'saɪfət] *adj.* 1. расшифрованный; 2. дешифрованный. @ **deciphered message** дешифрованное сообщение. @ **deciphered message** расшифрованное сообщение.

decipherer [di'saɪfərə] *n.* 1. устройство расшифрования; 2. дешифратор.

deciphering (D) [di'saɪfəɪŋ] *n.* 1. расшифровывание; 2. дешифрование; 3. устройство для дешифрования сообщений. @ **deciphering alphabet** алфавит расшифрования. @ **deciphering equation** уравнение расшифрования. @ **deciphering function** функция расшифрования. @ **deciphering key** ключ расшифрования. @ **deciphering process** процесс дешифрования. @ **deciphering rule** правило расшифрования.

decipherment [di'saɪfəmənt] *n.* = **deciphering**

decodability *n.* декодируемость.

decode ['di:'koud] *n.* декодированное сообщение; *v.* декодировать, декодировать, дешифровывать.

decoder ['di:'koudə] *n.* декодирующее устройство, декодер, дешифратор. @ **decoder error** ошибка декодирования.

decoding ['di:'koudɪŋ] декодирование. @ Процесс преобразования кодированного сообщения в исходное. @ **decoding scheme** схема декодирования. @

decoding algorithm декодирующий алгоритм.@ **decoding key** ключ декодирования.

decodement ['di:'koudment] *n.* 1. декодирование; 2. декодированный текст.

decrypt ['dekript] *n.* расшифровка (дешифровка) текста; *v.* расшифровывать (дешифровывать) текст.

de-crypt *v.* = **decrypt** *v.*

decrypted ['dekriptid] *adj.* 1. расшифрованный; 2. дешифрованный.@ **decrypted message** расшифрованное (дешифрованное) сообщение.

decrypter *n.* = **decryptor** *n.*

decrypting ['dekriptɪŋ] *adj.* дешифровальный.@ **decrypting service** дешифровальная служба.@ **decrypting unit** дешифровальное подразделение.

decryption ['dekripsən] *n.* 1. расшифровывание; 2. дешифрование; 3. открытый текст.@ **decryption capabilities** дешифровальные возможности.@ **decryption device** дешифратор.@ **decryption efforts** усилия дешифровальщиков.@ **decryption key** ключ расшифрования.@ **decryption of ciphertext** открытый текст шифровки.@ **decryption process** процесс дешифрования.@ **decryption round structure** структура цикла (раунда) расшифрования.

decryment *n.* = **decryption** *n.*

decrypt-only key ['dekript'ounli ki:] ключ только для расшифрования.

decryptor ['dekriptə] *n.* 1. получатель шифрованного сообщения; 2. дешифровальщик.

decypher *v.* = **decipher**

de(-)encryption [de,ɪn'kripsən] *n.* 1. расшифрование (процесс нормального применения криптографического преобразования шифрованного текста в открытый); 2. дешифрование (процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста).

default [dɪ'fɔ:lt] *n.* (используемый) по умолчанию.@ О значении или действии, используемом или выполняемом, если не указано иначе. *v.* принимать значение по умолчанию..# **in default of** за неимением, за отсутствием.

defense [dɪ'fens] *n.* 1. оборона; ; 2. защита.@ **Defense Advanced Research Projects Agency (DARPA)** Управление перспективных исследований и разработок Министерства обороны США.@ **defense Data Network (DON)** Оборонная сеть (передачи) данных.@ **defense Intelligence Agency (DIA)** Разведывательное управление министерства обороны (USA).@ **defense Message System (DMS)** Система (передачи) оборонных сообщений (USA).@ **defense Signals Directorate** Управление безопасности связи (австралийское правительственное ведомство, занимающееся перехватом и дешифрованием сообщений).

defined-plaintext *adj.* = **chosen-plaintext**

defraud [dɪ' frɔ:d] *v.* вводить в заблуждение.@ **defraud a decryptor** вводить в заблуждение получателя шифрованного сообщения.

degenerate [di'dʒenəreɪt] *adj.* вырожденный; вырождающийся *v.* вырождаться. @ **degenerate function** вырожденная функция.

degradation [ˌdegrə'deɪʃən] *n.* 1. снижение производительности; 2. понижение (в звании и т. п.); 3. унижение; 4. упадок; деградация; 5. вырождение.

degradation failure [ˌdegrə'deɪʃən 'feɪljə] деградационный отказ. @ Постепенный отказ за счет ухода характеристик за допустимые пределы.

degree [di'ɡri:] *n.* 1. степень, ступень, уровень, порядок; 2. градус; 3. сорт; 4. звание, ученая степень. @ **degree of a map** степень отображения. @ **degree of accuracy** степень точности. @ **degree of convergence** степень сходимости. @ **degree of correlation** степень корреляции. @ **degree of curvature** порядок кривой. @ **degree of differential equation** порядок дифференциального уравнения. @ **degree of freedom** степень свободы. @ **degree of polynomial** степень многочлена, полинома. @ **degree of unsolvability** степень неразрешимости. @ **degree of vertex** степень вершины. @ **degree of wholeness** степень целостности. @ **degree of security** степень защищенности (криптосистемы). @ **degree operator** оператор задержки. # **to a certain degree** до некоторой степени. # **by degree** постепенно.

delay [di'lei] *n.* отсрочка, задержка, запаздывание, промедление; *v.* задерживать, запаздывать. @ **delay characteristic** характеристика задержки. @ **delay circuit** схема задержки, цепь задержки. @ **delay component** элемент задержки, запаздывающее звено. @ **delay device** устройство (элемент) задержки. @ **delay differential equations** дифференциальные уравнения с запаздывающим аргументом. @ **delay element** элемент задержки, звено с задержкой. @ **delay factor** величина задержки. @ **delay generator** генератор задержки. @ **delay line (DL)** линия задержки. @ **delay line storage** запоминающее устройство на линиях задержки. @ **delay period** период задержки. @ **delay pulse oscillator (DPO)** генератор задержанных импульсов. @ **delay time** время задержки. @ **delay unit** элемент (устройство) задержки, блок задержки. @ **delay-and-sum (DS)** задержка и суммирование.

deliver [di'livə] *v.* 1. доставлять; 2. произносить (речь); читать (лекцию); 3. подавать, питать; *n.* подача, питание.

delivery [di'livəri] *n.* доставка, транспортировка.

demand [di'ma:nd] *v.* требовать; нуждаться; *n.* 1. требование; потребность; 2. спрос. @ **demand assignment (DA)** предоставление (каналов) по требованию. @ **demand assignment multiple access (DAMA)** многостанционный доступ с предоставлением каналов по требованию. @ **demand function** функция спроса. @ **demand meter (DM)** индикатор числа запросов. @ **demand processing** обработка (данных) по мере поступления. # **to meet the demand** удовлетворять требованиям.

demand I/O [di'ma:nd] ввод-вывод по запросу. @ В операционных системах — режим обработки запросов на ввод-вывод, при котором фактическая операция обмена с внешним устройством производится по запросу программы.

demand multiplexing [dɪ'ma:nd 'mʌltɪpleksɪŋ] динамическое мультиплексирование, мультиплексирование по требованию.@ Временное мультиплексирование, при котором логическому каналу выделяется времени только при наличии на нем данных.

demand paging [dɪ'ma:nd 'peɪdʒɪŋ] подкачка по обращению.@ В системах с виртуальной памятью – организация подкачки, при которой необходимая страница или сегмент подкачиваются, когда программа обращается к ним.

demand reading (writing) [dɪ'ma:nd 'ri:diŋ ('raɪtɪŋ)] считывание (запись) по запросу.@ Процесс, при котором происходит непосредственный обмен данными между процессором и памятью.

demand staging [dɪ'ma:nd 'steɪdʒɪŋ] перемещение по запросу.@ Перемещение данных в иерархической памяти по запросу программы.

denial [dɪ'naɪəl] *n.* 1. отрицание; 2. опровержение.# **flat denial** категорическое опровержение; 3. отказ.# **to take no denial** не принимать отказа.

denial of service [dɪ'naɪəl əv 'sɜ:vɪs] отказ в обслуживании.@ Разновидность угрозы, направленной на разрушение защиты данных в вычислительной системе.

dense [dens] *adj.* плотный, неразрезанный, густой.@ **dense of knapsack** неразрезанный вектор ранца.

dense index [dens 'ɪndeks] плотный индекс.@ Вторичный индекс, содержащий ссылки на все индексируемые элементы.

denseness ['densnɪs] *n.* плотность

density ['densɪti] *n.* плотность, концентрация.@ **density of knapsack** плотность вектора ранца.

deny [dɪ'naɪ] *v.* 1. отрицать; 2. отказываться(ся), отказать.# **to be denied** не обладать, быть лишенным чего-л.@ **deny access** отказать в доступе.

department "62" = Federal Information Security Agency (FISA)

department [dɪ'pa:tment] *n.* 1. управление; 2. министерство; 3. отделение.@ **department "8200"** "Отделение 8200" (подразделение израильской разведывательной организации "Моссад", занимающееся перехватом и дешифрованием сообщений).@ **department of Defense (DOD)** министерство обороны (USA).

depend [dɪ'pend] *v.* 1. зависеть от (**on, upon**); 2. полагаться на (**on, upon**).# **depending on (upon)** в зависимости от.

dependence [dɪ'pendəns] *n.* зависимость.

depth [depθ] *n.* 1. глубина.@ 1. Глубина узла в дереве представляет собой длину естественного пути из корневого узла. 2. Глубина дерева определяется как максимальная глубина узлов этого дерева. 2. глубина, толщина; 3. мощность.

depth sorting [depθ 'sɔ:tɪŋ] упорядочение по глубине.@ Способ удаления невидимых поверхностей, при котором компоненты изображаемого объекта рисуются в порядке приближения к точке наблюдения, начиная от более даль-

них. При этом изображения близких компонентов перекрывают изображения дальних.

depth-balanced [depθ'bælənsɪd] сбалансированный по глубине.@ **depth-balanced tree** сбалансированное дерево.

depth-first search ['depθ'fə:st sə:tʃ] поиск в глубину, перебор в глубину.@ Способ обхода дерева поиска, при котором сначала анализируется поддерево, начинающееся в данной вершине, а затем – непроанализированные вершины того же уровня.

derive [di'raɪv] *v.* 1. происходить от; устанавливать происхождение; 2. получать; извлекать; 3. выводить; ответвлять.@ **derive a key** устанавливать (получать) ключ.# **to derive benefit** извлекать пользу.

derived [di'raɪvt] *adj.* производный.@ **derived key** производный ключ (полученный преобразованием другого ключа).@ **derived field** производное поле, производный элемент данных.@ **derived row** производное правило.

derived data item [di'raɪvt 'deɪtə 'aɪtəm] производный элемент данных.@ В сетевых базах данных – элемент данных, значение которого является копией или заданной функцией значения другого элемента данных.

derived type [di'raɪvt taɪp] производный тип.@ Тип данных, определенный через другие (базовые или производные) типы.

DES(Data Encryption Standard)-алгоритм.@ Итеративный 16-цикловой обратимый блочный шифр Фейстеля. Размер входного блока – 64 бита. Размер ключа k шифра – 56 бит. Цикловые ключи $q_1, \dots, q_{16}$ есть алгоритмически выбираемые выборки 48 бит из 56 бит ключа k .@ **DES chip** микросхема, реализующая DES-алгоритм.@ **DES Cracker** "DES-крэкер" (специализированный вычислитель, предназначенный для взлома DES-алгоритма).@ **DES implementation** реализация DES-алгоритма.@ **DES protection** криптографическая защита с помощью DES-алгоритма.@ **DES translation** перешифрование по DES-алгоритму (расшифрование текста, зашифрованного с помощью какой-то криптосистемы, и повторное его шифрование посредством DES-алгоритма).@ **DES-based authentication** аутентификация на основе DES-алгоритма.@ **DES-encrypted message** сообщение, зашифрованное по DES-алгоритму.@ **DES-key** DES-ключ (ключ для DES-алгоритма).@ **DES-like** подобный DES-алгоритму.

descramble [di:'skræmbl] *v.* дескремблировать.

descrambled [di:'skræmblt] *adj.* дескремблированный.

descrambler (DSCR) [di:'skræmblə] *n.* дескремблер @ Устройство, предназначенное для восстановления исходной структуры цифрового сигнала электросвязи, преобразованного скремблером.

descrambling [di:'skræmblɪŋ] *n.* дескремблирование.@ **descrambling key** ключ дескремблирования.

desensitized [di:'sensɪtaɪzd] *adj.* децентрализованный.@ **desensitized authentication** децентрализованная аутентификация.

design [di'zain] *v.* 1. разрабатывать, проектировать; 2. предназначать; *n.* 1. проект; план; конструкция; разработка; расчет; 2. эскиз, рисунок.@ **design automation (DA)** автоматизация проектирования, автоматизация программи-

рования. @ **design ciphers** разрабатывать шифры. @ **design data** расчетные (исходные) данные. @ **design error failure** конструктивный отказ. @ **design of experiments** планирование экспериментов. @ **design review** обсуждение проекта.

designate ['dɛzɪneɪt] *v.* обозначать.

designated ['dɛzɪneɪtɪd] *adj.* назначенный. @ **designated confirmer signature** цифровая подпись с назначенным конфирмантом.

designation ['dɛzɪneɪʃən] *n.* обозначение.

designer [dɪ'zainə] *n.* конструктор; проектировщик; разработчик. @ **designer of a cryptosystem** разработчик криптосистемы.

destination [ˌdestɪ'neɪʃən] *n.* 1. адресат, пункт назначения; получатель. @ Узел сети, к которому адресовано сообщение. 2. место назначения. @ Область или ячейка памяти, в которую пересылаются данные. @ **destination address** адрес получателя. @ **destination address bus** шина адреса получателя. @ **destination code** адрес (назначения). @ **destination cryptor** шифратор получателя (сообщения). @ **destination file** выходной файл. @ **destination key** ключ получателя (сообщения). @ **destination station** адресат, пункт назначения.

destination field [ˌdestɪ'neɪʃən fɪːld] поле адреса. @ Часть заголовка сообщения, в котором помещается адрес назначения.

destinee *n.* = **destination**

detail ['diːteɪl] *n.* подробность; деталь; *v.* детально разбирать, рассматривать. # **to detail** подробно. # **in considerable detail** очень подробно. # **in full detail** во всех деталях. # **in some detail** довольно подробно. # **to go (enter) into details** вдаваться в подробности.

de-tapper [diː'tæpə] *n.* прибор для обнаружения несанкционированных подключений к линии связи.

detectable *adj.* поддающийся обнаружению.

detectable [dɪ'tektəɪbl] *adj.* обнаруживаемый; поддающийся обнаружению. @ **detectable wiretap** поддающийся обнаружению перехват с подключением к проводной линии связи.

detectable element [dɪ'tektəɪbl 'elɪmənt] обнаруживаемый элемент. @ В машинной графике — элемент отображения, который может быть выделен указкой.

detector [dɪ'tektə] *n.* критерий, детектор.

determination [dɪ'təːrmi'neɪʃən] *n.* определение. @ **determination of the cipher system used** определение используемой шифрсистемы.

determine [dɪ'təːrmin] *v.* 1. определять; 2. решать. @ **determine a key** определять ключ. @ **determine the period of a sequence** определять период последовательности.

deterministic [dɪ'təːrminɪstɪk] *adj.* детерминированный, детерминистский. @ Детерминированным может быть процесс, метод и т. д., исход реализации которого полностью определяется значениями входных переменных и начальным состоянием системы. @ **deterministic encryption** детерминированное шифрование (каждому открытому тексту сообщения ставится в соответст-

вие ровно один шифрованный текст, полученный после применения криптосистемы с указанным ключом.).@ **deterministic key generation** детерминированная генерация ключей.@ **deterministic key** детерминированный ключ.

deterministic language [di'tə:rnɪstɪk 'læŋgwɪdʒ] детерминированный язык.@ Любой бесконтекстный язык, распознаваемый детерминированным автоматом с магазинной памятью.

development [di'veləpmənt] *n.* 1. развитие; 2. усовершенствование; 3. подготовительные работы; разработка; 4. проектно-конструкторские работы; 5. достижение; 6. вывод, заключение; 7. *обычно pl.* события; явления.# **under development** развиваемый, разрабатываемый.@ **development Center for Embedded COMSEC Products** Центр разработки встраиваемых устройств безопасности связи (USA).@ **development system** система разработки программ.

device (dev) [di'vaɪs] *n.* 1. внешнее устройство. 2. устройство, прибор, механизм, приспособление, аппарат, элемент; 3. прием, способ.@ **device key** ключ (криптографического) устройства (прибора).@ **device allocation** распределение устройств.@ **device control unit** контроллер (внешнего) устройства.@ **device under test (DUT)** испытываемый прибор.

device adapter [di'vaɪs ə'dæptə] адаптер (внешнего) устройства.@ Устройство сопряжения ЭВМ и внешнего устройства.

device control (DC) [di'vaɪs kən'troul] символ управления устройством.@ Управляющий символ, зарезервированный для задания команд, специфических для конкретных устройств. В коде ASCII для этого выделены коды 17, 18, 19 и 20.

device controller [di'vaɪs kən'troulə] контроллер (внешнего) устройства.@ Устройство сопряжения ЭВМ с внешним устройством и управление обменом. Между понятием «адаптер» и «контроллер» отсутствует четкая грань: «адаптер» подразумевает, в первую очередь, преобразование представления и скорости передачи информации, «контроллер» обычно выполняет более сложные функции управления устройством.

device coordinates [di'vaɪs kou'ɔ:dnɪts] координаты устройства.@ В машинной графике - задание положения элементов изображения в координатной сетке конкретного устройства.

device driver [di'vaɪs 'draɪvə] драйвер устройства.@ Программа, обеспечивающая взаимодействие операционной системы с физическим устройством. Драйвер обрабатывает прерывание обслуживаемого устройства, поддерживает очередь запросов и преобразует запросы в команды управления устройством.

device name [di'vaɪs neɪm] имя устройства.@ 1. Символ или последовательность символов, идентифицирующих внешнее устройство для операционной системы. 2. Часть имени файла, указывающая устройство, на котором он расположен.

device number [di'vais 'nʌmbə] номер устройства.@ Числовой код, идентифицирующий внешнее устройство в группе однородных устройств, управляемых одним драйвером или одним контроллером.

device space [di'vais speɪs] пространство устройства.@ В машинной графике - множество адресуемых точек устройства отображения.

device status word (DSW) [di'vais 'steɪtəs wə:d] слово состояния устройства.@ Программно-доступный регистр, разряды которого описывают состояние внешнего устройства или нескольких внешних устройств.

device-dependent [di'vais,di'pendənt] зависящий от устройств, привязанный к устройствам.@ О программе, операции или представлении данных, использующих особенности конкретных физических устройств или обращающихся к ним в обход файловой системы.

deviceindependence [di'vais,ɪndɪ'pendəns] *n.* независимость от (внешних) устройств.

device-independent [di'vais,ɪndɪ'pendənt] не зависящий от (внешних) устройств.@ 1. О программе, сохраняющей функциональные характеристики вне зависимости от внешних устройств, на которых располагаются обрабатываемые ею данные. 2. В машинной графике — о средствах или преобразованиях, применение которых не зависит от используемых устройств изображения.

devise [di'vaɪz] *v.* изобретать; разрабатывать.@ **devise a cryptosystem** разрабатывать криптосистему.

devote [di'vəʊt] *v.* посвящать; уделять.# **to be devoted** увлекаться чем-л.; быть преданным.

diamond ['daɪəmənd] *n.* 1. ромб; 2. алмаз.@ **Diamond Encryption Algorithm (DEA)** Ромбовый алгоритм шифрования.

dictionary ['dɪkʃənri] *n.* словарь.@ **dictionary attack** "словарная" атака (вскрытие ключа путем перебора словарного справочника, составленного из наиболее часто используемых на практике ключей — имен, фамилий, инициалов, номеров телефонов и т.д.).@ **dictionary computer** "словарный" компьютер (предназначен для отбора сообщений, в которых присутствуют заданные ключевые слова).@ **dictionary program** "словарная" программа (предназначена для отбора сообщений, в которых присутствуют заданные ключевые слова и фразы).@ **dictionary secure** защищенный от "словарной" атаки.

difference ['dɪfrəns] *n.* 1. разница, различие, разность; 2. расхождение, разногласие; 3. приращение.@ **differences in plaintext pairs** попарные различия и открытых текстах.# **it makes all the difference (in the word)** это существенно меняет дело; это очень важно.# **it makes no difference** нет никакой разницы; это не имеет значения.

differential [ˌdɪfə'renʃəl] *n.* дифференциал, разность, перепад; *adj.* 1. дифференциальный; 2. отличительный.@ **differential attack** дифференциальная атака.@ **differential control** дифференциальное управление.@ **differential cryptanalysis** дифференциальный криптоанализ.@ **differential equation** дифференциальное уравнение.@ **differential neighbourhood** бесконечно малая ок-

рестность. @ **differential operator** оператор дифференцирования. @ **differential parameter** дифференциальный параметр. @ **differential phase-shift keying (DPSK)** дифференциальная фазовая манипуляция. @ **differential pulse-code modulation (DPCM)** дифференциальная импульсно-кодовая манипуляция. @ **differential sing** 1. знак дифференциала; 2. дифференциальный признак; 3. отличительный признак. @ **differential synthesis algorithm (DSA)** алгоритм дифференциального синтеза. @ **differential techniques** методы дифференциального криптоанализа. @ **differential-linear attack** линейно-дифференциальная атака. @ **differential-resistant function** дифференциально стойкая функция (стойкая против дифференциального криптоанализа).

differential file (dif) [ˈdɪfərənsjəl faɪl] файл различий; файл изменений. @ Файл, содержащий записи, которыми различаются два сравниваемых файла или две версии одного файла.

difficulty [ˈdɪfɪkəlti] *n.* сложность. @ **difficulty of factoring** сложность разложения на множители.

Diffie-Hellman (D-H) = Diffie-Hellman key exchange algorithm

Diffie-Hellman exponent показатель экспоненты в алгоритме обмена ключами Диффи-Хеллмана.

Diffie-Hellman key exchange algorithm алгоритм обмена ключами Диффи-Хеллмана.

Diffie-Hellman one-way function односторонняя функция Диффи-Хеллмана.

diffusion [dɪˈfjuːʒən] *n.* 1. рассеивание, диффузия (распространение влияния одного знака открытого текста на множество знаков шифртекста); 2. размывание (преобразование) открытого текста для изменения его статистических свойств.

digest [ˈdaɪdʒest] *n.* 1. сжатие; 2. сборник (материалов); резюме; обзорная статья. @ **digest of a message** резюме сообщения.

digest [ˈdɪdʒest] *v.* 1. переваривать(ся); 2. усваивать; 3. обрабатывать

digital [ˈdɪdʒɪtl] *adj.* цифровой; численный, дискретный. @ **digital adder** цифровой сумматор. @ **digital analog decoder** цифро-аналоговый преобразователь. @ **digital approximation** цифровое приближение. @ **digital automation** цифровая автоматика. @ **digital calculations** цифровые вычисления. @ **digital cash** цифровая наличность. @ **digital cassette** «цифровая кассета». @ **digital character** цифра. @ **digital communication (digicom)** цифровая связь. @ **digital computation** вычисление в цифровой форме. @ **digital computing circuit** цифровая вычислительная машина. @ **digital control oscillator (DCO)** генератор с цифровым управлением. @ **digital control system** цифровая система управления (регулирования). @ **digital coordinate(s)** координаты в цифровой форме. @ **digital data receiver (DDR)** приемник цифровых данных. @ **digital data transmitter (DDT)** устройство передачи цифровых данных. @ **digital data** цифровые (дискретные) данные. @ **digital device** цифровое устройство (элемент). @ **digital differential analyzer (DDA)** цифровой дифференциальный анализатор. @ **digital disk** цифровой диск. @ **digital display (DD)** 1. цифровой индикатор; 2.

цифровая индикация. @ **digital divider** цифровой делитель. @ **digital drum** цифровой барабан. @ **digital encryption algorithm** алгоритм цифрового шифрования. @ **digital form** цифровая (дискретная) форма. @ **digital indicator** цифровой индикатор. @ **digital information display (DID)** индикатор цифровой информации. @ **digital information** цифровая (дискретная) информация. @ **digital input module (DIM)** модуль цифрового ввода. @ **digital key** цифровой ключ. @ **digital machine** цифровая вычислительная машина. @ **digital matched filter (DMF)** цифровой согласованный фильтр. @ **digital microcircuit (DMC)** цифровая интегральная схема. @ **digital microprocessor-based oscilloscope (DMO)** цифровой микропроцессорный осциллограф. @ **digital module** цифровой модуль. @ **digital multimeter (DMM)** цифровой универсальный измерительный прибор. @ **digital multiplexed interface (DMI)** цифровой мультиплексный интерфейс. @ **digital multiplier** цифровое множительное устройство, цифровой умножитель. @ **digital network analyzer (dina)** цифровой схемный анализатор. @ **digital output** 1. цифровое устройство вывода данных; 2. цифровые выходные данные. @ **digital output module (DOM)** модуль цифрового вывода. @ **digital panel meter (DPM)** цифровой стендовый измерительный прибор. @ **digital phase locked loop (DPLL)** цифровая система фазовой автоподстройки частоты. @ **digital process** дискретный (цифровой) процесс. @ **digital processing unit** цифровое устройство обработки данных. @ **digital quantity** цифровая величина. @ **digital representation** цифровое представление. @ **digital signal processing (DSP)** цифровая обработка сигналов. @ **digital signal** цифровой сигнал. @ **digital Signature Algorithm (DSA)** Алгоритм цифровой подписи. @ **digital Signature Standard (DSS)** Стандарт цифровой подписи (USA). @ **digital signature (DSG)** цифровая подпись. @ **digital sorting** цифровая сортировка. @ **digital storage unit (DSU)** цифровое ЗУ. @ **digital storage** цифровое запоминающее устройство. @ **digital switching system (DSS)** цифровая система коммутации. @ **digital system desing language (DDL)** язык проектирования цифровых систем. @ **digital technique** цифровая техника. @ **digital timestamp** цифровая отметка времени. @ **digital variable** переменная в цифровой форме, дискретная форма. @ **digital video recording (DVR)** цифровая видеозапись. @ **digital voltmeter (DVM)** цифровой вольтметр. @ **digital wire** разрядный провод в запоминающем устройстве с прямой выборкой. @ **digital-coded information** цифровая информация. @ **digital-operational multiplier** цифровое операционное множительное устройство, цифровой операционный умножитель. @ **digital-to-analog(ue) (D-A, D/A)** цифро-аналоговый. @ **digital-to-analog(ue) conversion (DAC)** цифро-аналоговое преобразование. @ **digital-to-analog(ue) converter (DAC)** цифро-аналоговый преобразователь. @ **digital-to-synchro converter (DAC)** преобразователь цифровой код – угол поворота вала сельсина. @ **digital-to-voice translation (DIVOT)** преобразователь цифрового кода в речевой сигнал.

digital desing language ['dɪdʒɪtl dɪ'zain 'læŋɡwɪdʒ] язык цифрового проектирования. @ Язык высокого уровня, называемый языком межрегистровых пере-

сылок, используемый для облегчения описания и преобразования цифровых систем, а также их межсоединений.

digital filtering ['dɪdʒɪtl 'fɪltərɪŋ] цифровая фильтрация.@ Фильтрация сигналов на основе методов их цифровой обработки.

digital logic ['dɪdʒɪtl 'lɒdʒɪk] дискретная логика.@ Методологическая основа обработки выражений и таблиц состояний, содержащих дискретные переменные (синоним булевой алгебры).

digital system ['dɪdʒɪtl 'sɪstɪm] цифровая система.@ Любая система, оперирующая с цифровыми (дискретными) сигналами.

digraph *n.* = **bigram**

digraphic ['daɪgra:fɪk] *adj.* биграммный (двухбуквенный).@ **digraphic characteristics** биграммные характеристики.@ **digraphic coincidence test** тест на совпадение биграмм.@ **digraphic frequency counts** подсчет встречаемости биграмм (в тексте), биграммная маркировка (текста).@ **digraphic Phi test** биграммный ф-тест.@ **digraphic substitution** биграммная замена (с одновременной обработкой сразу двух знаков).

dimension [dɪ'dɪmɪnʃən] *n.* 1. размерность, размерность (векторного пространства).@ 1. Число индексов, определяющих элемент массива. 2. Диапазон значений индекса массива; для вектора – число элементов. 2. *pl.* размеры, величина, объем; 3. размерные линии.

dimensional [dɪ'dɪmɪnʃənl] *adj.* размерный.

dimensionally [dɪ'dɪmɪnʃənlɪ] *n.* размерность.

dimensionless [dɪ'dɪmɪnʃənləs] *adj.* безразмерный.

dinome [dɪ'noʊm] *n.* пара цифр, две цифры.

dinomic [dɪ'noʊmɪk] *adj.* двухцифровой; *n.* двухцифровая шифрсистема.@ **dinomic cipher system with variants** вариантная двухцифровая шифрсистема (при шифровании каждый символ открытого текста может заменяться на разные пары цифр).@ **dinomic cipher system** двухцифровая шифрсистема (при зашифровании каждый символ открытого текста заменяется на две цифры).

diplomatic (D) [dɪplə'mætɪk] *adj.* дипломатический.@ **diplomatic cipher** дипломатический шифр.

direct [dɪ'rekt] *v.* направлять; *adj.* 1. прямой; 2. непосредственный, прямой; 3. постоянный.@ **direct allocation** 1. жесткое (фиксированное) распределение для данной программы; 2. статическое распределение.@ **direct coding** программирование на языке машины.@ **direct consequence** прямая последовательность.@ **direct coupling (DC)** непосредственная связь.@ **direct data capture** сбор данных под (непосредственным) управлением ЭВМ.@ **direct data entry (DDE)** прямой ввод данных.@ **direct data set** прямой набор данных, набор данных прямого доступа.@ **direct digital control (DDC)** прямое цифровое управление.@ **direct display** дисплей для непосредственного отображения данных (*напр. содержимого памяти*).@ **direct eavesdropping** прямой перехват (путем непосредственного подключения к линии связи).@ **direct electronic Fourier transform** прямое электронное преобразование Фурье.@ **direct en-**

ryption непосредственное шифрование, (аппаратными средствами).@ **direct inserted subroutine** открытая подпрограмма.@ **direct interpolation** прямая интерполяция.@ **direct inward dialing (DID)** автоматическое установление входящего соединения.@ **direct memory access controller (DMAC)** контроллер прямого доступа к памяти (ЗУ).@ **direct numerical control (DNC)** централизованное управление от ЭВМ.@ **direct outward dialing (DOD)** автоматическое установление исходящего соединения.@ **direct product** прямое произведение (произведение групп).@ **direct read after write (DRAW)** считывание сразу после записи.@ **direct row** прямое правило.@ **direct standard cipher alphabet** прямой стандартный шифр алфавит.@ **direct storage allocation** распределение динамической памяти.@ **direct symmetry method technique** метод прямой симметрии (применяется для вскрытия шифров периодической многоалфавитной замены).

direct search = brute-force attack

direct address [di'rekt ə'dres] прямой адрес.@ Адрес в машинной команде, указывающий на ячейку, где находится операнд, т.е. не требующий преобразований для получения исполнительного адреса.

direct addressing [di'rekt ə'dresɪŋ] прямая адресация.@ Способ адресации, при которой исполнительный адрес равен адресу, указанному в команде.

direct execution [di'rekt ,eksɪ'kju:ʃən] немедленное выполнение.@ Выполнение команды непосредственно после ее ввода.

direct file [di'rekt faɪl] файл прямого доступа.@ Файл, к записям которого можно обращаться в любом порядке; для доступа к записи указывается ее номер или логический адрес.

direct memory access (DMA) [di'rekt 'meməri 'ækses] прямой доступ в память, ПДП.@ Способ быстросействующего подключения внешнего устройства, при котором оно обращается к оперативной памяти, не прерывая работы процессора.

direct-access file [di'rekt'ækses faɪl] файл прямого доступа.@ **direct-access library** библиотека с непосредственными (прямыми) доступами.@ **direct-access storage** запоминающее устройство с непосредственной выборкой.

direct access [di'rekt 'ækses] прямой доступ.@ Способ доступа, при котором все элементы данных (слова, записи, блоки) равнодоступны и для доступа к указанному элементу данных не требуется просмотра других элементов данных.

direct-access hashing [di'rekt'ækses hæʃɪŋ] прямое хеширование. @ Способ хеширования, при котором функция расстановки выдает различные значения для различных входных данных.

direct-access method (DAM) [di'rekt'ækses 'meθəd] прямой метод доступа.@ Метод доступа, при котором запись идентифицируется номером записи внутри файла или физическим адресом на устройстве.

direct-access storage device (DASD) [di'rekt'ækses 'stɔ:rɪdʒ dɪ'vaɪs] запоминающее устройство прямого доступа, ЗУПД.@ Запоминающее устройство, по-

звляющее эффективно организовать прямой доступ. Время доступа к элементам ЗУПД практически не зависит от их расположения. Как правило, подразумеваются запоминающие устройства на магнитных дисках.

directed [dɪ'rektɪd] *adj.* направленный.@ **directed key search** направленный поиск ключа.@ **directed random search algorithm** алгоритм направленного случайного поиска.

director [dɪ'rektə] *n.* директор.@ **director of NSA (DIRNSA)** директор NSA.

directorate *n.* = **department**

directory [dɪ'rektəri] *n.* справочник.

disavow communications отказываться от сообщения.

disavow ['dɪsə'vau] *n.* отказываться.@ **disavow communications** отказываться от сообщений.

discard [dɪ'ska:d] *v.* 1. отбрасывать; 2. отвергать; отказываться; переставать пользоваться, прекращать использовать.@ **discard a key** переставать пользоваться ключом (прекращать использовать ключ).

discern [dɪ'sɜ:n] *v.* 1. различать, замечать; 2. отличать, проводить различие.# **to discern no difference** не видеть разницы.

disclosure [dɪs'klɒʃə] *n.* раскрытие, разглашение (секретных сведений).@ **disclosure of sensitive information** раскрытие (разглашение) секретной информации.

discover [dɪs'klʌvə] *v.* 1. обнаруживать, узнавать; 2. открывать, делать открытия; раскрывать.@ **discover a key** раскрывать ключ.

discoverable [dɪs'klʌvəbl] *adj.* раскрываемый.@ **discoverable key** раскрываемый ключ.

discrete [dɪs'kri:t] *adj.* раздельный; отдельный; дискретный.@ **discrete channel with memory (DCM)** дискретный канал с памятью.@ **discrete component** дискретный компонент (элемент).@ **discrete exponential cryptosystem** криптосистема на основе дискретного возведения в степень.@ **discrete exponential function** функция дискретного возведения в степень.@ **discrete Fourier transform (DFT)** дискретное преобразование Фурье.@ **discrete logarithm problem (DLP)** задача вычисления дискретного логарифма.@ **discrete logarithm (DL)** дискретный логарифм.@ **discrete memoryless channel (DMC)** дискретный канал без памяти.@ **discrete process** дискретный процесс.@ **discrete programming** дискретное программирование.@ **discrete representation** дискретное представление.@ **discrete time** дискретное время.@ **discrete variable representation** дискретное представление переменных величин.

discrete and components system [dɪs'kri:t ænd kəm'pounənts 'sɪstɪm] дискретные и аналоговые системы. @ Системы, в которых регистрируемые, передаваемые и отображаемые сигналы могут представлять данные соответственно в дискретном виде (т. е. как целые числа) и в аналоговом виде (т. е. как «действительные» числа).

discrete range [dis'kri:t reɪndʒ] дискретный диапазон.@ Отрезок упорядоченного дискретного множества.

discrete simulation [dis'kri:t ˌsɪmjʊ'leɪʃən] дискретное моделирование.@ Моделирование, при котором исследуемый процесс представляется дискретной последовательностью событий.

discrete structure [dis'kri:t 'strʌktʃə] дискретная структура.@ Множество дискретных элементов, на котором определен некоторый набор операций. Термин «дискретный» означает отсутствие непрерывности, поэтому к дискретным множествам следует относить конечные множества и счетные множества, в то же время несчетные множества, такие как множества действительных чисел не являются дискретными.

discretion [dis'kreʃən] *n.* 1. свобода действий, усмотрение; 2. благоразумие; осторожность.# **at the discretion of** на усмотрение кого-л.

discuss [dis'kʌs] *v.* обсуждать, рассматривать.# **under discussion** обсуждаемый, рассматриваемый.

disjunction [dis'ɔʃŋkʃən] *n.* дизъюнкция, логическое сложение.

disjunctive [dis'ɔʃŋktɪv] *adj.* дизъюнктивный.@ **disjunctive normal form (DNF)** дизъюнктивная нормальная форма.

disjunctive search [dis'ɔʃŋktɪv sə:tʃ] дизъюнктивный поиск.@ Поиск данных, удовлетворяющих по крайней мере одному из указанных критериев.

dispatch [dis'pætʃ] *n.* донесение, депеша.@ **dispatch in cipher** шифрованное донесение.

dispel [dis'pel] *v.* разгонять; рассеивать.# **to dispel doubts** рассеять сомнения

dispense [dis'pens] *v.* 1. распределять; 2. обходиться без чего-л. (**with**); 3. освобождать от чего-л. (**from**).@ **dispense keys** распределять ключи.

disperse array [dis'pə:s ə'reɪ] разреженный массив; разреженная матрица.@ Массив (обычно матрица), большинство элементов которого равно нулю. Для экономного хранения и обработки таких массивов необходимы специальные способы их представления.

disperse matrix [dis'pə:s 'meɪtrɪks] разреженная матрица.

dispersion *n.* [dis'pə:ʃən] дисперсия.@ **dispersion area** область разброса данных.

displace [dis'pleɪs] *v.* смещать; переставлять, перекладывать.@ **displace a cryptogram by two positions to the left** передвинуть (сдвинуть) криптограмму на две позиции влево.

disposal [dis'prouzəl] *n.* 1. расположение, размещение; 2. передача; 3. избавление, устранение.# **at one's disposal** в чьем-л. расположении.

dispose [dis'prouz] *v.* 1. освободить (*блок динамически распределяемой памяти*); 2. располагать; размещать; 3. распределять; 4. избавиться от чего-л.; удалить, уничтожить, устранить (**of**).@ **dispose of keys** уничтожать ключи.# **to dispose of some problems** разрешить некоторые проблемы.

dissemination [dɪ'semɪneɪʃən] *n.* распространение (рассылка радиоразведывательной информации заинтересованным лицам и ведомствам).

distinguish [dɪs'tɪŋɡwɪʃ] *v.* 1. различать; проводить различие (**between**); 2. отличать. # **to distinguish oneself by** отличиться, прославиться.

distinguished [dɪs'tɪŋɡwɪʃt] *adj.* выдающийся, известный. # **as distinguished from** в отличие от. # **to be distinguished from** в отличие от.

distort [dɪs'tɔ:t] *v.* искажать.

distorted [dɪs'tɔ:tɪd] *adj.* искаженный. @ **distorted information** искаженная информация, искажаемая информация. @ **distorted message** искаженное сообщение.

distribute [dɪs'trɪbjʊ:t] *v.* распределять, распространять, квалифицировать, доставлять. @ **distribute keys** распределять ключи.

distributed [dɪs'trɪbjʊ:tɪd] *adj.* распределенный. @ **distributed constant** распределенные параметры. @ **distributed feedback (DFB)** [dɪs'trɪbjʊ:tɪd 'fi:d.bæk] распределенная обратная связь. @ **distributed key generation** распределенная генерация ключей. @ **distributed key infrastructure** распределенная инфраструктура ключей. @ **distributed key management** распределенное управление ключами. @ **distributed system security architecture (DSSA)** архитектура безопасности распределенных систем (разработанная в 1986 г. криптосистема американской фирмы "DEC", использующая две схемы шифрования: (а) симметричную для обеспечения конфиденциальности и целостности данных; (б) асимметричную для аутентификации и распределения ключей).

distributed processing [dɪs'trɪbjʊ:tɪd 'prəʊsesɪŋ] распределенная обработка. @ Обработка задания посредством нескольких процессов, выполняющихся на различных узлах распределенной системы и обменивающихся информацией по сети передачи данных.

distributed array processor [dɪs'trɪbjʊ:tɪd ə'reɪ 'prəʊsesə] распределенный векторный процессор. @ ЭВМ, с каждым элементом памяти которой связан процессор, выполняющий операции над ним.

distributed data base [dɪs'trɪbjʊ:tɪd 'deɪtə beɪs] распределенная база данных. @ База данных, данные которой физически расположены на различных носителях или в различных узлах сети.

distributed file system [dɪs'trɪbjʊ:tɪd faɪl 'sɪstɪm] распределенная файловая система. @ Файловая система, в которой файлы, расположенные на других узлах распределенной вычислительной системы (сети) доступны программе точно так же, как файлы ЭВМ, на которой она выполняется.

distributed intelligence [dɪs'trɪbjʊ:tɪd ɪn'telɪdʒəns] распределенное управление; распределенные вычислительные средства. @ Организация распределенной системы, при которой управление осуществляется группой программ, выполняющихся на различных узлах системы.

distributed logic [dɪs'trɪbjʊ:tɪd 'lɒdʒɪk] распределенное управление. @ Вычислительная или управляющая системы, имеющие несколько процессоров, управляющих их различными частями.

distributed system (DS) [dis'tribju:tɪd 'sɪstɪm] 1. распределенная (вычислительная) система. @ Вычислительная система, состоящая из нескольких взаимосвязанных ЭВМ, работающих независимо и выполняющих общее задание. 2. система с распределенными параметрами.

distribution [dis'tribju:ʃən] *n.* 1. распределение, распространение, доставка; 2. (вероятностное) распределение. @ **distribution key** ключ для распределения других ключей. @ **distribution of keys** распределение ключей. @ **distribution curve** кривая распределения. @ **distribution function** функция распределения вероятностей. @ **distribution of eigenvalues** распределение собственных значений. @ **distribution of zeros** распределение нулей. @ **distribution system** распределительная система.

distribution counting sort [dis'tribju:ʃən 'kauntɪŋ sɔ:t] сортировка с подсчетом и распределением. @ Алгоритм сортировки, согласно которому для каждого значения сортировочного ключа отбираются все записи, обладающие этим ключом. При этом предполагается, что у нескольких записей может быть один и тот же ключ.

distribution kit [dis'tribju:ʃən kɪt] дистрибутивный комплект, дистрибутив. @ Программное изделие в виде, поставляемом изготовителем.

disuse ['dis'ju:s] *n.* неупотребление. # **to come (fall) in to disuse** выйти из употребления.

divide [dɪ'vaɪd] *v.* 1. делить(ся); 2. разветвлять; 3. измельчать.

divide-and-conquer [dɪ'vaɪd ænd 'kɒŋkə] *v.* разделяй и властвуй. @ **divide-and-conquer attack** криптоанализ методом "разделяй и властвуй". @ **divide-by-two circuit** схема деления на два.

divide and conquer sorting [dɪ'vaɪd ænd 'kɒŋkə 'sɔ:tɪŋ] сортировка по принципу «разделяй и властвуй». @ Алгоритм сортировки, аналогичный поразрядной сортировки, но отличающийся тем, что в нем обработка начинается со старшего значащего разряда ключа сортировки и оканчивается младшим.

divide stop light [dɪ'vaɪd stɒp 'laɪt] индикатор остановки при делении. @ Останов в случае выхода результата из разрядной сетки.

do [du:] *v.* (**did**, **done**) 1. делать; 2. подходить (годиться); 3. в утвердительном предложении употребляется для усиления последующего смыслового глагола и переводится как «все же», «действительно»; 4. употребляется для замены какого-л. глагола (вместо повторения); 5. избавляться от (**away with**); 6. обходиться без (**without**). @ **do cryptanalysis** заниматься криптоанализом. # **as it does (as they do)** фактически, в действительности. # **in doing so** при этом. # **to do away (with)** избавляться (от). # **to do one's best** делать все возможное. # **to do without** обходиться без. # **to have to do with** иметь дело с, иметь отношение к. # **to have much to do with** иметь много общего с. # **to have nothing to do with** не иметь ничего общего с.

doctored ['dɒktəd] *adj.* фальсифицированный, поддельный. @ **doctored message** фальсифицированное (поддельное) сообщение.

DOD 520028-STD стандарт (USA) для оценки уровня защищенности вычислительных систем (установлен директивой МО USA № 520028-STD и определяет 4 иерархических класса защищенности вычислительных систем, разрабатываемых и используемых в интересах американского правительства).

DOD Computer Security Center Центр защиты компьютеров МО (USA).

dot *adj.* = **scalar**

dot [dɒt] *n.* точка. @ **dot cipher** точечный шифр (в виде точек на сетке формата).

double ['dʌblə] *adj.* двойной; раздвоенный; *v.* удваивать. @ **double calculation** вычисление с двойным просчетом, двойной просчет. @ **double carry** двойной перенос. @ **double density recording** запись с удвоенной плотностью. @ **double encryption** двойное шифрование. @ **double frequency-shift keying (DFSK)** двойная частотная манипуляция. @ **double integral** двойной интеграл. @ **double key** двойной ключ. @ **double length arithmetic** арифметические операции со словами удвоенной длины. @ **double length operation** операция с числами двойной длины. @ **double length word** слово двойной длины, слово с двойным количеством разрядов. @ **double length** двойная длина. @ **double negation** двойное отрицание. @ **double precision arithmetic** 1. арифметика с двойной точностью; 2. арифметическое устройство для работы с удвоенной точностью. @ **double precision computation** вычисление с удвоенной точностью. @ **double precision hardware** 1. аппаратура с удвоенным количеством разрядов; 2. аппаратура для вычисления с удвоенной точностью. @ **double sampling** двойная выборка, двукратный отбор проб. @ **double space** двойной пробел, двойной интервал. @ **double substitution cipher** шифр двойной замены. @ **double transposition cipher** шифр двойной перестановки. @ **double word** двойное слово. @ **double word-length arithmetic** 1. арифметические операции со словами двойной длины; 2. арифметическое устройство для работы со словами двойной длины. @ **double-** в сложных и сложносоставных словах имеет значение дважды-, двух-.

double buffering ['dʌbl 'bʌfərɪŋ] двойная буферизация. @ Разновидность метода буферизации, в котором используется два буфера.

double complement ['dʌbl 'kɒmplɪmənt] двойное дополнение. @ В логике двойное дополнение означает двойное отрицание элемента.

double precision ['dʌbl prɪ'sɪʒən] удвоенная точность, двойная точность. @ Метод представления чисел, требующий вдвое больше разрядов, чем обычно. Операции над числами с двойной точностью называются арифметикой двойной точности либо арифметикой над словами двойной длины.

double precision number ['dʌbl prɪ'sɪʒən 'nʌmbə] число с двойной точностью. @ Число, для представления которого используются два машинных слова (обычно 64 бита).

double-address instruction ['dʌblə'dres ɪn'strʌkʃən] двухадресная команда. @ Машинная команда, содержащая адреса двух операндов, один из которых обычно является также и адресом результата.

double-density disk (DD) ['dʌbl 'densɪtɪ dɪsk] диск для записи с удвоенной плотностью.

double-error correcting code ['dʌbl'erə kə'rektɪŋ koud] код с исправлением двойных ошибок.

double-level grammar ['dʌbl'levl 'græmə] двухуровневая грамматика, грамматика ван Вейнгардена.

double-pole (DP) ['dʌblə'poul] двухполюсный.

double-encrypted ['dʌblə,ɪn'kriptɪd] *adj.* дважды зашифрованный. @ **double-encrypted data** дважды зашифрованные данные.

double-iterated ['dʌblə,ɪtə'reɪtɪd] *adj.* дважды итеративный. @ **double-iterat-ed knapsack** дважды итеративный вектор ранца.

double-key ['dʌblə'ki:] *adj.* двухключевой. @ **double-key cryptography** двухключевая криптография (криптография с открытым ключом). @ **double-key encryption** шифрование двойным ключом.

double-length key ['dʌblə'leŋθ 'ki:] ключ двойной длины (по сравнению с принятой).

downline ['dʌblə'lain] *adj.* отправленный по линии связи из центра. @ **downline key load** загрузка (ввод) ключа по линии связи из центра распределения ключей.

download ['dʌblə'loud] *n.* загрузка (ввод) по линии связи (напр, ключей); *v.* загружать (вводить) по линии связи. @ **download a key** загружать (вводить) ключ по линии связи.

downloaded ['dʌblə' loudɪd] *adj.* загружаемый (вводимый) по каналу связи. @ **downloaded key** ключ, загружаемый (вводимый) по линии связи.

draw [drɔ:] *v.* (**drew, drawn**) 1. тащить, тянуть; 2. чертить, рисовать; 3. составлять (**up**); 4. черпать, извлекать (**on, upon**); 5. выводить (**заключение**). # **to draw attention to** привлекать внимание к. # **to draw a conclusion** делать вывод, выводить заключение. # **to draw a distinction** проводить различие. # **to draw to a close** подходить к концу.

Dreyfus affair дело Дрейфуса.

drop [drɒp] *v.* 1. ронять; 2. падать, снижаться; опускаться. # **drop in** зайти; *n.* 1. капля; 2. падение.

drop shadow [drɒp 'ʃædou] ронять тень, затемнять.

drop-in ['drɒp'ɪn] вклинивание сигнала, появление ложного сигнала.

drop-out ['drɒp'laʊt] выпадение сигнала, пропадание сигнала.

dropped bit [drɒpt bɪt] потерянный двоичный знак, потерянный бит.

dual ['dju:l] *adj.* 1. двойной 2. обратный. @ **dual key system** система с двойным ключом (позволяет одновременно порождать ключи двух типов: для ключевого обмена, для цифровой подписи). @ **dual shift register** обратный регистр сдвига.

dual-processor configuration ['dju:l'prəusesə kən'fɪgju'reɪʃən] двух-процессорная конфигурация.

due [dju:] *adj.* 1. должный, надлежащий; 2. обусловленный; 3. предложенный, принадлежащий. # **due to** из-за, благодаря, вследствие; обусловленный. # **due to the fact that** вследствие того, что. # **in due course (time)** в свое время. # **to be due to** происходить благодаря (вследствие, из-за); обуславливаться, быть обусловленным, являться следствием чего-л.; принадлежать, быть предложенным.

dummy ['dʌmɪ] *n.* 1. макет; 2. манекен; *adj.* 1. фиктивный; подставной; поддельный; пустой 2. холостой (*ход*). @ **dummy argument** формальный параметр. @ **dummy information** фиктивная информация. @ **dummy order** фиктивная команда. @ **dummy padding** пустое холостое заполнение (дополнение сообщения ничего не значащей информацией). @ **dummy statement** пустой оператор.

dummy instruction ['dʌmɪ ɪn'strʌkʃən] пустая команда, НОП. @ Элемент данных, записанный в форме команды и вводимый в поток команд, но как команда не исполняющийся.

duplet ['dju:plɪt] *n.* дуплет (два одинаковых, идущих подряд знака текста).

during ['dʒu:ərɪŋ] *prp.* в продолжение, в течение; во время. # **during (in) the course of** в течение. # **during which time** (и) за это время.

dynamic [daɪ'næmɪk] *adj.* динамический. @ 1. Выполняемый или выделяемый во время работы системы. 2. Способный изменяться или подвергаться изменению. Применительно к операционной системе это означает, что система может изменяться во время работы. В программировании термин «динамический» относится к тем операциям, которые выполняются в процессе работы программы, а не на стадии компиляции. Например, выделение места в памяти для динамических массивов происходит в процессе работы программы. @ **dynamic address translation (DAT)** динамический перевод адреса. @ **dynamic array** динамический массив; массив с переменными границами. @ **dynamic check** динамический контроль. @ **dynamic loading** динамическая загрузка. @ **dynamic multiplexing** динамическое мультиплексирование. @ **dynamic range (DR)** динамический диапазон. @ **dynamic scattering (DS)** динамическое рассеяние. @ **dynamic switching (DS)** динамическое переключение; динамическая коммутация. @ **dynamic tracking filter (DTF)** динамический следящий фильтр.

dynamic allocation [daɪ'næmɪk 'æləkeɪʃən] динамическое распределение. @ Способ распределения, при котором ресурсы выделяются процессу по мере необходимости и затем освобождаются для передачи другим процессам. Статическое распределение, напротив, производится в момент первой инициализации системы.

dynamic area [daɪ'næmɪk 'ɛəriə] динамическая область, динамически определяемая область. @ Область памяти, сегменты которой динамически определяются для различного использования.

dynamic buffering [daɪ'næmɪk 'bʌfərɪŋ] динамическая буферизация. @ Динамическое распределение памяти для буферов обмена.

dynamic data structure [daɪ'næmɪk 'deɪtə 'strʌktʃə] динамическая структура данных.@ Структура данных, определяющие характеристики которой могут изменяться на протяжении ее существования.

dynamic dump [daɪ'næmɪk dʌmp] динамический (мгновенный) дамп.@ Дамп, выполняемый во время работы программы.

dynamic linking [daɪ'næmɪk 'lɪŋkɪŋ] динамическая компоновка, динамическая загрузка.@ Организация системы программирования, в которой отсутствует отдельная стадия компоновки и понятие загрузочного модуля; необходимые объектные модули подключаются при загрузке программы или по мере обращения к ним при выполнении.

dynamic memory [daɪ'næmɪk 'meməri] динамическое запоминающее устройство.@ Запоминающее устройство, в котором необходима периодическая регенерация хранимых данных.

dynamic memory allocation [daɪ'næmɪk 'meməri 'æləkeɪʃən] динамическое распределение памяти.@ Способ распределения памяти, при котором память выделяется и освобождается по запросам программы.

dynamic model [daɪ'næmɪk 'mɒdl] модель динамическая.@ Модель, отображающая процессы, происходящие в системе со временем; в частности, модели функционирования и развития.

dynamic program loading [daɪ'næmɪk 'prɒɡræm 'ləʊdɪŋ] динамическая загрузка.@ Способ загрузки программ, при котором в оперативную память считывается не вся программа» модули, отсутствующие в памяти, подгружаются по мере обращения к ним.

dynamic programming [daɪ'næmɪk 'prɒɡræmɪŋ] динамическое программирование.@ Метод оптимизации, предусматривающий уточнение стратегии поиска на каждом шаге оптимизации.

dynamic relocation [daɪ'næmɪk rɪ'lou'keɪʃən] динамическая настройка.@ Настройка адресов команд программы на конкретное положение в памяти при загрузке или во время выполнения программы.

dynamic scope [daɪ'næmɪk skuːp] динамический контекст, контекст использования.@ Соответствие между именами и переменными в некоторой точке программы, определяемое ходом выполнения программы. В динамический контекст вызванной процедуры или функции включаются переменные, описанные в вызвавшей процедуре; поэтому соответствие между именем и объектом может быть разным при вызове одной и той же процедуры из разных мест. Динамический контекст используется в интерпретируемых языках и языках функционального программирования.

dynamic storage [daɪ'næmɪk 'stɔːrɪdʒ] динамическое запоминающее устройство.@ Запоминающее устройство, в котором необходима периодическая регенерация хранимых данных.

dynamically [[daɪ'næmɪkəlɪ] *adv.* динамически.@ **dynamically changing key** динамически (непрерывно) изменяемый (во времени) ключ.

dynamics [daɪ'næmɪks] *n.* динамика.

Е*

each [i:tʃ] *adj., pron.* каждый.# **each other** друг друга.

early ['ɜ:lɪ] *adj.* ранний; *adv.* рано.# **in early** в начале.# **early in** в начале.# **as early as** еще

easy ['i:zi] *adj.* простой, тривиальный.@ **easy knapsack** тривиальный ранцевый вектор.@ **easy-to-break cipher** легко вскрываемый шифр.

eavesdrop ['i:vzdrɒp] *v.* подслушивать, перехватывать.@ **eavesdrop on legitimate messages** перехватывать истинные сообщения.

eavesdropper ['i:vzdrɒpə] *n.* пассивный нарушитель, перехватчик.

eavesdropping ['i:vzdrɒpɪŋ] *n.* подслушивание; перехват; несанкционированное извлечение информации (из канала связи).@ **eavesdropping by emanation** перехват посредством приема побочных электромагнитных излучений (несущих информацию).@ **eavesdropping by wiretap** перехват с подключением к проводной линии связи (перехват по отводному каналу).@ **eavesdropping network** сеть перехвата.@ **eavesdropping on telephone conversations** подслушивать телефонные разговоры.

effect [ɪ'fekt] *n.* 1. влияние, действие, воздействие; 2. эффект, результат; 3. следствие, результат; *v.* осуществлять, производить.# **in effect** в действительности.# **to the effect that** в том смысле, что; с тем, чтобы; так, чтобы.# **to this effect** для этой цели.# **to put into effect** осуществлять, приводить в исполнение

effective [ɪ'fektɪv] *adj.* 1. действительный, эффективный; 2. действующий, имеющий силу (*закон и т. п.*); 3. действующее.@ **effective size of a secret key** эффективным размером (длина) секретного ключа.# **to become effective** входить в силу.

effective *adj.* = **secure**

effectively [ɪ'fektɪvli] *adv.* практически.@ **effectively unbreakable cryptosystem** практически нераскрываемая криптосистема (вследствие чрезмерных затрат времени и средств).

efficiency [ɪ'fɪʃənsɪ] *n.* 1. эффективность; 2. производительность, КПД.@ **efficiency factor** коэффициент эффективности (эффективность).@ **efficiency of encryption** эффективность шифрования.

effort ['efət] *n.* усилие, попытка; работа.@ **effort involved in an attack** вычислительная сложность алгоритма вскрытия (криптосистемы).# **to exert (make) every effort** прилагать все усилия.# **to make efforts** приложить усилие.

electrically [ɪ'lektrɪkəli] *adv.* электрически.

electromagnetic (EM) [ɪlek'trɒmæg'netɪk] электромагнитный.@ **electromagnetic compatibility (EMC)** электромагнитная совместимость.@ **electromagnetic eavesdropping** перехват посредством приема электромагнитных излучений (несущих информацию).@ **electromagnetic interference filter (EMI-FIL)** фильтр подавления электромагнитных помех.@ **electromagnetic interfer-**

ence (EMI) 1. электромагнитная помеха; 2. радиопомеха. @ **electromagnetic radiation (EMR)** электромагнитное излучение.

electronic [ɪˈlekˈtrɒnɪk] *adj.* электронный. @ **electronic calculator** электронное вычислительное устройство. @ **electronic circuit analysis program (ECAP)** программа для анализа электронных схем. @ **electronic code book (ECB)** электронная кодовая книга (один из способов использования DES-алгоритма). @ **electronic counter-countermeasures (ECCM)** радиоэлектронная защита, противодействие преднамеренным радиопомехам. @ **electronic crosspoint (EXP)** электронный (бесконтактный) коммутационный элемент. @ **electronic cryptography** криптография с использованием электронной техники. @ **electronic data gathering equipment (EDGE)** электронная аппаратура сбора данных. @ **electronic data processing (EDP)** электронная обработка данных. @ **electronic data processing machine (EDPM)** ЭВМ обработки данных. @ **electronic data processing system (EDPS)** система электронной обработки данных. @ **electronic emission** электронное излучение. @ **electronic espionage** электронный шпионаж. @ **electronic fill device Funds Transfer** Электронная передача фондов. @ **electronic fill device** электронное устройство ввода (ключей). @ **electronic funds transfer (EFT) system** автоматизированная система электронных платежей. @ **electronic interception** перехват с помощью электронных средств. @ **electronic key distribution** электронное распределение ключей. @ **electronic key management system (EKMS)** система управления электронными ключами (предназначена для автоматизации хранения, распределения, использования и уничтожения электронных ключей). @ **electronic keying** электронный ввод ключей. @ **electronic mail (E-mail)** электронная почта. @ **electronic mail message** сообщение электронной почты. @ **electronic money** электронные деньги. @ **electronic post-production (EPP)** электронный монтаж. @ **electronic reconnaissance** электронная разведка. @ **electronic signal monitoring (ESM)** 1. радиоперехват; 2. радиотехническая разведка. @ **electronic surveillance** электронная слежка. @ **electronic switching system (ESS)** электронная система коммутации. @ **electronic transmission** электронная передача. @ **electronic vertical format unit (EVFU)** блок управления форматом по вертикали. @ **electronic warfare** электронные средства для ведения боевых действий.

electronic document [ɪˈlekˈtrɒnɪk ˈdɒkjumənt] электронный документ; электронный текст. @ Совокупность данных в памяти вычислительной системы, предназначенная для восприятия человеком с помощью соответствующих программных и аппаратных средств. Электронный документ может включать текстовую, графическую и звуковую информацию, иметь нелинейную структуру; различные пользователи могут просматривать его в различной форме и изменять его.

electronic filing [ɪˈlekˈtrɒnɪk ˈfɪlɪŋ] электронная картотека. @ Система, предназначенная для хранения, каталогизации и поиска документов с применением ЭВМ.

electronic office [ɪˈlekˈtrɒnɪk ˈɒfɪs] электронное учреждение. @ Система автоматизации работы учреждений, основанная на использовании ЭВМ.

electronically [ɪlek'trɒnɪkəlɪ] *adv.* электронно.@ **electronically addressed light modulator (EALM)** модулятор света с электронно-лучевой адресацией.@ **electronically controlled (EC)** с электронным управлением.@ **electronically generated key** ключ, генерируемый элементарным устройством.@ **electronically transferred key** ключ, доставляемый электронными средствами.

element (elem) ['elɪmənt] *n.* 1. элемент, звено, часть, блок, устройство; 2. *pl.* основы (науки и т. н.); 3. стихия.@ **element of a group** 1. схема одноименности; 2. элемент эквивалентности группы; 3. сумма эквивалентности.

elemental ['elɪməntəl] *adj.* элементарный.

elementary [elɪ'mentəri] *adj.* 1. первичный; 2. элементарный.@ **elementary action** элементарная операция.@ **elementary digital network (EDN)** элементарная цифровая схема.@ **elementary cryptanalysis** элементарный криптоанализ.@ **elementary cryptography** элементарная криптография.@ **elementary function** элементарная функция.@ **elementary key** первичный ключ (для выполнения предварительных преобразований).@ **elementary potential digital computing component (EPDCC)** базовый элемент ЦВМ.

elicit [ɪ'lɪsɪt] *v.* выявлять, вызывать; извлекать.# **to elicit a reply** добиться ответа.

elliptic [ɪ'lɪptɪk] *adj.* эллиптический.@ **elliptic curve cryptosystem** эллиптическая криптосистема (разновидность криптосистемы с открытым ключом, принципы функционирования которой позаимствованы из теории эллиптических кривых над конечными полями).@ **elliptic integral** эллиптический интеграл.

elliptic(al) [ɪ'lɪptɪk(əl)] *adj.* эллиптический.

emanation [ɛmə'neɪʃən] *n.* излучение (работающей радиоэлектронной аппаратуры).@ **emanation integrity** непроницаемость для излучения.

embed [ɪm'bed] *v.* 1. вставлять; встраивать; 2. внедрять; 3. заделывать; 4. вводить.

embeddable [ɪm'bedeɪbl] *adj.* встраиваемый.

embedded [ɪm'bedɪd] *adj.* встроенный; вложенныйю.@ **embedded cryptographic system** встроенная криптографическая система (является составной частью другой системы, основное назначение которой не связано с криптографией).@ **embedded cryptographic system** встроенная криптографическая система (является составной частью другой системы, основное назначение которой не связано с криптографией).@ **embedded cryptography** встроенные криптографические средства.@ **embedded interpreter** встроенный интерпретатор.@ **embedded loops** вложенные циклы, кратные циклы.@ **embedded procedures** встроенные процедуры.

embedded [ɪm'bedɪd] *adj.* 1. вложенный.@ О конструкции программы, являющейся частью другой конструкции. 2. встроенный.@ Об оборудовании, используемом в составе другого оборудования.

embedded computer [ɪm'bedɪd kəm'pjʊ:tə] встроенная ЭВМ.@ ЭВМ, используемая как узел устройства для управления или обработки измерений.

embedded computer system [ɪm'bedɪd kəm'pjʊ:tə 'sɪstɪm] система со встроенной ЭВМ.@ Любая аппаратная система, включающая в себя ЭВМ, но не предназначенная для выполнения обычных вычислительных функций.

embedded pointer [ɪm'bedɪd 'pɔɪntə] встроенный указатель.@ Указатель, хранимый непосредственно в записи данных, а не в отдельном индексе или списке.

embedded scopes [ɪm'bedɪd skuːps] вложенные контексты.@ В языках с блочной структурой область видимости идентификатора, описанного в некотором блоке, включая все блоки, вложенные в данный блок. Таким образом, вложенные видимости (контексты) образуют вложенную структуру.

embedded software [ɪm'bedɪd 'sɒftwɛə] «встроенное» программное обеспечение.@ Программное обеспечение (обычно в ПЗУ) для процессора, работающего в составе некоторого устройства.

embedding [ɪm'bedɪŋ] *adj.* объемлющий.

emergency key erase button кнопка (клавиша) экстренного стирания ключей в чрезвычайных обстоятельствах.

emergency [ɪ'mɜːdʒənsɪ] *n.* 1. аварийная ситуация, авария; 2. крайняя необходимость; экстренный случай; чрезвычайные обстоятельства.@ **emergency key** ключ, используемый в чрезвычайных обстоятельствах.

emission [ɪ'mɪʃən] *n.* помехоэмиссия; эмиссия; излучение.@ **emission security (EMSEC)** безопасность по электромагнитному излучению (меры предосторожности, предпринимаемые для того, чтобы посторонние лица не смогли получить доступ к открытым текстам и ключевой информации путем анализа электромагнитных излучений от криптографического оборудования).

emissivity [ə,mɪ'sɪvɪtɪ] *n.* эмиссионная способность.

en route [en raʊt] *adv.* во время передачи.@ **en route to a destination a key should be kept secret** во время передачи получателю ключ должен храниться в секрете.

enable [ɪ'neɪbl] *v.* 1. разрешать; разблокировать; включать; 2. давать возможность.@ **enable enable** импульс разрешения.@ **enable encryption** разрешать (включать) шифрование.@ **enable realtime preview** использовать функцию предварительного просмотра в рабочем режиме.

enabled interrupt [ɪ'neɪblɪd ˌɪntə'rʌpt] разрешенное прерывание, немаскированное прерывание.

encipheribilih [en'saɪfənɪbɪlɪh] *n.* шифруемость; *adj.* цифрованный, зашифрованный.@ **encipheribilih block** блок шифр (зашифрованный блок).@ **encipheribilih ciphertext** повторно зашифрованный шифртекст.@ **encipheribilih code** код с перешифровкой.@ **encipheribilih data** зашифрованные данные.@ **encipheribilih key** зашифрованный ключ.@ **encipheribilih message** зашифрованное сообщение.

encipher (E, ECPH) [en'saɪfə] *v.* шифровать, зашифровывать.@ **encipher below decipher above (EBDA)** шифртекст сверху, открытый текст — внизу (одно из правил шифрования-расшифрования при работе с шифром Плейфейе-

ра).@ **encipher on the Enigma** шифровать при помощи "Энигмы".@ **encipher on the fly** шифровать на лету (в темпе ввода открытого текста).@ **encipher right decipher left (ERDL)** шифртекст справа, открытый текст слева (одно из правил шифрования-расшифрования при работе с шифром Плейфейера).@ **encipher with a binary sequence** шифровать при помощи двоичной последовательности.

encipher function = encryption function

encipher in a key = encrypt in a key

encipherer [en'saɪfərə] *n.* кодирующее устройство, шифратор.

enciphering (E, ECPH) [en'saɪfɪŋ] *n.* шифрование, зашифрование.@ Процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа в результате которого возникает шифрованный текст.@ **enciphering alphabet** шифрующий алфавит.@ **enciphering bit** бит (ключа) шифрования (ключевой последовательности).@ **enciphering data** шифрование данных.@ **enciphering equation** уравнение зашифрования.@ **enciphering error** ошибка шифрования.@ **enciphering graph** граф шифрования.@ **enciphering key sequence generator** генератор ключевой (шифрующей) последовательности.@ **enciphering machine** шифратор.@ **enciphering matrix** матрица шифрования (шифрующая матрица).@ **enciphering method** метод шифрования.@ **enciphering process** процесс зашифрования.@ **enciphering rule** правило шифрования.@ **enciphering sequence generator** генератор шифрующей последовательности.@ **enciphering sequence** шифрующая последовательность.@ **enciphering transformation** шифрующее преобразование.

enciphering key generator = key generator (KG, Key-Gen)

encipherment [en'saɪfəmənt] *n.* шифрование, зашифрование.

enclosure [ɪn'klaʊdʒə] *n.* корпус, кожух.

encode [ɪn'kəʊd] *v.* (за)кодировать, шифровать.@ **1.** Преобразовывать данные в форму, в которой они хранятся или передаются. **2.** Выполнять операцию, обратную операции декодировать.

encoded [ɪn'kəʊdɪd] *adj.* кодированный, закодированный.@ **encoded message** кодированное (закодированное) сообщение.

encodement [ɪn'kəʊdɪmənt] *n.* кодирование, шифрование (процесс).

encoder [ɪn'kəʊdə] *n.* 1. кодирующее устройство, кодер; 2. кодировщик, шифровальщик.@ **encoder-decoder** кодер-декодер.

encoding [ɪn'kəʊdɪŋ] *n.* кодирование.@ **encoding format** формат кодирования.@ **encoding key** ключ кодирования (шифрования).@ **encoding machine** шифровальная машина.@ **encoding matrix** кодирующая (шифрующая) матрица.@ **encoding rule** правило кодирования (шифрования).@ **encoding scheme** схема кодирования (шифрования).

encourage [ɪn'kʌrɪdʒ] *v.* 1. ободрять; поощрять; поддерживать; 2. способствовать; стимулировать.# **to encourage attention** привлекать внимание.

encrypt [ɪn'kript] *v.* шифровать, зашифровывать.@ **encrypt a message with a secret key** шифровать сообщение с помощью секретного ключа.@ **encrypt in**

a key шифровать на ключе.@ **encrypt information into a cipher** шифровать информацию.@ **encrypt-on-demand program** программа шифрования по запросу (пользователя).

encrypt to a key = encrypt in a key

encrypt under a key = encrypt in a key

encryption *n.* = **encryption**

encrypted text = **ciphertext**

encrypter *n.* = **encryptor**

encrypting *adj.* = **enciphering**

encrypted [in'kriptid] *adj.* шифрованный, зашифрованный.@ **encrypted channel** канат с криптографической защитой.@ **encrypted file** шифрованный файл.@ **encrypted key exchange** обмен зашифрованными ключами.@ **encrypted key** зашифрованный ключ.@ **encrypted Messaging Protocol (EMP)** протокол шифрованных сообщений (используется для защиты от несанкционированного доступа к файлам в файловой системе NFS).

encryption (ENC) [in'kripʃən] *n.* шифрование.@ **encryption algorithm name** название алгоритма шифрования.@ **encryption algorithm** алгоритм шифрования.@ **encryption application** криптографическое приложение.@ **encryption board** плата (со схемами) шифрования.@ **encryption by random grids** шифрование случайными решетками.@ **encryption calculator** калькулятор с функцией шифрования.@ **encryption circuit** схема шифрования.@ **encryption equipment manufacturer** производитель шифровального оборудования.@ **encryption export controls** контроль за экспортом средств шифрования.@ **encryption feature** возможность шифрования.@ **encryption formula** формула шифрования.@ **encryption function** функция шифрования.@ **encryption gear** устройство шифрования.@ **encryption granularity** гранулярность шифрования (минимальная длина отрезка или блока шифруемого текста).@ **encryption integrity** целостность шифрования (шифртекста).@ **encryption is easy, but key management is hard (old saying in the cryptography business)** "Шифровать легко, трудно ключами управлять" (старинная поговорка у криптографов).@ **encryption issue** вопрос шифрования.@ **encryption key name** имя ключа шифрования.@ **encryption key weakness** нестойкость ключа шифрования.@ **encryption key (ENC)** ключ шифрования.@ **encryption market** рынок (сбыта) средств шифрования.@ **encryption mechanism** механизм шифрования.@ **encryption menu** меню шифрования.@ **encryption module** модуль шифрования.@ **encryption option** опция шифрования.@ **encryption package** шифратор в отдельном корпусе.@ **encryption procedure** процедура шифрования.@ **encryption process** процесс шифрования.@ **encryption product** 1. устройство шифрования (шифратор); 2. программа шифрования.@ **encryption program** программа шифрования.@ **encryption protection** криптографическая защита (криптографическое закрытие информации).@ **encryption protocol** протокол шифрования (определяет порядок применения алгоритма шифрования).@ **encryption research** исследования в области шифрования.@ **encryption round structure** структура цикла (раунда) шифрования.@ **encryption software mod-**

ule программный модуль шифрования. @ **encryption software package** пакет программ шифрования. @ **encryption standard** стандарт шифрования. @ **encryption technology** технология шифрования. @ **encryption under DES** шифрование по DES-алгоритму. @ **encryption-decryption device** шифратор-дешифратор. @ **encryption-decryption key pair** пара ключей шифрования-расшифрования. @ **encryption-decryption (e-d)** шифрование-расшифрование. @ **encryption-of-data-only mode** режим шифрования только информационных данных (без шифрования заголовков, данных управления и контроля). @ **encryption-only key** ключ только для зашифрования. @ **encryption-protected** снабженный криптозащитой.

encryption chip = **cryptochip**

encryption error = **encipherment error**

encryption machine = **cipher machine**

encryption-based authentication = **cryptographic authentication**

encryptor [in'kriptə] *n.* блок шифрования, схема шифрования; шифратор.

end [end] *n.* 1. конец. @ Служебное слово, указывающее на конец программной конструкции (составного оператора или элемента описаний). 2. завершение, конец (*выполнения процесса*); 3. цель; 4. результат; *adj.* конечной, конечный; *v.* кончать(ся); заканчивать(ся). @ **end formula** конечная (оконечная) формула. @ **end mark** метка (маркер) конца. @ **end of address (EOA)** конец адреса. @ **end of block (EOB)** конец блока. @ **end of file indicator** признак конца файла (массива). @ **end of volume (EOV)** конец тома; признак конца тома. @ **end point** 1. конечная (конечная) точка; 2. начальная и конечная точка; 3. пределы интегрирования. # **end to end** непрерывно. # **end-use testing** эксплуатационное испытание. # **at the end** в конце. # **in the end** в конце концов. # **to (to-wards) this end** с этой целью. # **with this end in view** с этой целью.

end user [end 'ju:zə] конечный пользователь. @ Человек или организация, применяющая ЭВМ для решения собственных задач.

end-around borrow [end,ə'raund 'bɔ:rou] циклический отрицательный перенос, циклический заем. @ **end-around shift** циклический сдвиг.

end-around carry [end,ə'raund 'kæri] циклический перенос, круговой перенос. @ При сложении отрицательных чисел в дополнительном коде – перенос из самого старшего разряда в самый младший.

end-of-data mark [end'ɒv'deɪtə ma:k] метка (маркер) конца данных

end-of-file mark [end'ɒv'faɪl ma:k] метка (маркер) конца массива данных

end-of-tape marker [end'ɒv'teɪp 'ma:kə] маркер конца ленты. @ Физическая метка, указывающая конец доступной для записи поверхности магнитной ленты.

end-point control [end'pɔɪnt kən'troul] управление по выходным данным.

end-to-end [end'tu:'end] *adj.* сквозной, межконцевой, оконечный, абонентский. @ **end-to-end encryption cryptosystem** криптосистема межконцевого шифрования.

end-to-end encryption (ETE) [end'tu:'end 'ekrɪpʃən] сквозное шифрование. @

1. Передача зашифрованного сообщения через всю систему без промежуточных этапов расшифровки и повторного шифрования. 2. Сквозное межконцевое (оконечное) абонентское шифрование (производится отправителем зашифрованных данных и предполагает их расшифрование получателем).

endeavour [ɪn'devə] *v.* пытаться, стараться.

ending *n.* ['endɪŋ] окончание. @ **ending file label** метка конца файла. @ **ending tape label** метка конца ленты.

endless loop ['endles lu:p] бесконечная петля.

endomorph [ɪndə'mɔ:fɪ:k] *adj.* эндоморфный. @ **endomorph cipher** эндоморфный шифр (шифр, в котором для каждой пары шифрующих преобразований имеется третье, равное их произведению).

endorse [ɪn'dɔ:s] *v.* 1. подтверждать, одобрять; 2. аттестовать.

endorsed [ɪn'dɔ:st] *adj.* аттестованный, сертифицированный. @ **endorsed Cryptographic Products List (ECPL)** Список сертифицированной криптографической аппаратуры. @ **endorsed for un-classified cryptographic item** аттестованный для использования в несекретной криптографическом изделии (несекретное криптографическое оборудование одобрено NSA USA для использования в целях защиты информации, которое имеет значение для обеспечения государственной безопасности USA).

endorsement [ɪn'dɔ:smənt] *n.* аттестация; сертификация (оценка криптографического оборудования на предмет его возможного использования для защиты информации, имеющей значение для обеспечения государственной безопасности страны).

enemy ['enɪmɪ] *n.* враг, противник. @ **enemy's cipher** шифр противника. @ **enemy cryptanalyst** криптоаналитик противника.

engage [ɪn'geɪdʒ] *v.* 1. нанимать; 2. заниматься, быть занятым. # **to be engaged in** заниматься чем-л.

Enigma [ɪ'nɪgmə] 1 *n.* "Энигма" ("Загадка") (немецкая шифровальная машина, находившаяся в эксплуатации в 20-е—40-е годы). @ **Enigma key** ключ "Энигмы". @ **Enigma secret** секрет "Энигмы". @ **Enigma simulator** эмулятор "Энигмы". @ **Enigma variations** модификации "Энигмы".

entrap [ɪn'træp] *v.* поймать в ловушку, запутать, обмануть.

entrapment [ɪn'træpmənt] *n.* ловушка (намеренное внесение очевидных изъянов в работу криптографического оборудования с тем, чтобы своевременно выявлять все попытки его взлома в процессе эксплуатации).

entropic ['entrəpɪk] *adj.* энтропийный. @ **entropic key** энтропийный ключ.

entropy ['entrəpi] *n.* энтропия. @ Мера неопределенности случайного объекта.

entry *n.* ввод (напр, ключа).

entry ['entri] *n.* 1. элемент (каталога, списка, таблицы); статья (словаря); 2. вход; точка входа; 3. ввод (напр, ключа); 4. ввод данных; 5. запись. @ Начало

выполнения программы или процедуры. @ **entry time** момент входа. @ **entry label** имя (точки) входа.

entry conditions ['entrɪ kən'dɪʃəns] начальные условия; предусловия. @ Условия, которые выполняются или должны выполняться в момент начала выполнения (под) программы.

entry instruction ['entrɪ ɪn'strʌkʃən] точка входа, команда входа в программу. @ Команда, с которой начинается выполнение команды или процедуры.

entry point ['entrɪ pɔɪnt] точка входа, адрес (точки) входа. @ Адрес команды или сама команда, с которой начинается выполнение программы или процедуры.

equal (EQ) ['i:kwəl] *v.* равняться, быть равным; *adj.* равный, одинаковый, идентичный; равносильный. @ **equal order digits** цифры одинаковых разрядов. @ **equal cipher systems** идентичные шифрсистемы (две шифр системы называются идентичными, если имеют одинаковые пространства сообщений и криптограмм, а также совпадающие шифрующие преобразования).

equally ['i:kwəlɪ] *adv.* равно. @ **equally probable** равновероятный.

equally likely = **equally probable**

equation (eq., eqn.) ['i'kwɛɪʃən] *n.* уравнение, равенство.

equipment key = **hardware key**

equipment ['i'kwɪpmənt] *n.* 1. оборудование, аппаратура; 2. приспособление.

equiprobability ['i:kwɪprɒbə'bɪlɪtɪ] *n.* равная вероятность. @ **equiprobability curve** кривая равных вероятностей.

equivalence ['i'kwɪvələns] *n.* эквивалентность (логическая операция). @ **equivalence class** класс эквивалентности. @ **equivalence gate** схема функции эквивалентности. @ **equivalence relation** отношение эквивалентности.

equivalencing ['i'kwɪvələnsɪŋ] *n.* эквивалентирование.

equiprobable ['i'kwɪprɒbəblɪ] *adj.* равновероятный. @ **equiprobable keys** равновероятные ключи.

equivalent ['i'kwɪvələnt] *n.* эквивалент; *adj.* эквивалентный. @ **equivalent keys** эквивалентные ключи. @ **equivalent binary representation** эквивалентное двоичное представление. @ **equivalent noise bandwidth (ENBW)** эквивалентная шумовая полоса. @ **equivalent noise generator (ENG)** эквивалентный шумовой генератор.

equivalent binary digits ['i'kwɪvələnt 'baɪnəri 'dɪʒɪt] эквивалентные двоичные знаки. @ Для заданного исходного алфавита число эквивалентных двоичных знаков есть минимальное число бит, необходимое для получения при помощи некоторого блочного кода такого числа кодовых слов, которое по крайней мере было бы не меньше числа символов в этом алфавите.

equivalent table ['i'kwɪvələnt 'teɪbl] таблица пересчета. @ Таблица перевода одних величин в другие.

equivalent trees ['i'kwɪvələnt tri:s] эквивалентные деревья. @ Подобные деревья с одинаковыми данными в соответствующих вершинах.

equivocation [i'kwivou'keɪʃən] *n.* надежность. @ **equivocation function** функция надежности ключа (мера неопределенности ключа для криптоаналитика, анализирующего первые такие криптограммы).

erasable [i'reɪz'əbl] *adj.* стираемый.

erasure [i'reɪz'ʃuə] *n.* стирание (записи); уничтожение (информации)

error (err) [i'erə] *n.* 1. ошибка. 2. погрешность; 3. расхождение. @ **error-correcting code** код, исправляющий ошибки. @ **error-free key entry** безошибочный ввод ключа. @ **error-propagating cryptosystem** криптосистема с размножением ошибок. @ **escrow key** ключ депонирования (с помощью ключа депонирования шифруются ключи, передаваемые на хранение третьим лицам). # **trial and error method** метод проб и ошибок. # **to be in error** заблуждаться.

escrow [i'eskrou] *n.* депонирование (у третьих лиц) @ Депонирование представляет собой размещение документа в электронной форме.

escrowed [i'eskrouɪd] *adj.* депонированный (у третьих лиц). @ **escrowed Encryption Standard** (американский) Стандарт шифрования с депонированием (ключей).

espionage [i'espɪə'na:ʒ] *n.* шпионаж.

establish [i'stæblɪʃ] *v.* 1. учреждать; основывать; 2. устанавливать, определять; 3. подтверждать. @ **establish a secret key** устанавливать (определять) секретный ключ.

establishment [i'stæblɪʃmənt] *n.* установление.

estimate [i'estɪmɪt] *n.* 1. оценка. @ Приближенное определение значения некоторой величины, выполняемое до точного вычисления ее или зависящих от нее величин. *v.* 1. оценивать; 2. определять; вычислять. # **as a conservative estimate** по скромному подсчету.

estimation [i'estɪ'meɪʃən] *n.* 1. суждение; мнение; оценка; 2. уважение; 3. подсчет, вычисление.

Euclidean algorithm алгоритм Евклида (метод нахождения наибольшего общего делителя, названный так по имени древнегреческого математика, который впервые описал его в III веке до нашей эры).

Euclid's algorithm *n.* = **Euclidean algorithm**

Euler function функция Эйлера.

Euler pseudoprime to the base b псевдопростое число Эйлера по основанию b.

Euler totient function = **Euler function**

eused [i'ju:zd] *adj.* повторно использованный. @ **eused key** повторно использованный ключ.

eve [i:v] *n.* канун. # **on the eve** накануне.

even [i:vən] *adv.* даже; *adj.* 1. ровный, гладкий; 2. четкий; 3. равный, такой же; *v.* выравнивать (**out**). @ **even distribution** равномерное распределение. @ **even frequency count** гладкая маркировка (текста). # **even so** даже в этом случае. # **even though** даже если.

event [i'vent] *n.* 1. событие. @ Условие, выполнение которого должно или может вызвать определенную реакцию программы или операционной системы. 2. событие; 3. случай; 4. явление; 5. исход, результат. # **at all events** во всяком случае. # **in any event** во всяком случае. # **in the event** в конечном счете.

eventually [i'ventʃuəli] *adv.* в конце концов, в конечном счете; в результате. @ **eventually periodic sequence** в конечном счете периодическая последовательность.

ever ['evə] *adv.* 1. когда-либо; 2. всегда. # **ever increasing** все возрастающий. # **ever since** с тех пор. # **ever so** очень. # **for ever** навсегда. # **if ever** если это вообще (имеет место). # **hardly ever** почти никогда; редко.

every ['evri] *pron.* каждый; всякий. # **every now and again** время от времени. # **every now and then** время от времени.

evidence ['evidəns] *v.* служить доказательством; доказывать (свидетельствовать); *n.* 1. очевидность; 2. доказательство; основание; 3. данные; 4. признак. # **bas (is) evidenced by** о чем свидетельствует. # **in evidence** заметный. # **to give evidence** свидетельствовать.

exact [ig'zækt] *v.* требовать (*настоятельно*); *adj.* точный. # **to be more exact** точнее.

example [ig'za:mpəl] *n.* пример. # **for example** например.

except [ik'sept] *v.* исключать; *prp.* исключая, кроме. # **except (for, that)** за исключением, кроме. # **except in so far as** за исключением того, что.

exception [ik'sepʃən] *n.* 1. особая ситуация, исключительная ситуация. @ Условия обычно обнаружение ошибки, требующие прерывания нормальной последовательности выполнения программы. 2. исключение. # **with the exception** за исключением.

excess [ik'ses] *n.* избыток. # **in excess of** свыше. # **to be in excess of** превышать.

exchange [iks'tʃeɪndʒ] *n.* 1. перестановка (*двух элементов*); 2. обмен (*информацией*); 3. смена, замена; 4. переадресация; *v.* заменять; *v.* обменивать(ся); *n.* обмен. @ **exchange in a network** обмен в сети. @ **exchange of keys** обмен ключами. @ **exchange register** регистр обмена, регистр пересылок. @ **exchange selection** выборка с обменом.

exclusive(-)OR (XOR) [iks'klu:sɪv ɔ:] *n.* схема исключающая, схема разнотенности; *v.* выполнять операцию "исключающее ИЛИ" (сложение по mod 2). @ **exclusive(-)OR ciphertext and plaintext bits** складывать биты шифрованного и открытого текста по mod 2. @ **exclusive(-)OR cipher** шифр на основе операции "исключающее ИЛИ" (сложение по mod 2). @ **exclusive(-)OR combiner** смеситель по mod 2.

exclusive segments [iks'klu:sɪv 'segmənts] взаимноисключающие сегменты. @ Сегменты перекрытий, которые не могут находиться в оперативной памяти одновременно.

exclusive usage mode [iks'klu:sɪv 'ju:zɪdʒ moʊd] монопольный режим.

exclusion [iks'klu:ʒən] *n.* запрет. @ **exclusion of a binary function** запрет двоичной функции.

exercise ['eksəsaɪz] *v.* 1. проявлять; 2. осуществлять; 3. оказывать (*влияние и т. п.*); 4. действовать; 5. тренировка, учение. @ **exercise key** тренировочный (учебный) ключ (предназначен для использования во время военных маневров или в процессе обучения гражданского обслуживающего персонала). # **to exercise care** позаботиться. # **to exercise caution** соблюдать осторожность.

exert [ɪg'zɜ:t] *v.* 1. оказывать (*влияние и т. п.*); влиять; 2. проявлять, прилагать; развивать; 3. осуществлять, напрягать (силы); 4. действовать. # **to exert every effort** прилагать все усилия.

exhaustion [ɪg'zɔ:sʃən] *n.* полный перебор. @ **exhaustion process** процесс истощения.

exhaustive [ɪg'zɔ:stɪv] *adj.* исчерпывающий, тотальный, полный. @ **exhaustive break** вскрытие тотальным перебором (всех возможных вариантов). @ **exhaustive cryptanalysis** переборный (неалгоритмический) криптоанализ. @ **exhaustive process** сходящийся (конечный, затухающий) процесс. @ **exhaustive search** исчерпывающий поиск (меню поиска неизвестного ключа к шифру полным перебором всех возможных ключей). @ **exhaustive search** полный перебор.

exhaustive key determination = exhaustive cryptanalysis

existence [ɪg'zɪstəns] *n.* 1. существование; жизнь; 2. наличие. # **in existence** существующий в природе. @ **existence condition** условие существования.

expand [ɪks'pænd] *v.* 1. расширять(ся); увеличивать(ся) в объеме; развивать(ся); распространять(ся); 2. разложить в ряд; 3. расширять. @ Увеличивать возможности программы или вычислительной системы, вводя в нее дополнительные компоненты.

expanded [ɪks'pændɪd] *adj.* расширенный, дополненный. @ **expanded key** расширенный (дополненный) ключ (для увеличения его длины).

expanding [ɪks'pændɪŋ] *adj.* 1. расширяющий; 2. размножающий (ошибки). @ **expanding encipherer** расширяющий шифратор (увеличивает длину текста при зашифровании).

expansion [ɪks'pænsjən] *n.* 1. расширение; распространение; 2. экспансия. @ **expansion box (E-box)** блок расширения. @ **expansion cipher** расширяющий шифр (увеличивает длину текста при зашифровании). @ **expansion factor** коэффициент расширения (открытого текста при шифровании). @ **expansion permutation** перестановка с расширением.

expansion bus [ɪks'pænsjən bls] шина расширения. @ Шина для подключения дополнительных устройств.

expect [ɪks'pækt] *v.* 1. ожидать; 2. предполагать; 3. надеяться.

expectation [ɪkspek'teɪʃən] *n.* 1. математическое ожидание; 2. вероятность; 3. надежда, предвкушение; *pl.* виды на будущее. # **expectation of life** вероятная продолжительность жизни.

expected [ɪks'pæktɪd] *adj.* ожидаемый. @ **expected frequency distribution** ожидаемое распределение частот встречаемости букв (в тексте).

expense [ɪks'pens] *n.* трата, расход. # **at the expense of** за счет.

experience [iks'piəriəns] *n.* 1. опыт (*жизненный*); 2. случай; 3. наблюдения; 4. (*pl.*) (по)знания; 5. стаж практической деятельности; 6. квалификация, мастерство; *v.* испытывать, ощущать; знать по опыту. # **as a matter of experience** исходя из опыта. # **to know something by (from) experience** знать что-л. по опыту. # **to pool the experience** делиться опытом.

expert-cryptanalyst ['ekspə:t,kriptə'nælist] *n.* эксперт-криптоаналитик.

explicit [iks'plisɪt] *adj.* 1. ясный; явный; подробный; явно заданный; 2. открытый, незашифрованный. @ **explicit declaration** явное объявление. @ **explicit definition** явное определение. @ **explicit function** явная функция. @ **explicit key** незашифрованный ключ. @ **explicit program** подробная программа, разбитая на элементарные операции.

explicitly [iks'plisɪtli] *adv.* точно, определенно.

exploration [eks'plɔ:reɪʃən] *n.* поиск.

exploratory [eks'plɔ:rətəri] *adj.* исследующий; исследовательский.

exploratory data analysis (EDA) [eks'plɔ:rətəri 'deɪtə ə'næləsɪz] разведочный анализ данных. @ Термин для обозначения методов исследования численной информации с целью распознавания ее структуры.

explore [iks'plɔ:] *v.* 1. исследовать, изучать; 2. разведывать.

exponential [eks'pəʊnənʃəl] *adj.* показательный; экспоненциальный. @ **exponential law** экспоненциальный закон. @ **exponential notation** экспоненциальное представление числа. @ **exponential time (space)** экспоненциальное время (пространство). @ **exponential time algorithm** алгоритм с экспоненциальной сложностью. @ **exponential type distribution** распределение экспоненциального типа. @ **exponential waveform** экспоненциальный сигнал.

exponential key agreement = **key agreement protocol**

exponential key exchange = **key agreement protocol**

exponentially [eks'pəʊnənʃəli] *adv.* экспоненциально. @ **exponentially-derived key** ключ, получаемый при использовании экспоненциальной функции.

exponentiation cipher шифр на основе (дискретного) возведения в степень

exponentiation [eks'pəʊntɪeɪʃəl] потенцирование, возведение в степень. @ Операция возведения в степень, n -кратное умножение числа x на себя (x^n).

exponentiation-based cipher = **exponentiation cipher**

export ['ekspɔ:t] экспорт. @ **export workspace** экспорт рабочей среды.

export list ['ekspɔ:t list] список экспорта. @ В описании модуля – список определенных в данном модуле имен, которые могут быть использованы в других модулях.

exportable ['ekspɔ:təbl] *n.* разрешенный к экспорту. @ **exportable 40-bit session keys** разрешенные к экспорту 40-битовые сеансовые ключи.

exported ['ekspɔ:tɪd] *adj.* экспортируемый. @ О переменной, константе, типе, процедуре или другом программном объекте, которые определены в данном модуле и могут быть использованы в других модулях.

exposure [iks'pəʊʒə] *n.* 1. экспозиция, выдержка; 2. раскрытие, разглашение (зашифрованной информации или ключа). @ **exposure key** расширенный

(дополненный) ключ. @ **exposure message** расширенное (дополненное) сообщение (получена путем добавления аутентификатора к исходному тексту сообщения).

extend [iks'tend] *v.* 1. простирать(ся); 2. расширять(ся); 3. распространять на; 4. тянуть, вытягивать; 5. удлинять.

extended [iks'tendɪd] *adj.* 1. расширенный, дополненный; 2. растянутый, вытянутый. @ **extended calculus** расширенное исчисление.

extended addressing [iks'tendɪd ə'dresɪŋ] расширенная адресация. @ Любой из методов адресации, обеспечивающих доступ к памяти с адресным пространством, большим нежели адресное пространство, предусматриваемое форматом команды.

extended ASCII [iks'tendɪd] расширенный код ASCII. @ Восемьразрядный код для представления текстовой информации, совпадающий с кодом ASCII для символов от 32 до 127.

extended Backus-Naur form (EBNF) [iks'tendɪd fɔ:m] расширенная форма Бекуса-Науру, расширенная БНФ. @ Способ описания грамматик для определения синтаксиса языков программирования. Расширенная БНФ отличается от БНФ более удобными средствами записи повторяющихся и необязательных компонент.

extended binary-coded decimal interchange code (EBCDIC) [iks'tendɪd 'baɪnəri'kəʊdɪd 'ɪntə'tʃeɪndʒ kəʊd] расширенный двоично-десятичный код обмена информацией. @ Восемьразрядный код для представления текстовых данных.

extended-precision [iks'tendɪd,prɪ'sɪʒən] с повышенной точностью. @ О числах, представляемых несколькими машинными словами, и об арифметических операциях над ними.

extension [iks'tenʃən] *n.* 1. расширение, распространение; удлинение; продолжение, развитие; 2. вытягивание; 3. протяжение; протяженность. @ **extension field** алгебраическое расширение поля.

extension of a source [iks'tenʃən əv ə sɔ:s] расширение источника. @ В теории кодирования расширением называется процесс одновременного кодирования группы символов или результаты этого процесса.

extension register (E-register) [iks'tenʃən 'redʒɪstə] регистр расширения. @ Дополнительный регистр арифметического устройства, используемый для размещения результата умножения.

extent [iks'tent] *n.* 1. степень, предел, мера; 2. протяжение; размер; 3. экстен-
тент. @ Непрерывная область на диске. 4. диапазон; протяженность. # **to the extent (of)** до, вплоть до; в пределах. # **to the extent that** в том смысле, что. # **to a certain extent** в известной мере; до некоторой степени. # **to same extent** до некоторой степени. # **to such an extent** до такой степени.

external [eks'tɜnl] *adj.* 1. наружный, внешний; 2. иностранный; *n. pl.* 1. внешность; внешнее, несущественное; 2. внешние обстоятельства. @ **external arithmetic** (дополнительный) арифметический процессор. @ **external decimal** неупакованное десятичное (число). @ **external delay** простой по внешней причине. @ **external device** внешнее устройство. @ **external-signal interrupt** пре-

рывание внешним сигналом. @ **external error control (EEC) for cryptosystems** наружный контроль за ошибками в криптосистемах. @ **external key entry** ввод ключа извне (ввод ключа от внешнего источника). @ **external key** внешний ключ (ключ от внешнего источника). @ **external variant cipher system** внешняя вариантная шифрсистема. @ **external disturbance** внешнее возмущение. @ **external environment** условия эксплуатации. @ **external error control (EEC) for cryptosystems** наружный контроль за ошибками в криптосистемах. @ **external fragmentation** (внешняя) фрагментация. @ **external interrupt** внешнее прерывание; прерывание от внешнего устройства. @ **external key entry** ввод ключа извне (ввод ключа от внешнего источника). @ **external key** внешний ключ (ключ от внешнего источника). @ **external memory** внешняя память, внешнее запоминающее устройство. @ **external name** внешнее имя. @ **external node** концевая вершина. @ **external programming** внешнее программирование. @ **external specification** внешние спецификации. @ **external storage** внешняя память, внешнее запоминающее устройство. @ **external variant cipher system** внешняя вариантная шифрсистема. @ **external-signal interrupt** прерывание внешним сигналом.

external file [eks'tɛnl fail] внешний файл. @ Переменный файл, связанный с некоторым файлом операционной системы.

external function [eks'tɛnl 'fʌŋkʃən] внешняя функция. @ Функция, определенная и оформленная вне тела программы.

external key [eks'tɛnl ki:] внешний ключ. @ В реляционных базах данных — недоступный пользователю системный атрибут, уникально идентифицирующий кортеж.

external label [eks'tɛnl 'leɪbl] внешняя метка. @ Метка, определенная в другом модуле программы.

external path length [eks'tɛnl pa:θ leŋθ] длина концевого маршрута. @ В некотором дереве это сумма длин всех маршрутов из корневой вершины в концевую.

external performance [eks'tɛnl pə'fɔ:məns] фактическое быстродействие. @ Быстродействие с точки зрения прикладной программы, определяемое быстродействием процессора и периферийных устройств, накладными расходами операционной системы и системы программирования.

external reference (extrn) [eks'tɛnl 'refrəns] внешняя ссылка. @ Использование внешнего имени.

external representation [eks'tɛnl ,reprɪzen'teɪʃən] внешнее представление. @ Представление данных в форме, пригодной для прочтения человеком.

external schema [eks'tɛnl ski:m] внешняя схема. @ Схема, описывающая базу данных или ее часть с точки зрения прикладной программы или пользователя.

external sort [eks'tɛnl sɔ:t] внешняя сортировка. @ Сортировка с применением внешних запоминающих устройств.

external symbol [eks'tənl 'sɪmbəl] внешний символ.@ Имя или метка, определенные в другом модуле программы и значение которых определяется при компоновке.

external symbol dictionary [eks'tənl 'sɪmbəl 'dɪkʃənri] словарь внешних символов.@ Часть объектного или загрузочного модуля, описывающая определенные или написанные в нем внешние символы.

externally [eks'tənlɪ] *adv.* извне.

externally loaded key = **external key**

externally supplied key = **external key**

extra- [eks'trə-] *pref.* сверх-; особо-; экстра-; *adj.* 1. дополнительный; 2. особый; 3. высшего качества.@ **extra address** дополнительный адрес.@ **extra key** дополнительный ключ.@ **extra large-scale integration (ELSI)** степень интеграции выше сверхвысокой.@ **extra order** дополнительный разряд.

extract ['ekstrækt] *v.* 1. выделять (*например, часть машинного слова*); 2. выбирать, извлекать (*часть записей файла*).@ **extract instruction** команда выборки, команда выделения.

extraction [iks'trækʃən] *n.* извлечение

extractor [iks'træktə] *n.* устройство ввода; экстрактор (функция или устройство, выполняющие обратное преобразование по отношению к функции или устройству объединения).

extrapolation *n.* [ekstrə'pəleɪʃən] экстраполяция.@ Оценка значения функции по другим ее значениям в точке, лежащей вне интервала, на котором определены значения этой функции.

extreme [iks'tri:m] *adj.* крайний, чрезвычайный.

F*

fabricated ['fæbrɪkeɪtɪd] *adj.* сфабрикованный.

face [feɪs] *n.* 1. начертание шрифта. 2. очко (*литеры на шрифтоносителе*); 3. лицо, лицевая сторона, поверхность, плоская поверхность, грань, торец; *v.* 1. встречать, сталкиваться; 2. быть обращенным (в определенную сторону).# **in the face of** перед лицом чего-л.; несмотря на.# **on the face of it** судя по внешнему виду; на первый взгляд.# **to face a problem** столкнуться с проблемой.

facilitate [fə'sɪlɪteɪt] *v.* облегчать; способствовать.

facilities [fə'sɪlɪtɪks] *n.* удобства; средства.

facility [fə'sɪlɪtɪ] *n.* 1. средства, устройство, оборудование, аппаратура; 2. линия связи; 3. легкость; 4. возможность; 5. *pl.* устройства; приспособления; установки; оборудование; исследовательские лаборатории; заводы; 6. *pl.* средства (обслуживания); удобства; условия.

facsimile (fax, facts) [fæk'sɪmɪli] *n.* 1. факсимиле; 2. факсимильная связь; *adj.* факсимильный.@ **facsimile encryption** шифрование факсимильных сообщений.

fact [fæktə] *n.* факт.# **the fact is (that)** дело в том (что).# **the fact that** то, что.# **as a matter of the fact** фактически, на самом деле.# **due to the fact** вследствие того, что.# **in addition to the fact that** кроме того, что.# **in fact** в действительности.# **in point of fact** действительно, фактически.

factor ['fæktə] *n.* 1. коэффициент; множитель; 2. фактор; *v.* 1. разлагать на множители; 2. действовать.@ **factor analysis** факторный анализ.@ **factor a composite number** разлагать составное число на множители.@ **factor-ring** фактор-кольцо.

factorable code ['fæktəɪbl koud] каскадный код.@ Код с исправлением ошибок, который можно рассматривать как результат последовательного применения нескольких других кодов.

factoring *n.* = **factorization**

factorization (FAC) [fæk'tɔ:ɪzeɪʃən] *n.* 1. разложение на множители; вынесение за скобки; 2. факторизация.@ **factorization cryptosystem (FACC)** криптосистема на основе (сложности задачи) разложения больших чисел на (простые) сомножители.

factory ['fæktəri] *n.* изготовитель.@ **factory-installed key** ключ, устанавливаемый при изготовлении криптографической аппаратуры.

factory-programmed key = **factory-installed key**

fail [feɪl] *v.* 1. отказывать; выходить из строя; 2. выдавать «неуспех» (*о процессе решения подзадачи при переборе с возвратами*); 3. не выполняться (*о логическом условии*); быть ложным (*об утверждении*); 4. потерпеть неудачу; не иметь успеха; не удаваться; 5. быть не в состоянии сделать что-л.; не (*перед инф.*); 6. разрушаться.# **without fail** непременно, обязательно.

fail-safe [feɪl'seɪf] *adj.* нечувствительный к сбоям.@ **fail-safe circuit** цепь, предотвращающая передачу открытого текста при работе в режиме шифрования.

fail-stop [feɪl'stɒp] *adj.* прекращающий работу при появлении ошибки.@ **fail-stop signature scheme** схема цифровой подписи с прекращением работы при появлении ошибки.

failure *n.* = **fault**

fake [feɪk] *adj.* поддельный, фальшивый.@ **fake key** поддельный (фальшивый) ключ.

fall [fɔ:l] *v.* (**fell, fallen**) 1. падать; спадать, понижаться; 2. (*в сочетании с прилаг.*) становиться; 3. не хватать, не достигать (**short**); распадаться (**apart**); 5. распадаться на (**into**); 6. приходиться, падать на, выпадать; *n.* 1. понижение, спад; 2. осень.# **to fall into disuse** выходить из употребления.# **to fall short of expectations** не оправдать ожиданий.

false *adj.* = **fake**

familiar ['fæmɪljə] *adj.* хорошо знакомый, известный; привычный.# **in the familiar way** обычным путем.# **to be familiar with** знать что-л.

family ['fæmɪli] *n.* семейство.@ **family of cipher machines** семейство шифровальных машин.

far [fa:] *adj.* дальний, на большом расстоянии; *adv.* 1. далеко; 2. значительно. # **far away** дальний, отдаленный; далеко. # **far and away** значительно; несомненно. # **far and by** в общем, вообще говоря. # **far cry** большое расстояние; большая разница; отдаленное отношение. # **far from** далеко не (*неперед ing-form*). # **far reaching** многообещающий, далеко идущий, важный, огромный. # **as far as** насколько; поскольку; до. # **as far as ... is concerned** что касается, когда речь идет о. # **as far as it goes** поскольку дело касается, что касается. # **as far back as** еще, уже. # **by far** значительно; несомненно. # **few and far between** немногочисленные и редкие. # **(in) so far as** поскольку. # **(in) so far as ... is concerned** что касается; поскольку речь идет о; когда дело касается. # **so far** до сих пор. # **thus far** до сих пор. # **this is far from being the case** это далеко не так, дело обстоит совсем не так.

fashion ['fæʃən] *n.* 1. образ, манера; 2. форма; 3. стиль, мода; *v.* придавать вид (форму). # **after (in) a fashion** некоторым образом, до известной степени. # **after the fashion** наподобие; следуя методу, по методу. # **in this fashion** таким образом.

fast [fa:st] *adj.* 1. быстрый; 2. прочный; крепкий; *adv.* крепко, прочно. @ **fast Data Finder (FDF)** устройство быстрого поиска данных (микросхема для ускорения процесса поиска в больших компьютерных базах данных). @ **fast digital processor (FDP)** быстродействующий цифровой процессор. @ **fast Encryption Algorithm (FEAL)** быстрый алгоритм шифрования **fast Fourier transform (FFT)** быстрое преобразование Фурье, БПФ. @ **fast Encryption Algorithm** быстрый алгоритм шифрования. @ **fast multiplier** быстродействующий умножитель. @ **fast parallel arithmetic unit** быстродействующее арифметическое устройство параллельного типа. @ **fast response** быстрое срабатывание. @ **fast Walsh Transform (FWT)** быстрое преобразование Уолша.

fast core [fa:st kɔ:] сверхоперативное запоминающее устройство (ЗУ). @ Вид оперативного ЗУ время доступа к которому меньше, чем у приборов, на которых построено основное ЗУ.

fault [fɔ:lt] *n.* 1. ошибка; отказ; неисправность. @ Частичная или полная потеря работоспособности или неправильное функционирование. Термин «fault» подразумевает проявление ошибки, а термин «error» – причину ошибки. 2. недостаток, дефект, сбой. @ **fault analysis attack** атака методом анализа сбоя. @ **fault analysis** анализ сбоя (для вскрытия ключей в работе криптографического процессора намеренно вызывается возникновение сбоя). # **to a fault** очень, слишком. # **to be at fault** быть, находиться в затруднении. # **to be in fault** быть виноватым.

favour ['feivə] *v.* 1. благоприиятствовать, способствовать; 2. предпочитать; высказываться за; *n.* расположение, благосклонность; одолжение. # **in favour of** в пользу, за, предпочтительно; вместо.

feasible ['fi:zəbl] *adj.* 1. возможный; 2. осуществимый. @ **feasible solution** 1. допустимое решение, удовлетворяющее условиям; 2. возможное решение. @ **feasible decryption** осуществимое дешифрование.

federal ['fedərəl] *adj.* федеральный. @ **Federal Agency for Government Communications and Information (FAPSI)** Федеральное агентство правительственной связи и информации (Российское правительственное ведомство, занимающееся перехватом и дешифрованием сообщений). @ **federal Bureau of Investigation (FBI)** Федеральное бюро расследований (USA). @ **federal Information Processing Standard 140-1 (FIPS 140-1)** Федеральный стандарт (USA) на обработку информации 140-1 (соответствие этому стандарту является необходимым требованием, которое предъявляется к криптографическим системам защиты информации в правительственных ведомствах USA и Канады). @ **federal Information Security Agency** Федеральное агентство безопасности информации (немецкое правительственное ведомство, занимающееся перехватом и дешифрованием сообщений).

federal Agency of Government Communications and Information = federal Agency for Government Communications and Information

feedback ['fi:d.bæk] *n.* обратная связь. @ **feedback coefficient** коэффициент обратной связи. @ **feedback function** функция обратной связи. @ **feedback polynomial** полином обратной связи.

Feistel cipher шифр Фейстела (является разновидностью итеративного блочного шифра).

Fermat prime простое число Ферма.

Fermat's little theorem малая теорема Ферма.

few [fju:] *adj.* немногие; мало. # **a few** несколько, некоторые. # **few and far between** немногочисленные и редкие.

Fibonacci keystream generator генератор ключевой последовательности (ключевого потока) на основе чисел Фибоначчи.

field [fi:ld] *n.* 1. поле; 2. область, сфера (деятельности); *adj.* полевой (применяемый на поле боя). @ **field cipher** полевой шифр. @ **field of characteristic q** поле с характеристикой q. @ **field of cryptography** область криптографии. @ **field-mode encryption** шифрование отдельных полей данных.

file [faɪl] *n.* файл. @ **file grow factor** коэффициент расширения файла (при его шифровании).

fill device (FD) = key fill device

fill [fɪl] *n.* 1. = **padding**; 2. заполнение (регистра сдвига); ввод (загрузка) (ключа); *v.* заполнять.

fill out = pad *v.*

filler *n.* = **padding**

filter ['fɪltə] *n.* фильтр (функция, осуществляющая преобразование некоторого входного множества и получающая на выходе только те элементы этого множества, которые удовлетворяют определенному критерию). @ **filter generator** фильтрующий генератор (линейный регистр сдвига с обратной связью и нелинейным выходом).

financial [faɪ'nænʃəl] *adj.* финансовый. @ **financial cryptography** финансовая криптография. @ **financial Institution Message Authentication Standard**

(FIMAS) Стандарт аутентификации сообщений для финансовых учреждений (USA).

find [faɪnd] *v.* отыскивать, находить. @ **find a key** находить ключ.

fingerprint ['fɪŋɡə'prɪnt] *n.* = **message digest (MD)** алгоритмы сжатия (хэширования) данных Ривеста (созданная американским криптологом Р. Ривестом серия алгоритмов, которые произвольному набору данных ставят в соответствие некоторое число, при этом вероятность повторного получения точно такого же числа для другого набора данных очень мала).

finite [fɪnɪt] *adj.* конечный. @ **finite field logarithm** логарифм над конечным полем. @ **finite field with q elements** конечное поле из q элементов. @ **finite key** ключ конечной длины.

firewall ['faɪəwɔ:l] *n.* межсетевой шлюз, брандмауэр, экранирующий фильтр (аппаратно-программный комплекс управления доступом из одной сети в другую).

first [fɜ:st] *adj.* первый; *adv.* 1. сначала; 2. впервые. # **first of all** прежде всего. # **at first** сначала. # **for the first time** впервые, в первый раз. # **in the first place** сначала; во-первых.

fit [fɪt] *v.* 1. соответствовать; годиться; подходить; 2. приспособливать(ся), прилаживать(ся); подгонять; 3. оборудовать; устанавливать, монтировать; 4. снабжать; *n.* соответствие. # **to be fit for** годиться.

fixed [fɪkst] *adj.* стационарный, постоянный. @ **fixed cipher mode** режим шифрования на постоянном ключе. @ **fixed coefficient random number generator** генератор последовательности случайных чисел с постоянными коэффициентами. @ **fixed plaintext message unit** стационарный отрезок открытого текста сообщения (блок открытого текста, который остается неизменным после применения к нему шифра преобразования). @ **fixed-key cipher** шифр с постоянным ключом.

fixed length key = **finite key**

flat [flæt] *adj.* 1. плоский; 2. пологий.

flat addressing [flæt ə'dresɪŋ] простая адресация. @ Способ указания объекта в сети ЭВМ с помощью идентификатора, не имеющего внутренней структуры.

flat file [flæt faɪl] плоский файл. @ Файл, состоящий из записей одного типа и не содержащий указателей на другие записи; двумерный массив (таблица) элементов данных.

flat graph [flæt græf] плоский граф. @ Граф, который можно изобразить на плоскости таким образом, что его вершинам соответствуют разные точки, и ребра не пересекаются.

flaw [flɔ:] *n.* дефект, недостаток; слабое место. @ **flaw cipher** дефектный шифр. @ **flaw in the encipherment** дефект шифрования. @ **flaw L-security** L-кратная стойкость (невскрываемость при криптоанализе L шифрсообщений).

flawed [flɔ:d] *adj.* дефектный.

fold [fould] *n.* 1. сгиб, складка; 2. *suf.* с числительными образует прилагательное и наречие, например: **tenfold** десятикратный; в десять раз; **twofold** двукратный, в два раза.

folded tree ['fouldɪd tri:] свернутый древовидный дешифратор.

folder ['fouldə] *n.* папка.@ Термин, используемый для обозначения каталога текстовых файлов в системах, ориентированных на неподготовленного пользователя (например, в системах подготовки текстов).

folding ['fouldɪŋ] свертка.@ Метод хэширования ключа, согласно которому ключ разбивается на несколько частей, сложение которых дает адрес.

follow ['fəlu:] *v.* 1. следовать за; 2. следить; 3. понимать; 4. следовать (*методу и т. п.*); 5. преследовать (*цель и т. п.*).# **followed by** за которым следует; с последующим.# **as following from** исходя из.# **as follows** следующим образом; следующее.# **it the following** ниже, в дальнейшем.# **in what follows** ниже, в дальнейшем.# **it follows** из этого следует.# **to follow suit** следовать примеру.

footing ['futiŋ] *n.* точка опоры; опора; основание.# **on one footing** в равных условиях; на равных основаниях.# **on an equal footing** в равных условиях; на равных основаниях.# **on the same footing** в равных условиях; на равных основаниях.

for [fɔ:] *prp.* 1. для; *т. ж.* переводится дательным падежом; 2. за; 3. в течение; 4. из-за, по причине; по; *сj.* так как, ибо.# **for all that** несмотря на все это.# **for all we know** насколько нам известно.# **for a while** на некоторое время.# **for granted** без доказательства.# **for lack of** из-за отсутствия, из-за недостатка.# **for one** например.# **for once** на этот раз.# **for one's sake** ради кого-л.# **for one thing** во-пер-вых, прежде всего.# **for the present** на этот раз; пока.# **for this reason** по этой причине.# **for which reason** по этой причине.# **for the sake of** ради чего-л.# **as for** что касается, в отношении.

for list [fɔ: list] список цикла.

force [fɔ:s] *n.* сила; *v.* вынуждать, заставлять.# **to come into force** вступать в силу.

forced [fɔ:st] *adj.* принудительная.@ **forced key change** принудительная смена (замена) ключа.

foreign ['fɔ:ɪn] *adj.* 1. иностранный; 2. посторонний; 3. чуждый; 4. инородный.@ **foreign communications** зарубежные каналы связи.@ **foreign Intelligence Surveillance Act** Закон о контроле за сбором разведывательной информации о зарубежных странах (введен в действие в USA в 1978 г. в целях обеспечения надзора за деятельностью NSA со стороны американских правоохранительных органов).@ **foreign Intelligence Surveillance Appeals Court** Апелляционная судебная инстанция по контролю за сбором разведывательной информации о зарубежных странах.@ **foreign Intelligence Surveillance Court** Судебная инстанция по контролю за сбором разведывательной информации о зарубежных странах.@ **foreign key** внешний ключ.

foremost ['fɔ:moust] *adj.* 1. передний; передовой; 2. самый главный; выдающийся.# **first and foremost** прежде всего.

foreign format ['fɔːrɪn 'fɔːmæt] «чужой» формат.@ О дисках или магнитных лентах, размеченных для другой операционной системы или другого типа устройства.

forge [fɔːdʒ] *v.* подделывать.@ **forge a certificate** подделывать сертификат.@ **forge coded signals** подделывать кодированные сигналы.

forged [fɔːdʒt] *adj.* поддельный, подложный.@ **forged message** поддельное (подложное) сообщение.

format (fmt) ['fɔːmæt] *n.* 1. формат.@ Способ расположения и представления данных в памяти, в базе данных или на внешнем носителе. 2. разметка диска, формат диска.@ Способ разбиения поверхности носителя на адресуемые элементы (дорожки и сектора). 3. формат записи.@ Соответствие между битами данных и изменением намагниченности поверхности носителя.

format ['fɔːmæt] *v.* 1. форматировать.@ Размещать данные в соответствии с предписанным форматом. 2. размечать, форматировать.@ Записывать на носитель данных метки, определяющие расположение информационных записей (блоков, секторов) и участков, не пригодных для записи, а также другую управляющую информацию.

format character ['fɔːmæt 'kærɪktə] символ управления форматом.

format control ['fɔːmæt kən'traʊl] управление форматом, управление расположением информации в устройствах вычислительной машины.

format disk ['fɔːmæt disk] форматный диск.

format implication ['fɔːmæt ɪmˌplɪ'keɪʃən] формальная импликация.

former ['fɔːmə] *adj.* прежний, бывший.# **the former** первый (из двух названных выше).

formula ['fɔːmjulə] *n.* формула, аналитическое выражение.

formulae ['fɔːmjuli:] *pl. om formula*

formulas ['fɔːmjuləz] *pl. om formula*

formulate ['fɔːmjuleɪt] *v.* формулировать.

fortnight ['fɔːtnaɪt] *n.* две недели.# **this day fortnight** через две недели.

forward (type) cycle ['fɔːwəd (taɪp) 'saɪkl] цикл движения вперед.

forward ['fɔːwəd] *adv.* вперед; *v.* 1. передавать (*дальше*); ретранслировать; 2. препровождать, направлять; *adj.* опережающий; прямой, прямоходовой.@ **forward asymmetric encryption** шифрование с прямой асимметрией (ключ получателя не может быть определен по известному ключу отправителя).@ **forward interpolation formula** формула для интерполирования вперед.@ **forward scatter (FS)** рассеяние в направлении распространения, рассеяние вперед.@ **forward-chaining** вывод «от фактов к цели».# **to put (set) forward** выдвигать, предлагать.

forward declaration ['fɔːwəd ,deklə'reɪʃən] предописание.@ Частичное описание объекта программы (типа или процедуры), не определяющее его структуры или значения, но позволяющие сослаться на него в последующих описаниях.

forward error correction (FEC) ['fɔ:wəd 'erə kə'rekʃən] прямое исправление ошибок.@ Метод исправления ошибок, состоящий в добавлении избыточной информации в исходную информацию, что позволяет обнаруживать и исправлять определенные виды ошибок.

forward reference ['fɔ:wəd 'refrəns] ссылка вперед.@ Использование идентификатора, который определяется ниже. Язык, допускающий ссылки вперед, требует как минимум двухпроходного транслятора.

forward-compatible ['fɔ:wəd,kəm'pætəbl] совместимы снизу вверх.@ О программе, работающей на старой модели ЭВМ и не использующей средств и не использующей средств, имеющихся в новых или разрабатываемых моделях.

four- [fɔ] в сложных и сложносоставных словах имеет значение четырех-@ **four-square cipher system** шифрсистема "четыре квадрата".@ **four-wheel Enigma** четырех-роторная (четырёхдисковая) "Энигма".

Fourier transform преобразование Фурье.

frame (FRM) [freim] *n.* 1. фрейм.@ В искусственном интеллекте – единица представления знаний, описывающая объект или понятие. Фрейм состоит из ссылки на суперпонятие (родовое понятие) и описаний свойств, отличающих данный объект от суперпонятия. 2. кадр.@ В сетях передачи данных – порция данных, передаваемая канальным уровнем сетевого взаимодействия. 3. конверт. 4. кадр (*изображения*); 5. рамка.@ В интегрированных системах типа Framework – часть структурированного документа, содержащая таблицу, график, текст или несколько вложенных рамок и отображаемая на экране дисплея в отдельном окне. 6. запись активации; 7. основа; 8. система; 9. формальная модель.# **frame of reference** система отсчета (координат).

fraudulent ['frɔ:dʒulənt] *adj.* поддельный, ложный, обманный.@ **fraudulent ciphertext** ложный шифртекст.@ **fraudulent cryptogram** поддельная криптограмма.@ **fraudulent message** ложное (поддельное) сообщение.

free [fri:] *adj.* 1. свободный, независимый; 2. открытый, доступный; 3. не содержащий, свободный от (**from**); *v.* освобождать.# **free of charge** бесплатный, бесплатно.# **to set free** освобождать.

freely ['fri:lɪ] *adv.* свободно.@ **freely-selected key** свободно выбираемый ключ.

French [frentʃ] *adj.* французский.@ **French diplomatic communications (FDC)** французские дипломатические каналы связи.

frequency ['fri:kwənsɪ] *n.* частота, повторяемость.@ **frequency distribution** частотное распределение.@ **frequency division multiplexing (FDM)** мультиплексирование с частотным делением.@ **frequency hop inverter = hop inverter** инвертор перелета.@ **frequency matching** согласование частот (соотнесение частот встречаемости букв в шифрованном и открытом текстах).@ **frequency of key change** частота смены ключа.@ **frequency test** частотный тест (тест для проверки случайности двоичной последовательности путем подсчета в ней количества единиц и нулей).

frequency inverter = inverter

friendly ['frendli] *adj.* дружественный.@ **friendly cryptanalyst** дружественный криптоаналитик (специалист, анализирующий шифры с целью нахождения в них скрытых уязвимых мест, что позволяет вносить в эти шифры необходимые изменения для повышения их стойкости).

from [frɒm] *prep.* от; из; с; у; по; 2. на основании, исходя из.# **from above** сверху.# **from afar** издали.# **from below** снизу.# **from of old** издавна.# **from outside (without)** снаружи.# **from over (the sea)** из-за (моря).# **as from** начиная с.

front [frʌnt] *n.* передняя сторона, фасад; *adj.* передний.# **in front** перед; впереди.

full [fu:l] *adj.* полный, целый; полноценный (неурезанный, без сокращений).@ **full DES** полноценный DES.# **in full detail** во всех деталях.# **in full swing** в полном разгаре.

function ['fʌŋkʃən] *n.* 1. функция.@ 1. Процедура, возвращающая результат. В некоторых языках функция не должна иметь побочного эффекта. 2. Величина, зависящая от других величин 3. Отображение, ставящее в соответствие одному значению аргумента ровно одно значение отображения.

function ['fʌŋkʃən] *n.* 1. математическая функция; 2. *pl.* служебные обязанности; *v.* функционировать, действовать.@ **function button** функциональная клавиша.@ **function calculator** функциональное вычислительное устройство.@ **function call** 1. вызов функции; 2. обращение к системной операции.@ **function digit** разряд кода операции.@ **function deciphering** функция расшифрование.@ **function enciphering** функция шифрование.@ **function generation** генерация функции.@ **function keyboard** функциональная клавиатура.@ **function multiplier** функциональный умножитель.@ **function space** функциональное пространство, пространство функций.@ **function table** таблица функций.@ **function theory** теория функций.@ **function's inverse** обратная функция.

function key ['fʌŋkʃən ki:] функциональная клавиша.@ Управляющая клавиша, смысл которой не определен аппаратурной или операционной системой, а зависит от выполняемой программы.

function table ['fʌŋkʃən 'teɪbl] табличная функция.@ Таблица, задающая функцию.

further ['fə:ðə] *adj.* (сравнит. степень от **far**) дальнейший; другой; *v.* действовать; *adj.* 1. далее; 2. кроме того, к тому же; еще.# **further out** еще дальше.

future ['fju:tʃə] *n.* будущее; *adj.* будущий.# **for (in) the future** в будущем, впредь.# **to be left to the future** являться делом будущего.

G*

gain [geɪn] *n.* 1. усиление, коэффициент усиления; 2. прирост, увеличение; 3. выигрыш; *v.* 1. получать, приобретать; 2. увеличиваться; 3. достигать.# **one gains the impression** создается впечатление.@ **gain access** получить доступ.# **to gain**

(get, have) an (the) advantage over (of) получить, иметь преимущество перед.#
to gain an insight into проникнуть в сущность чего-л.; понять.

Galois field (GF(p)) поле Галуа.

Galois shift register регистр сдвига Галуа.

game [geɪm] *n.* игра.@ **game theory cryptography** криптография на основе теории игр.

gamma ['gæmə] *n.* гамма (случайная или псевдослучайная битовая последовательность).

gap [gæp] *n.* 1. интервал, промежуток, пропуск, пробел, зазор; 2. расхождение; 3. разрыв; 4. отставание; 5. отсутствие сигнала.# **to bridge (close, fill) the gap** заполнить пробел.

"gap" *n.* "брешь" (набор подряд идущих нулей в битовой последовательности, которому предшествует и за которым следует единица).

garbled ['ga:blt] *adj.* искаженный.@ **garbled message** искаженное сообщение.

"gardening" ['ga:dnɪŋ] *n.* "садоводство" (уловка, с помощью которой криптоаналитик заставляет противника послать криптограмму, открытый текст которой им известен).

gear [gɪə] *n.* устройство.

general ['dʒenərəl] *adj.* 1. универсальный, общий; 2. обычный; 3. главный.@ **general model of authentication** общая модель аутентификации.@ **general purpose computer** универсальный компьютер.# **in general** вообще.# **in a general way** обычным путем; в общих чертах.# **in general terms** в общих чертах.

generalized ['dʒenərəlaɪzd] *adj.* обобщенный.@ **generalized DES (GDES)** обобщенный DES-алгоритм.

generally ['dʒenərəli] *adv.* 1. вообще; обычно; 2. в основном, в общем.# **generally accepted** общепринятый.# **generally acknowledged** общепризнанный.# **generally speaking** вообще говоря.

generate ['dʒenəreɪt] *v.* 1. генерировать, порождать, формировать вызывать; 2. производить; 3. генерировать.@ **generate a ciphertext** формировать шифр-текст.

generated address ['dʒenəreɪtɪd ə'dres] полный адрес.

generating *adj.* порождающий.@ **generating cycle** порождающий цикл.@ **generating polynomial** порождающий многочлен.@ **generating polynomial** порождающий полином.@ **generating program** программа-генератор, генерирующая программа.@ **generating routine** генерирующая программа, программа-генератор.

generation [dʒenə'reɪʃən] *n.* 1. генерация; порождение; 2. поколение; 3. версия; 4. производство, создание, образование; 5. функциональное преобразование, порождение.@ **generation information** образование новой информации, формирование данных.@ **generation number** номер версии (файла).@ **generation of keys** генерация (порождение) ключей.

generation grammar ['dʒenəreɪʃən 'græmə] порождающая грамматика.@ Формальное описание языка в виде совокупности правил вывода.

generator (gntr) ['dʒenəreɪtə] *n.* 1. генератор, преобразователь; 2. датчик; 3. первообразный корень, порождающая функция; 4. генерирующая программа, программа-генератор.

generator polynomial = generating polynomial

generic *adj.* обобщенный.

generic [dʒɪ'nerɪk] *n.* родовой.@ Об операции, функции, процедуре, применяемых к аргументам различных типов и выполняемых для аргументов разных типов по-разному. *adj.* обобщенный.@ **generic description** обобщенное описание.@ **generic function** родовая функция.@ **generic key** обобщенный ключ (используется для получения из него других ключей).@ **generic operation** родовая операция.@ **generic package** родовой пакет, настраиваемый пакет.@ **generic subroutine** родовая подпрограмма.

generic type [dʒɪ'nerɪk taɪp] родовой тип, параметризованный тип, настраиваемый тип.@ Понятие языка программирования, определяющее класс типов данных, различающихся значениями некоторого параметра или группы параметров. Родовой тип используется только для описания конкретных типов или других родовых объектов, но не для определения переменных.

genetic [dʒɪ'netɪk] *adj.* генетический.@ **genetic algorithm (GA)** генетический алгоритм (разновидность алгоритма направленного случайного поиска).

genuine ['dʒenjɪn] *adj.* подлинный, настоящий.@ **genuine key** подлинный (настоящий) ключ.

geometric(al) [dʒɪə'metrɪk(əl)] *adj.* геометрический.@ **geometric(al) transposition cipher** шифр с геометрическими перестановками.@ **geometric(al) mean** средняя геометрическая величина.@ **geometric(al) model** геометрическая модель.@ **geometric(al) series** геометрический ряд.@ **geometric(al) layout description language (GLDL)** язык описания геометрических топологий.@ **geometric(al) theory of diffraction (GTD)** геометрическая теория дифракции.

geometry [dʒɪ'ɒmɪtri] *n.* геометрия; конфигурация.

German ['dʒə:mən] *adj.* немецкий.@ **"German Book"** "немецкий" сборник (во время второй мировой войны составлялся английскими криптоаналитиками и включал в себя все прочитанные немецкие шифртелеграммы на языке оригинала).

get [get] *v.* (**got**) 1. прочитывать.@ Операция чтения записи из файла, внешнего устройства или базы данных. *Ср.* **put read**; 2. получать; 3. достигать; 3. становиться.# **to get acquainted with** познакомиться, ознакомиться с.# **to get to know** узнавать, познакомиться.# **to get rid of** отделаться от чего-л.

Gifford's cipher шифр Гиффорда (поточковый шифр, изобретенный Гиффордом в 1984 г.).

gift [gift] *n.* 1. подарок, дар; 2. способность, дарование.# **the gift of the gab** дар слова, дар речи.# **the gift of tongues** способность к изучению иностранных языков

gist [dʒɪst] *n.* суть, сущность.

gisting [dʒɪstɪŋ] *n.* аннотирование, реферирование (замена содержания перехваченного сообщения текстом, передающим смысл этого сообщения в самых общих чертах).

give [gɪv] *v.* (**gave, given**) 1. давать; 2. уступать, сдаваться (**in**); 3. отказываться (**up**); 4. выделять (**off**).# **to give attention to** обращать внимание на.# **to give consideration to** рассматривать.# **to give credit for** отдать должное.# **to give place to** уступать место, давать место.# **to give rise to** вызывать, приводить к.# **to give way to** уступать (место); поддаваться.

glance [glɑːns] *n.* взгляд (мимолетный).# **at a glance** сразу.# **with a glance to** с учетом.

global ['gləʊbəl] *adj.* глобальный.@ 1. Об объекте программы – описанный на внешнем уровне и доступный всем компонентам программы. 2. О методе – применяемый к объекту в целом.@ **global control (GC)** глобальное управление.@ **global discretization error** полная ошибка дискретизации, полная ошибка усечения.@ **global identifier** глобальный идентификатор, глобальное имя.@ **global public key infrastructure (GPKI)** глобальная инфраструктура шифрования с открытым ключом.

global optimization ['gləʊbəl 'ɒptɪmaɪzɪʃən] глобальная оптимизация. @ 1. Оптимизация программы на уровне операторов и процедур: вынесение константных выражений из циклов, объединение общих последовательностей, выполнение смешанных вычислений. 2. Нахождение глобального минимума или максимума целевой функции.

global variable ['gləʊbəl 'vɛəriəbl] глобальная переменная.@ Переменная, описанная в объемлющем блоке; переменная, описанная на верхнем уровне.

go [ɡoʊ] *v.* (**went, gone**) 1. идти; 2. ехать; 3. делаться, становиться; 4. продолжаться (**on**).@ **go green** жарг переключаться с открытой на шифрованную связь.@ **go secure button** кнопка "включить защиту".# **to be going + inf.** собираться + *инф.*# **it goes like this** дело обстоит так.# **it goes without saying** само собой разумеется.# **as far as it goes** поскольку дело касается, что касается.

"**Gold Bug**" "Золотой жук" (рассказ американского писателя Э. По с описанием оригинального криптоаналитического исследования шифрованного текста).

Golomb's postulates = Golomb's randomness postulates

Golomb's randomness postulates критерии Голомба проверки случайности (двоичной последовательности).

good [ɡuːd] *adj.* стойкий.@ **good cipher** стойкий шифр.@ **good time** полезное время.

government Code and Cipher School (GC&CS) = Governmental School of Codes and Ciphers (GSC&C)

government ['ɡʌvnmənt] *n.* правительство.@ **government Communications Security Bureau** Бюро безопасности правительственной связи (Новой Зеландии).@ **government-endorsed encryptor** одобренный правительственным ведомством шифратор.

governmental ['gvʌnməntl] *adj.* правительственный.@ **governmental Communications Head-Quarters** Центр правительственной связи (Штаб-квартира правительственной связи) (английское правительственное ведомство, занимающееся перехватом и дешифрованием сообщений).@ **governmental School of Codes and Ciphers** Правительственная школа кодов и шифров (английское правительственное ведомство, занимавшееся перехватом и дешифрованием сообщений с 1919 по 1939 г.).

-gram [græm] в сложных и сложносоставных словах имеет значение — грамма.@ **N.-gram analysis** анализ *N.*-грамм.@ **N.-gram** *N.*-грамма.

G-random [dʒi:'rændəm] *adj.* G-случайный.@ **G-random binary sequence** G-случайная двоичная последовательность (двоичная последовательность называется G-случайной, если она удовлетворяет трем критериям случайности, сформулированным американским криптологом С. Голомбом в 1967г.).

grant ['gra:nt] *v.* 1. даровать; дарить; жаловать; 2. давать дотацию, предоставлять субсидию; 3. соглашаться, позволять; 4. допускать; *n.* 1. дар; дарственный акт; 2. дотация, субсидия; 3. *pl.* стипендия; 4. уступка, разрешение, согласие.# **for granted** без доказательства.# **to take for (as) granted** считать доказанным; принимать без доказательства.# **to take nothing for (as) granted** ничего не принимать на веру.

granularity *n.* гранулярность.

granularity ['grænjuləriti] *n.* 1. степень детализации; 2. гранулярность, грануляция.@ В параллельном программировании — характеристика программы, определяемая объемом неделимых параллельно выполняемых фрагментов.

graph [græf] *n.* 1. граф.@ Конечное множество вершин, соединенных ребрами. 2. график; диаграмма, номограмма, граф, вариант графемы.@ **graph follower** устройство ввода контурных графических изображений.@ **graph plotter** графопостроитель.@ **graph theory** теория графов.

graph(ic) data [g'ræf(ɪk) 'deɪtə] графическая информация.

grasp [gra:sp] *v.* 1. схватывать; 2. понимать.# **within grasp** в пределах досягаемости.

greatest bound ['greɪtɪst 'baʊnd] наибольшая нижняя граница.

greatest common divisor (GCD) ['greɪtɪst 'kɒmən dɪ'vaɪzə] наибольший общий делитель.

"Green Book" "Зеленая книга" (аналог американской "Оранжевой книги" в Англии).

grille [grɪl] *n.* решетка.@ **grille transposition** шифр перестановки на решетке.

grip [grɪp] *v.* 1. схватить; сжать; 2. понимать, постигать; 3. захватывать; *n.* зажим.# **to come to grips** подходить вплотную.

ground (gnd) [graʊnd] *n.* 1. заземление; 2. земля, почва; 3. основание; *v.* обосновывать; *adj.* основной.# **on the ground that** на том основании, что.

group [gru:p] *n.* группа.@ Множество, на котором определены ассоциативная операция и соответствующие ей единичный элемент и обратная опера-

ция. *v.* группировать. *adj.* групповой. @ **group choice** групповой выбор. @ **group code** групповой код. @ **group code recording** запись с использование группового кодирования. @ **group graph** граф группы. @ **group key** групповой ключ (предназначен для использования группой лиц). @ **group signature** групповая цифровая подпись. @ **group structure** групповая структура (про шифр говорят, что он имеет групповую структуру, если результат зашифрования открытого текста сначала на одном ключе, а затем повторного шифрования полученного шифртекста на втором эквивалентен шифрованию того же самого открытого текста на каком-то третьем ключе).

group mark [gru:p ma:k] метка группы. @ Элемент записи, указывающий начало или конец группы связанных полей.

grow [grou] *v.* (**grew, grown**) 1. расти; 2. делаться, становиться; 3. выращивать. # **to grow better (worse)** улучшаться (ухудшаться).

guard [ga:d] *v.* 1. охранять; 2. остерегаться; избегать (**against**); *n.* 1. предохранительное устройство; 2. дежурный. @ **guard band** защитная полоса. @ **guard bit** разряд защиты, бит защиты. @ **guard key** дежурный ключ (постоянно хранимый в криптографическом устройстве).

guard digit [ga:d 'diɔ:ɪt] разряды защиты. @ Дополнительные разряды промежуточных результатов, обеспечивающие сохранение точности.

guarded commands ['ga:ɪd kə'ma:nds] охраняемые команды. @ Управляющая структура, обобщающая условный оператор и оператор цикла с условием продолжения.

guess [ges] *n.* предположение, догадка; *v.* предполагать; угадывать. @ **guess a key** угадывать ключ. @ **guess plaintext attack** атака на основе угаданного открытого текста (атака на криптосистему с открытым ключом, в ходе которой атакующий угадывает открытый текст перехваченной криптограммы, шифрует его при помощи открытого ключа получателя и сравнивает с зашифрованным текстом).

guide [gaɪd] *n.* 1. руководство, путеводитель; 2. проводник, гид, экскурсовод; 3. ведущий принцип; 4. ориентир; 5. волновод; 6. световод, светопровод; *v.* 1. вести; 2. руководить, направлять.

Н*

hack *n.* = **hacking**

hack [hæk] *v.* заниматься хакерством, хачить.

hackee ['hæki:] *n.* женщина-"хакер".

hacker ['hækə] *n.* "хакер" (человек, прекрасно разбирающийся в компьютерах и способный вытворять с ними то, что другим кажется чистым волшебством, а том числе — находить пути обхода средств контроля доступа к компьютерным системам). @ **hacker-proof** защищенный от проникновения "хакеров". @ **hacker's trick** хакерский трюк.

hacking ['hækiŋ] *n.* хакинг, хак (получение информации из компьютера за счет обхода средств контроля доступа к ней).

Hadamard product произведение Адамара (поразрядное логическое умножение соответствующих членов двух последовательностей равной длины).@ **Hadamard product transform** преобразование Адамара.

Hagelin machine шифратор Хагелина.

half- [ha:f] в сложных и сложносоставных словах имеет значение полу-.@ **half-rotor** полуротор.

Hamming bound [ha:miŋ baund] граница Хемминга, граница сферической упаковки.

Hamming codes [ha:miŋ kouds] коды Хемминга.@ Семейство двоичных кодов совершенных кодов с исправлением ошибок связанных с именем Хемминга, но впервые описанные в 1942 г. математиком Р. Фишером. Они позволяют исправлять любую одиночную ошибку в блоке. При необходимости исправления кратных ошибок эти коды обобщаются, что приводит к кодам Боуза – Чоудрели – Хокенгема.

Hamming distance (metric) [ha:miŋ 'distəns] расстояние (метрика) Хемминга.

Hamming radius [ha:miŋ 'reidjəs] радиус Хемминга.

Hamming space [ha:miŋ speis] пространство Хемминга.@ В математической теории кодирования пространством Хемминга называют множество слов одинаковой длины, удаленность которых друг от друга измеряется расстоянием Хемминга. Размерность этого пространства равна числу разрядов слова, а координата по каждому измерению – значению соответствующего разряда слова. Сферой Хемминга называется множество слов из пространства Хемминга, для которых расстояние Хемминга от некоторого заданного слова («центра») не превышает некоторой заданной величины (радиуса Хемминга).

Hamming weight [ha:miŋ weit] вес Хемминга.@ **Hamming weight of a key** вес Хэмминга для ключа.

Hamming-weight attack = Hamming-weight cryptanalysis

Hamming-weight cryptanalysis криптоанализ с помощью веса Хэмминга (использует информацию о весе Хэмминга промежуточных значений, вычисляемых в ходе работы криптографического алгоритма).

hand [hænd] *n.* 1. рука; 2. прокрутка; *v.* передавать, вручать; *adj.* ручной.@ **hand cipher** ручной шифр.@ **hand-delivered key** ключ, доставляемый посыльным (курьером) .# **at hand** имеющийся (*близко под рукой*); рассматриваемый.# **in hand** имеющийся (*близко под рукой*); рассматриваемый.# **on hand** имеющийся (*близко под рукой*); рассматриваемый.# **to hand** имеющийся (*близко под рукой*); рассматриваемый.# **by hand** вручную.# **off hand** без подготовки, сразу.# **on all hands** со всех сторон.# **on the one (other) hand** с одной (другой) стороны.

hard [ha:d] *adj.* 1. постоянный, жесткий.@ Имеющий явное отражение в структуре информационного объекта (программы, файла, текста) и сохраняющийся в течение его существования. 2. трудный; 3. труднорешаемый (о математической задаче, для которой не существует алгоритма ее решения с полиномиальной сложностью); 4. твердый; тяжелый; *adv.* усиленно; упорно.@ **hard**

error постоянная ошибка. @ **hard integer** "трудное" целое число (целое, не обладающее большим количеством простых делителей, которые либо сами являются малыми по величине, либо имеют специальный вид, облегчающий их выделение). @ **hard-drive encryption program** программа шифрования информации на жестком диске. @ **hard-to-break cipher** трудновскрываемый шифр.

hard-to-invert function = one-way function (OWF)

hard copy [ha:d 'kɒpi] распечатка, документальная копия. @ Информация, выведенная из ЭВМ в виде распечатка или графика на бумагу или пленку.

hard disk [ha:d disk] жесткий диск. @ Запоминающее устройство с носителем в виде магнитного диска на металлической основе; обычно подразумевается винчестерский диск.

hard page break [ha:d peɪdʒ breɪk] «твердая» граница страницы. @ В системах подготовки текстов – переход на новую страницу, сохраняемый при изменении числа строк в документе.

hard space [ha:d speɪs] «твердый» пробел. @ В системах подготовки текстов – пробел, сохраняемый и не удлиняемый при форматировании.

hardware (HW, hdw) ['ha:dwɛə] *n.* 1. аппаратные средства, аппаратура, технические средства; 2. детали, оборудование; 3. металлические изделия. @ **hardware character generation** аппаратное формирование знаков. @ **hardware check** аппаратный контроль. @ **hardware circuitry** схемы аппаратных средств. @ **hardware compatibility** аппаратная совместимость. @ **hardware component** аппаратный компонент, составная часть аппаратуры. @ **hardware cracker** аппаратная система вскрытия (ключа, шифра). @ **hardware cryptoalgorithm-cracker** аппаратная система вскрытия криптоалгоритма. @ **hardware cracker** аппаратная система вскрытия (ключа, шифра). @ **hardware description** описание аппаратных средств. @ **hardware division** аппаратное деление. @ **hardware encryption** аппаратные средства шифрования (аппаратное шифрование). @ **hardware error** аппаратная ошибка, ошибка в аппаратуре. @ **hardware key** 1. ключ аппаратного шифрования; 2. ключ, вмонтированный в криптографическое устройство; 3. аппаратно генерируемый ключ. @ **hardware language** машинный язык, язык реализации. @ **hardware malfunction** аппаратная ошибка, неправильная работа оборудования. @ **hardware multiplication** аппаратное умножение. @ **hardware random number generator** аппаратно реализованный генератор случайных чисел. @ **hardware representation** аппаратное представление. @ **hardware sprite** аппаратный спрайт. @ **hardware stack** аппаратный стек. @ **hardware support** аппаратная поддержка; аппаратная реализация. @ **hard-copy key** ключ, записанный на твердом носителе (перфокарте, магнитном диске и т.д.). @ **hard-copy keying** ввод ключа с твердого носителя (перфокарты, магнитного диска и т.д.).

hardware compatible ['ha:dwɛə kəm'pætəbl] аппаратно-совместимый. @ Об устройствах с конструктивными взаимозаменяемыми узлами или об устройствах, допускающих сопряжение.

hardware environment ['ha:dwɛə in'vaɪənmənt] аппаратная среда. @ Аппаратные средства, используемые при выполнении программ.

hardware interrupt ['ha:dwɛə ,intə'rʌpt] аппаратное прерывание. @ Прерывание по ошибке при выполнении команды или прерывание от внешнего устройства.

hardware reliability ['ha:dwɛə rɪlaɪə'bɪlɪtɪ] надежность аппаратуры. @ Характеристика способности аппаратуры осуществлять свои функции в течении некоторого периода времени, обычно выражаемая через среднюю наработку на отказ.

hardware security ['ha:dwɛə sɪ'kjuəritɪ] аппаратная защита. @ Использование аппаратных средств, например регистров границ или замков и ключей для защиты данных в ЭВМ.

hardware-assisted encryption = hardware encryption

hardware-based key = hardware key

hardware-implemented encryption = hardware encryption

hardwired ['ha:dwɛəd] *adj.* постоянно (жестко) вмонтированный; постоянно запаянный; "защитый", реализованный аппаратными средствами. @ **hardwired key entry** ввод ключа методом постоянного монтажа (в аппаратуре).

hash(ing) function ['hæʃ(ɪŋ) 'fʌŋkʃən] функция расстановки, функция хеширования; хеш-функция.

hashing ['hæʃɪŋ] *n.* хеширование. @ Способ организации структур данных (хеш-таблиц), обеспечивающий эффективный поиск и пополнение; положение элемента данных в хеш-таблице определяется значением функции расстановки, отображающей множество ключей элементов данных в множество индексов таблицы и обеспечивающий равномерное заполнение. @ **hashing algorithm** алгоритм хеширования.

have [hæv] *v.* (**had**) иметь. # **to have a bearing on (upon)** иметь отношение к; оказывать влияние на. # **to have an effect on** влиять на. # **to have in mind** помнить; иметь в виду. # **to have in view** иметь в виду. # **to have nothing to do with** не иметь ничего общего с. # **to have recourse to** прибегать к помощи. # **to have regard to** учитывать, обращать внимание на. # **to have to do with** иметь дело с; иметь отношение к. # **to have + inf.** быть должным, вынужденным (что-л. сделать).

hazard ['hæzəd] *n.* 1. опасность; 2. шанс; 2. риск; *v.* рисковать; осмеливаться, отваживаться. # **at all hazards** во что бы то ни стало.

header ['hedə] *n.* 1. заголовок. @ 1. Управляющая часть файла, сообщения или записи, расположенная до информационной части. 2. Часть информационного объекта, содержащая его внешнее описание. 2. колонтитул, шапка (*страницы*). @ **header encryption** шифрование заголовка (сообщения).

heading ['hedɪŋ] *n.* заголовок, рубрика, «шапка».

help [help] *n.* 1. подсказка, диалоговая документация; 2. помощь; *v.* помогать. # **one cannot help + ing.-form** нельзя не + *инф.*

hexadecimal (hex.) ['heksədɛsɪməl] *adj.* шестнадцатеричный. @ **hexadecimal key** шестнадцатеричный ключ (представленный в шестнадцатеричной форме). @ **hexadecimal digit** шестнадцатеричная цифра (0 1 2 3 4 5 6 7 8 9 A B

C L E F).@ **hexadecimal multiplication** умножение в шестнадцатеричной системе счисления (шестнадцатеричное умножение).@ **hexadecimal notation** шестнадцатеричная система счисления.

hexadecimal format ['heksədəsiməl 'fɒmət] шестнадцатеричный формат.@ Формат с представлением данных в шестнадцатеричной форме.

hidden-key cryptography *n.* = **secret-key cryptography**

hierarchy ['haɪərə:kɪ] *n.* 1. иерархия.@ 1. Принцип организации, состоящий в том, что целевое рассматривается как состоящее из частей, каждая из которых сама является целым, состоящим из своих частей, и т. д. 2. Многоуровневая древовидная структура с отношениями подчиненности сверху вниз. В реальных системах встречаются различные отступления от идеальной иерархической структуры: связь только с одним элементом нижнего уровня («синекура»); связь более чем с одним элементом высшего уровня («двойное подчинение»); связь с высшим уровнем помимо непосредственного верхнего («дислокация»); более одного элемента на самом верху («незавершенность»); связь сверху вниз с элементами разных уровней («неоднородность»); связь между элементами одного уровня («зависимость»); связь с окружающей средой помимо верхнего уровня («нарушение субординации»), и их комбинации. 2. соподчинение.@ **hierarchy of functions** иерархия функций.@ **hierarchy of programs** иерархия программ.@ **hierarchy of sets** иерархия множеств.@ **hierarchy of storage** иерархия накопления информации.

hierarchy of keys = **key hierarchy**

high [haɪ] *adj.* 1. старший.@ 1. О разряде или байте – самый левый, представляющий старшую цифру числа. 2. Об области памяти – имеющий больший адрес. 2. высокий; *adv.* высоко.# **high in** с высоким содержанием чего-л..# **as high as** до (обычно перед цифрами).# **half as high** в два раза ниже.# **twice as high** в два раза выше.

high- [haɪ] в сложных и сложносоставных словах имеет значение высоко-.@ **high-frequency** *adj.* высокочастотный.@ **high-grade** *adj.* первоклассный; высокого уровня.@ **high-grade cryptosecurity** криптостопкость высокого уровня.@ **high-grade military communications** сообщения (переписка) высшего военного командования.@ **high-security** *adj.* высокостойкий, обладающий высокой стойкостью.@ **high-security cipher** шифр высокой стойкости.@ **high-security key** высокостойкий ключ.@ **high-speed** *adj.* высокоскоростной.@ **high-speed cryptography** высокоскоростная криптография.

high-level *adj.* = **high-grade**

high-level data link control (HDLC) [haɪ'levl 'deɪtə lɪnk kən'troul] высокоуровневый протокол управления каналом.@ Предложенный ISO стандарт канального протокола.

highest [haɪst] *superl* наивысший.@ **highest frequency letter** буква с наивысшей частотой встречаемости (в тексте).@ **highest order** самый старший разряд.

Hill cipher system шифрсистема Хилла (с помощью алгебраической процедуры, описанной Л. Хиллом в 1929 г., производится шифрование открытого текста порциями по n букв, где n - произвольное положительное целое).

hinge [hɪŋdʒ] *v.* 1. висеть (на петлях); 2. зависеть от (**on, upon**); *n.* петля; шарнир. # **off the hinges** в беспорядке, в расстройстве.

historical [hɪs'tɒrɪkəl] *adj.* исторический, связанный с историей. @ **historical work characteristic** *n.* достигнутая оценка рабочей характеристики (средний объем работы, необходимой для нахождения ключа шифра на основе знания n знаков шифртекста при использовании наилучшего из известных методов анализа данного шифра).

history ['hɪstəri] *n.* 1. история; 2. развитие; изменение. # **previous history** предистория.

hit [hɪt] *v.* 1. ударять; 2. попадать в цель. # **bin hit and miss fashion** наугад.

hobbyist ['hɒbɪst] *adj.* любительский, непрофессиональный. @ **hobbyist cipher** любительский шифр.

hold ['hould] *v.* (**held**) 1. держать; 2. содержать, вмещать; 3. полагать, считать; 4. иметь силу, быть справедливым (**for**); 5. проводить (*собрание, конференцию*); 6. придерживаться. # **to hold true (good)** быть справедливым (действительным). # **to take hold of** ухватиться, воспользоваться.

home [həʊm] *n.* 1. начало (экрана). @ Левый верхний угол экрана дисплея. 2. дом; *adj.* 1. домашний; 2. внутренний. # **to bring home to** убедить кого-л., довести до сознания. # **to feel at home** хорошо разбираться в чем-л.

homogeneous [həmə'dʒiːnjəs] *adj.* однородный. @ **homogeneous cipher** однородный шифр. @ **homogeneous equation** однородное уравнение.

homomorphism [həmə'mɔːfɪzəm] *n.* гомоморфизм (от греч. homos — равный, одинаковый, взаимный, общий), часть сложных слов, означающая: сходный, единый, принадлежащий к одному и тому же.

homophone ['hɒməfəʊ] гомофон.

homophonic ['hɒməfəʊnɪk] *adj.* гомофонический. @ **homophonic cipher** гомофонический шифр (при замене одного знака открытого текста выбор осуществляется из нескольких знаков шифртекста). @ **homophonic substitution** гомофонная замена.

hop [hɒp] *n.* скачкообразное изменение. @ **hostile** *adj.* враждебно настроенный.

hostile ['hɒstəl] 1. злоумышленник 2. враг. @ **hostile outsider** посторонний злоумышленник.

hotline ['hɒtlaɪn] *n.* линия экстренной связи. @ **hotline between Moscow and Washington** линия экстренной связи между Москвой и Вашингтоном

hours ['aʊəs] *n.* время работы.

however [haʊ'evə] *conj.* однако; *adv.* как бы ни. # **however much** сколько бы ни.

human ['hjuːmən] *adj.* человеческий. @ **human being** существо, человек. @ **human bias** 1. субъективная ошибка; 2. систематическое отклонение, вносимое

оператором.@ **human engineering** инженерная психология; эргономика.@ **human intelligence (HUMINT)** агентурная разведка.

human failure ['hju:mən 'feɪljə] отказ.@ Отказ по вине обслуживающего персонала.

human-computer interface ['hju:mən,kəm'pjʊ:tə ,intə'feɪs] пользовательский интерфейс, человеко-машинный интерфейс.@ Средства связи человека и вычислительной системы, включающие в себя, в частности, устройства ввода-вывода и вспомогательное программное обеспечение.

"hut" [hʌt] *n.* "барак" (так назывались административные здания на территории поместья Блетчли-Парк, в которых во время второй мировой войны размещались подразделения английской дешифровальной службы, занимавшейся чтением немецкой шифрпереписки).

hybrid ['haɪbrɪd] *adj.* гибридный.@ **hybrid cryptosystem** гибридная криптосистема.@ Гибридные криптосистемы сочетают принципы как симметричных, так и ассиметричных систем (криптосистема с открытым ключом задеируется только для управления общими ключами, которые затем используются в традиционных криптосистемах с секретным ключом).@ **hybrid computer** гибридная ЭВМ.@ Вычислительная система, содержащая как аналоговые, так и цифровые устройства.

hybrid public-secret key cryptosystem = hybrid cryptosystem

hyperbola [ˌhaɪ'pəbələ] *n.* гипербола.

hyperbolic [ˌhaɪpə'bɒlɪk] *adj.* гиперболический.@ **hyperbolic equation** гиперболическое уравнение.@ **hyperbolic function** гиперболическая функция.@ **hyperbolic logarithm** натуральный логарифм.@ **hyperbolic measure** гиперболическая мера.

hypergeometric ['haɪpə,dʒɪə'metɪk] *adj.* гипергеометрический.

hyphenation ['haɪfəneɪʃən] *n.* перенос, разделение слов для переноса.

hypotheses ['haɪ'pɒθɪsɪːz] *pl.* от **hypothesis**

hypothesis ['haɪ'pɒθɪsɪs] *n.* гипотеза, предположение.@ 1. Форма развития науки. 2. Предложение; утверждение, требующее доказательства или проверки.@ **hypothesis-testing problem** задача проверки гипотез.

I*

ideal [aɪ'diəl] *adj.* 1. идеальный; 2. воображаемый.

idealize [aɪ'diəlaɪz] *v.* идеализировать.

ideally [aɪ'diəl] *adv.* в идеальном случае.

identical [aɪ'dentɪkəl] *adj.* идентичный, тождественный.

identification (ID, id) [aɪ'dentɪfɪ'keɪʃən] *n.* идентификация, отождествление, определение, опознание, обозначение.@ Процесс отождествления объекта с одним из известных системе объектов. В сети передачи данных – опознавание выдавшего запрос пользователя, канала или процесса. 2. метка, определяющая

объект (например, надпись на катушке магнитной ленты).@ **identifications division** раздел идентификации.

identifier [aɪ'dentɪfaɪə] *n.* 1. идентификатор.@ Строка символов, обозначающая или именуемая объект программы или вычислительной системы. 2. устройство опознавания.@ **identifier list** список идентификаторов.

identify (ID, id) [aɪ'dentɪfaɪ] *v.* 1. идентифицировать, распознавать. 2. обозначать, именовать, идентифицировать; 3. отождествлять; *n.* 1. тождество, идентичность; 2. идентификация (личности).

identity [aɪ'dentɪti] *n.* 1. тождество; 2. тождественность, идентичность; подлинность; 3. личность; индивидуальность; *adj.* опознавательный, личный.@ **identity burst** блок идентификации.@ **identity element** нейтральный элемент.@ **identity function** функция тождества.@ **identity a key** устанавливать (определять) ключ.@ **identity transformation** тождественное преобразование.@ **identity-based cryptosystem** идентификационная криптосистема (криптосистема на основе идентификационной информации).@ **identification friend or foe system** система опознавания "свой-чужой".@ **identification of a cipher system** определение шифрсистемы.@ **identification of a plaintext** выявление открытого текста.

identity matrix [aɪ'dentɪti 'meɪtrɪks] единичная матрица.@ Диагональная матрица с единичными диагональными элементами.

ideal [aɪ'diəl] *adj.* 1. идеальный; 2. воображаемый.@ **ideal cipher** идеальный шифр (с бесконечным расстоянием единственности).

idealize [aɪ'diələɪz] *v.* идеализировать.

ideally [aɪ'diəl] *adv.* в идеальном случае.

idempotent [aɪdem pə'tenpə'tent] *adj.* идемпотентный.@ **idempotent element** идемпотентный элемент (элемент кольца, равный своему квадрату).

idiomorph *n.* = **word pattern**

idle [aɪdl] *adj.* бездействующий, простаивающий.@ **idle mode** холостой режим ожидания).

if [ɪf] *conj.* 1. если; 2. является вводным словом в косвенном вопросе и переводится как «ли».# **as if** как будто, как если бы.# **if any (anything)** если вообще (имеется, требуется и т. п.).# **if at all** если вообще (имеется, требуется и т. п.).# **if ever** если это вообще (имеет место).# **if for no other reason than** хотя бы потому, что.

image ['ɪmɪdʒ] *n.* 1. изображение.@ В машинной графике – представление изображения, обрабатываемое программами. 2. образ.@ Логическая копия данных, имеющих в другом месте или в другом представлении. 3. загрузочный модуль; образ задачи; 4. подобие.# **to speak in image** говорить образно.

immune [ɪ'mju:n] *adj.* стойкий.@ **immune to linear cryptanalysis** стойкий против линейного криптоанализа.

immunization [ɪ'mju:naɪ'zeɪʃən] *n.* повышение криптостойкости.

impenetrable [ɪm'penɪtrəbl] *adj.* сверхстойкий.@ **impenetrable cryptosystem** сверхстойкая криптосистема.

imperfect [ɪm'pə:fɪkt] *adj.* 1. дефектный; 2. неполный; 3. недостаточный; 4. несовершенный. @ **imperfect cipher** несовершенный шифр.

imperfection [ɪm'pə:fɪkʃən] *n.* 1. дефект; 2. искажение; 3. возмущение поля

impersonate a sender выдавать себя за отправителя (сообщения).

impersonate [ɪm'pə:səneɪt] *v.* выдавать себя за (кого-то). @ **impersonation attack** попытка имитации (атака с изменением авторства).

impersonation [ɪm'pə:səneɪʃən] *n.* изменение авторства, имитация. @ **impersonation of a transmitter** имитация передатчика (тип угрозы в теории аутентификации информации).

implant [ɪm'plɑ:nt] *n.* закладка (электронное устройство для получения несанкционированного доступа к электромагнитным излучениям, которые содержат информацию о ключах, открытых текстах и алгоритмах функционирования криптографического оборудования).

implementation [ɪm'plɑ:nteɪʃən] *n.* реализация, внедрение. @ **implementation of a cryptoalgorithm** реализация криптоалгоритма (программными или аппаратными средствами). @ **implementation-specific timing characteristics** зависящие от реализации временные характеристики (криптосистемы).

implemented [ɪm'plɑ:ntɪd] *adj.* реализованный.

impossible *adj.* неосуществимый, невыполнимый, находящийся за пределами возможного.

impossible cryptanalysis криптоанализ на основе событий с нулевой вероятностью (разновидность дифференциального криптоанализа).

impossible-to-break неподдающийся вскрытию (абсолютно стойкий).

impostor *n.* самозванец; человек, выдающий себя за другое лицо.

impression [ɪm'presʃən] *n.* 1. впечатление; 2. отпечаток. # **one has the impression** создается впечатление. # **to convey the impression** создавать впечатление.

improper [ɪm'prɒpə] *adj.* 1. несобственный; 2. неправильный (о дроби). @ **improper encryption** неправильное шифрование.

in prep [ɪn prep] (указывает на способ выражения, форму представления и т.д.). @ **in prep cipher** шифрованный (зашифрованный). @ **in prep clear** клером (открытым текстом). @ **in prep code** кодированный (закодированный).

in prep black жарг = **in prep cipher**

in prep red = **in prep clear**

in prep the clear = **in prep clear**

in so far as [ɪn sou fa: əz] *adv.* поскольку. # **in so far as ... is concerned** что касается ,когда речь идет о.

in-built [ɪn'bɪld] *adj.* встроенный, вмонтированный.

incidence ['ɪnsɪdəns] *n.* инцидентность. @ **incidence matrix of authenticating rules** матрица инцидентности при данных правилах аутентификации.

in-circuit [ɪn'sə:kɪt] *adj.* оперативный, линейный. @ **in-circuit encryption device** прибор оперативного (линейного) шифрования.

in-coming ['ɪn.kʌmɪŋ] *n.* 1. вход; 2. доходы; *adj.* 1. входной, входящий, поступающий; 2. наступающий; следующий; 3. вступающий. @ **in-coming data** входные данные. @ **in-coming message** входное сообщение.

indecipherable *adj.* = **undecipherable**

index ['ɪndeks] *n.* 1. индекс. @ 1. Структура данных, обеспечивающая доступ к записи по ключу. 2. Выражение, указывающее номер элемента массива. 2. перемещение текущей позиции вниз (*в обработке текста*). 3. показатель степени коэффициента; 4. алфавитный указатель; *v.* индексировать, формировать индекс, снабжать указателем, составлять указатель. @ **index buffer** буферный индекс-регистр. @ **index of a point to a curve** порядок точки относительно кривой. @ **index of a radical** показатель корня. @ **index of coincidence (IC)** индекс совпадения. @ **index of cryptographic strength** показатель криптографической стойкости. @ **index of dispersion** 1. характеристика однородности выборки; 2. индекс рассеяния. @ **index point** индексная позиция. @ **index sequential access method (ISAM)** индексно-последовательный метод доступа. @ **index word** модификатор. @ **indexed sequential processing (ISP)** индексно-последовательная обработка информации.

index mode ['ɪndeks moʊd] режим индексации. @ Выполнение машинной команды с использованием индексной адресации.

index register ['ɪndeks 'redʒɪstə] индексный регистр. @ Регистр центрального процессора, значение которого используется командами с индексной адресацией.

indexed addressing ['ɪndekst ə'dresɪŋ] индексная адресация. @ Способ адресации, при котором исполнительный адрес равен сумме содержимого индексного регистра и базы, заданной в команде.

indexed file ['ɪndekst faɪl] индексированный файл. @ Файл, для доступа к записям которого имеется индекс.

indexed sequential file ['ɪndekst sɪ'kwɛnsjəl faɪl] индексно-последовательный файл. @ Файл, сочетающий свойства файлов с произвольной выборкой и последовательных файлов.

indicative [ɪn'dɪkətɪv] *adj.* показательный, характерный, свидетельствующий о (of). # **to be indicative of** указывать на.

indicator ['ɪndɪkətə] *n.* 1. признак, флаг; 2. индикатор, индикаторный регистр, указатель. @ **indicator sequence** индикаторная последовательность (вектор-индикатор).

indirect [ɪndɪ'rekt] *adj.* 1. косвенный; 2. побочный; дополнительный. @ **indirect eavesdropping** косвенный перехват (напр, с помощью приема электромагнитного излучения работающих радиоэлектронных устройств). @ **indirect encryption** шифрование программными средствами. @ **indirect file** командный файл. @ **indirect proof** косвенное доказательство. @ **indirect sampling** косвенный выбор. @ **indirect symmetry technique** метод косвенной симметрии (применяется для вскрытия шифров периодической многоалфавитной заме-

ны).@ **indirect with autoincrement ad-dressing** косвенная адресация с автоувеличением.

indirect symmetry method = **indirect symmetry technique**

indirect address [ˌɪndɪ'rekt ə'dres] косвенный адрес.@ Адрес слова, содержащего фактический адрес.

indirect addressing [ˌɪndɪ'rekt ə'dresɪŋ] косвенная адресация.@ Способ адресации при котором исполнительный адрес равен содержимому слова по адресу, указанному в команде.

indivisible *adj.* = **prime**

industry ['ɪndʌstri] *n.* 1. промышленность; 2. *pl.* отрасли промышленности.# **home industry** отечественная промышленность.

infallible [ɪn'fæləbl] *adj.* надежный.@ **infallible cipher** надежный шифр.

infeasible [ɪn'fiːzəbl] *adj.* неосуществимый, невыполнимый.

inference ['ɪnfərəns] *n.* 1. (логический) вывод, умозаключение; следствие; 2. заключение, вывод.# **to draw an inference** делать вывод, выводить заключение.

inferior [ɪn'fɪəriə] *adj.* 1. низший; 2. худший; плохой.# **to be inferior (to)** уступать, быть хуже.

infinite ['ɪnɪtɪt] *adj.* 1. бесконечный, безграничный; 2. несметный, бесчисленный.@ **infinite random key** бесконечный случайный ключ.@ **infinite graph** бесконечный граф. .@ **infinite random key** бесконечный случайный ключ.@ **infinite impulse response (IIR)** импульсная характеристика бесконечной длительности.@ **infinite product** бесконечное произведение.@ **infinite sequence** бесконечная последовательность.@ **infinite series** бесконечный ряд.

infinitely ['ɪnɪtɪtli] *adv.* бесконечно, неограниченно.

infinitesimal [ˌɪnfɪni'tesɪməl] *adj.* бесконечно малый.

infinitesimal neighbourhood [ˌɪnfɪni'tesɪməl 'neɪbəhʊd] бесконечно малая окрестность.

infinity [ɪn'fɪnɪti] *n.* бесконечность; безграничность.

information (inf) [ˌɪnfə'meɪʃən] *n.* информация.@ 1. Сведения, неизвестные до их получения. 2. В обычной речи – любые сведения, известия, сообщения, новости и т. п. 3. В научно-технических приложениях – то, что несет на себе сигнал. 4. Как философская категория – всеобщее свойство материи, являющееся аспектом свойства отражения, допускающим количественное описание. 2. значения, приписываемые данным; 3. данные.@ **information authentication** аутентификация информации.@ **information bit** информационный разряд.@ **information capacity** информационная емкость.@ **information carrier** носитель информации.@ **information channel** канал связи, информационный канал.@ **information conveyed by a message** содержание сообщения.@ **information density** плотность информации.@ **information destination** приемник информации.@ **information display rate** скорость воспроизведения информации.@ **information exchange system (IES)** система информационного обмена.@ **information gain** прирост информации.@ **information generator** 1. гене-

ратор данных; 2. источник информации. @ **information handling** обработка информации. @ **information authentication** аутентификация информации. @ **information hiding** сокрытие информации. @ **information loss** потери информации. @ **information management system (IMS)** 1. информационная система; 2. система управления базами данных. @ **information message** информационное сообщение (*в отличие от служебного или управляющего сообщения*). @ **information processing** обработка информации (данных). @ **information rate** скорость передачи или поступления информации. @ **information register** информационный регистр. @ **information retrieval language** информационно-поисковый язык. @ **information retrieval problem** проблема (задача) поиска информации. @ **information retrieval system** информационно-поисковая система. @ **information retrieval** информационный поиск, поиск информации. @ **information separator (IS)** разделитель информации. @ **information source** источник информации. @ **information storage and retrieval** хранение и поиск информации. @ **information structure** информационный объект. @ **information transfer scheme** схема передачи информации. @ **information unit** единица количества информации. @ **information word** информационное слово. @ **information(al) language** информационный язык. @ **information-bearing emission** излучение (работающей радиоэлектронной аппаратуры), несущее информацию. @ **information-logical machine** информационно-логическая вычислительная машина. @ **information-processing machine** вычислительная машина для обработки информации. @ **information-processing system** 1. информационная система обработки данных; 2. устройство для обработки данных; 3. информационная система. @ **information theory cryptography** криптография на основе теории информации. @ **information-theoretic security** теоретико-информационная стойкость. @ **information security (INFOSEC)** защита (безопасность) информации. @ **information war (infowar)** информационная война.

information character [ˌɪnfəˈmeɪʃən ˈkærɪktə] информационный символ, текстовый символ. @ Символ сообщения, являющийся частью его содержания, в отличие от управляющего символа или разделителя.

information feedback system [ˌɪnfəˈmeɪʃən ˈfiːdˌbæk ˈsɪstɪm] информационная система с обратной связью. @ Система обработки данных или информации с обратной связью для контроля ошибок.

Information Management System (IMS). @ Иерархическая система управления базами данных, разработанная фирмой IBM.

information system [ˌɪnfəˈmeɪʃən ˈsɪstɪm] информационная система. @ Вычислительная система, обеспечивающая доступ пользователей и программ к общей информации.

information technology (IT) [ˌɪnfəˈmeɪʃən tekˈnɒlədʒɪ] информационная техника. @ Технические средства обработки, хранения и передачи информации, их применение и создание.

information theory [ˌɪnfəˈmeɪʃən ˈθɪəri] теория информации. @ Математическая дисциплина, изучающая количественные и качественные свойства информации.

informative [ˌɪnfəˈmeɪtɪv] *adj.* 1. информативный, информационный, информирующий; 2. содержательный; 3. поучительный.

inherent [ɪnˈhɪərənt] *adj.* вмонтированный, встроенный; присущий; свойственный; неотъемлемый; собственный. @ **inherent addressing** неявная адресация. @ **inherent bias** неустранимое смещение. @ **inherent key** встроенный (вмонтированный) (в схему криптографического устройства) ключ.

inherent model [ɪnˈhɪərənt ˈmɒdl] модель ингерентная. @ Модель, согласованная с окружающей культурной средой, входящая в нее не как чуждый ей элемент, а как ее естественная часть.

inherently [ɪnˈhɪərəntli] *adv.* по существу, по своей природе.

inherently ambiguous language [ɪnˈhɪərəntli æmˈbɪɡjuəs ˈlæŋɡwɪdʒ] существенно неоднозначный язык. @ Бесконтекстный язык, для которого не существует однозначной грамматики.

inherit [ɪnˈherɪt] *v.* наследовать; унаследовать.

inheritance [ɪnˈherɪtəns] *n.* наследственность; наследование.

inheritance hierarchy [ɪnˈherɪtəns ˈhaɪərəːki] иерархия наследования. @ В представлении знаний – иерархическая организация единиц представления, при которой при отсутствии информации о некотором свойстве видового понятия или экземпляра используется описание этого свойства для родового понятия.

inherited error [ɪnˈherɪtɪd ˈerə] 1. унаследованная ошибка. @ Ошибка, вызванная неточностью исходных данных или ранее выполненных операций. 2. ошибка в исходных данных.

inhibit [ɪnˈhɪbɪt] *v.* 1. запрещать, блокировать; 2. препятствовать; 3. сдерживать; задерживать; тормозить; *n.* запрет. @ Предотвращение возможности осуществления события, например, использование логического вентиля для запрета прохождения другого сигнала. @ **inhibit circuit** схема запрета. @ **inhibit input (inh)** запрещающий входной сигнал.

inhibiting input [ɪnˈhɪbɪtɪŋ ˈɪnpʊt] запрещающий вход.

inhibitory action [ɪnˈhɪbɪtəri ˈækʃən] запрещающее действие, запрещение, задерживающее действие.

initial [ɪˈnɪʃəl] *adj.* начальный; первоначальный. @ **initial address** начальный адрес. @ **initial algebra** начальная алгебра. @ **initial conditions** 1. начальные условия; 2. исходные данные; 3. режим исходного состояния. @ **initial data** исходные данные. @ **initial fill** начальное заполнение (регистра сдвига). @ **initial input program** начальная программа ввода. @ **initial key** 1. начальный ключ; 2. ключ инициализации (криптосистемы). @ **initial key load** начальная загрузка (начальное заполнение) ключей. @ **initial permutation (IP)** начальная перестановка. @ **initial key permutation** начальная перестановка ключей (в DES-алгоритме). @ **initial key state** начальное состояние ключей (напр, шифра-

тора).@ **initial order** начальная команда.@ **initial program load** начальная загрузка.@ **initial program loader (IPL)** начальный загрузчик, программа начальной загрузки.@ **initial state** начальное состояние.@ **initial value problem** задача с начальными значениями, задача Коши.@ **initial value** начальное значение.

initial program load [ˈɪnɪʃəl ˈprəʊgræm laʊd] начальная загрузка программы.@ Загрузка операционной системы в «пустую» машину.

initialization [ˈɪnɪʃɪəlaɪzɪʃən] *n.* 1. инициализация, инициирование; 2. начальное заполнение; начальная загрузка.@ 1. Присваивание начальных значений переменным программы. 2. Разметка диска и запись на него управляющей информации.@ **initialization communication** начать сеанс связи.@ **initialization vector (IV)** вектор начального заполнения.

initialize [ˈɪnɪʃɪəlaɪz] *v.* инициализировать.

initializer [ˈɪnɪʃɪəlaɪzə] *n.* инициализатор.@ Выражение, описывающее начальные значения переменной или переменных.

initiate [ˈɪnɪʃɪət] *v.* 1. положить начало; 2. возникнуть.

initiation *n.* = **initialization**

inject [ɪnˈdʒekt] *v.* вводить.@ **inject a key** вводить ключ.

injection [ɪnˈdʒektʃən] *n.* ввод (напр, ключа).

injector [ɪnˈdʒektə] *n.* устройство ввода.

in-line *adj.* = **on-line**

in-phase [ɪnˈfeɪz] *adj.* совпадающий по фазе.@ **in-phase autocorrelation** совпадающая по фазе автокорреляция.

input [ˈɪnpʊt] *n.* вход; *adj.* входной.@ **input alphabet** входной алфавит.@ **input message** входное сообщение.@ **input sequence** входная последовательность.@ **input transformation** входное преобразование (блока шифртекста).

insecure [ˈɪnsɪˈkjuə] *adj.* 1. нестойкий; 2. защищенный.@ **insecure channel** незащищенный канал (связи).@ **insecure cryptosystem** нестойкая криптосистема.

insert [ɪnˈsɜ:t] *v.* 1. вставлять; вводить; вносить; 2. подключать.@ **insert a key** вводить (устанавливать) ключ.@ **insert oneself into a communications link** подключаться к линии связи.

inserted [ˈɪnˈsɜ:tɪd] *adj.* введенный, установленный (в криптографическое устройство).@ **inserted key** введенный (установленный) (в криптографическое устройство) ключ.

insertion [ˈɪnˈsɜ:ʃən] *n.* ввод; вставка.

insider deceit = **insider cheating**

insider [ˈɪnˈsaɪdə] *n.* свой (человек).@ **insider cheating** обман со стороны своего.

insight [ˈɪnsaɪt] *n.* проникновение (**into**); понимание, представление; озарение.# **to gain an insight into** проникнуть в сущность чего-л.; понять.# **to provide insight into** дать представление о.

install [ɪn'stɔ:l] *v.* 1. устанавливать, настраивать.@ Задавать параметры и состав программной системы для работы на конкретной вычислительной машине. 2. устанавливать, включать.@ Делать задачу доступной в данной операционной среде. 3. устанавливать, монтировать (*сменный носитель на внешнее запоминающее устройство*); 4. устанавливать; налаживать (*вычислительную систему*), вводить в действие.@ **install individual keys on computers** вводить в действие индивидуальные ключи на компьютерах.

installation [ɪn'stə'leɪʃən] *n.* 1. установка, настройка; 2. вычислительная система, ЭВМ; 3. монтаж, ввод в строй, расположение, размещение, инсталляция (напр, ключа).@ **installation and checkout phase** опытная эксплуатация.

installed task [ɪn'stɔ:ld ta:sk] инсталлированная задача, включенная задача.@ Задача, информация о параметрах и расположения загрузочного модуля которой занесена в таблицы операционной системы. Вызов инсталлированной задачи не требует поиска в каталогах.

installator [ɪn'stə'leɪə] *n.* лицо, осуществляющее установку (инсталляцию).

installed *adj.* = **inserted**

instance ['ɪnstəns] *n.* 1. экземпляр (*объекта некоторого типа*); 2. пример; отдельный факт, случай; 3. требование; просьба; *v.* приводить в качестве примера.# **at the instance of** по требованию; по просьбе.# **for instance** например.# **in the first instance** сначала; прежде всего.

instant ['ɪnstənt] *n.* мгновение, момент; *adj.* 1. неотложный; немедленный; 2. текущий, текущего месяца.# **the instant** в тот момент, когда.

instantaneous [ɪnstən'teɪnjəs] *adj.* мгновенный.@ **instantaneous encipherer** шифратор мгновенного действия.

instantaneously [ɪnstən'teɪnjəsli] немедленно (декодируемый); мгновенно.

instantiate [ɪn'stən'teɪt] *v.* создавать экземпляр (*объекта некоторого типа*).

instantiation [ɪn'stən'teɪʃən] *n.* 1. экземпляр, реализация (*некоторого абстрактного описания*); конкретизация; 2. создание экземпляра (*объекта некоторого типа*).

integrity [ɪn'tegriti] *n.* целостность, сохранность, защищенность (состояние, в котором данные используются только установленным образом).@ Способность противостоять изменениям при системных ошибках.@ **integrity of a key against substitution or alteration** защищенность ключа от подмены или изменения.@ **integrity of information** целостность (сохранность) информации.

integro-differential equation [ɪn'tegrɔ,dɪfə'renʃəl ɪ'kweɪʃən] интегро-дифференциальное уравнение.

intellect ['ɪntlekt] *n.* 1. интеллект, ум, рассудок; 2. интеллект.@ 1. Интеллект естественный; внутренне – способность к абстракции; внешне – способность ориентироваться в незнакомых условиях и находить решение слабо формализованных задач. 2. Интеллект искусственный – техническая имитация определенных возможностей естественного интеллекта (например, узнавания,

образования понятий, принятия решений, синтеза речевых и эстетических сигналов и т. п.).

intelligence [ɪn'telɪdʒəns] *n.* 1. интеллект; 2. «интеллект». @ Программы, управляющие устройством. 3. сведения.

intelligent [ɪn'telɪdʒənt] *adj.* 1. интеллектуальный. @ Представляющий большие возможности, чем другие устройства или программы того же класса; 2. использующий микропроцессор; 3. умный; 4. эрудированный; 4. умелый.

intelligent control [ɪn'telɪdʒənt kən'troul] управление с искусственным интеллектом.

intelligent controller [ɪn'telɪdʒənt kən'troulə] интеллектуальный контроллер. @ Контроллер, выполняющий, кроме непосредственного управления обменом, дополнительные функции: редактирование данных, контроль их правильности, обработку сложных команд.

intelligent copier [ɪn'telɪdʒənt 'kɒpiə] интеллектуальное копировальное устройство. @ Копировальное устройство на базе лазерного печатающего устройства, обеспечивающее цифровую обработку копируемого изображения (масштабирование, увеличение контрастности, выделение контуров, объединение изображений) и прием и передачу изображений по линиям связи.

intelligent data base [ɪn'telɪdʒənt 'deɪtə beɪs] интеллектуальная база данных. @ База данных, в которой для ответа на запрос используются как непосредственно хранимые факты, так и факты, получаемые логическим выводом; база данных с языком запросов, близким к естественному языку.

intelligent front end (IFE) [ɪn'telɪdʒənt frʌnt end] 1. интеллектуальная система сопряжения. @ Программа, предназначенная для облегчения доступа к существующей системе программного обеспечения или вычислительной системе. Ее целесообразно использовать при наличии сложного и достаточно развитого программного обеспечения, для освоения которого требуется слишком много времени. 2. интеллектуальная связная ЭВМ, связная ЭВМ с развитой логикой.

intelligent knowledge-based system [ɪn'telɪdʒənt 'nɒlɪdʒ'beɪst 'sɪstɪm] интеллектуальная система, основанная на использовании знаний. @ Система с элементами искусственного интеллекта.

intelligent machine [ɪn'telɪdʒənt mə'ʃiːn] «думающая» машина.

intelligent peripheral interface (IPI) [ɪn'telɪdʒənt pə'rɪfərəl ,ɪntə'feɪs] интеллектуальный периферийный интерфейс.

intelligent terminal [ɪn'telɪdʒənt 'təːmɪnəl] интеллектуальный терминал, «тяжелый» терминал. @ 1. Терминал с собственной памятью и микропроцессором, представляющий средства редактирования и преобразования данных независимо от работы ЭВМ, к которым он подключен. 2. МикроЭВМ или ПЭВМ, используемые в качестве терминала большой ЭВМ.

intelligibility [ɪn'telɪdʒə'bɪlɪtɪ] *n.* разборчивость; внятность; понятность.

intelligibility threshold [ɪn'telɪdʒə'bɪlɪtɪ 'θreʃhəʊld] порог разборчивости.

intelligence [ɪn'telɪdʒəns] *n.* разведка. @ **intelligence cycle** разведывательный цикл (многоступенчатый процесс, в ходе которого производится поиск, сбор, обработка и доведение до заинтересованных лиц радиоразведывательной информации).

intend [ɪn'tend] *v.* 1. намериваться, предполагать; иметь в виду; 2. предназначать. @ **intend task** заданная задача.

intended [ɪn'tendɪd] *adj.* предполагаемый. @ **intended recipient** предполагаемый адресат (сообщении).

inter- [ɪntər-] *pref.* между-; взаимно-; *например*: **international** международный, **interaction** взаимодействие.

interact [ɪntər'ækt] *v.* взаимодействовать.

interaction [ɪntər'ækʃən] *n.* 1. взаимовлияние; 2. взаимодействие; 3. взаимосвязь; 4. диалог. @ **interaction space** пространство взаимодействия.

interactive [ɪntər'æktɪv] *adj.* интерактивный; диалоговый. @ О системе, в которой пользователь задает программе команды во время ее работы. @ **interactive blend** интерактивное перетекание. @ **interactive connector** интерактивная соединительная линия. @ **interactive contour** интерактивный ореол. @ **interactive design system (IDS)** интерактивная система проектирования. @ **interactive distortion** интерактивная деформация. @ **interactive drop shadow** интерактивная тень. @ **interactive envelope** интерактивная огибающая. @ **interactive environment** 1. диалоговый режим; 2. диалоговая система. @ **interactive extrude** интерактивная экструзия. @ **interactive graphics system (IGS)** интерактивная графическая система. @ **interactive graphics** интерактивная графика. @ **interactive key distribution** интерактивное (диалоговое) распределение ключей. @ **interactive mode** интерактивный режим; диалоговый режим. @ **interactive pattern analysis and classification system (IPACS)** интерактивная система анализа и классификации образов. @ **interactive processing** диалоговая обработка. @ **interactive system** интерактивная система; диалоговая система. @ **interactive transparency** интерактивная прозрачность. @ **interactive utility** интерактивная сервисная программа; диалоговая сервисная программа.

interactive debugger [ɪntər'æktɪv dɪ'blʌɡə] диалоговый отладчик. @ Отладчик, позволяющий отлаживать программу в диалоге с ЭВМ.

inter-bit [ɪntər'bit] *adj.* межбитовый. @ **inter-bit dependency** межбитовая зависимость.

intercept [ɪntə'sept] *n.* перехват (перехваченное сообщение); *v.* перехватить (сообщение). @ **intercept a letter, a message, a telegram** перехватить письмо, сообщение, телеграмму. @ **intercept operator** оператор (средства) перехвата.

intercept station = intercepting station

interceptability [ɪntə'septəbɪlɪtɪ] *n.* доступность для перехвата, уязвимость к перехвату.

intercepted communications = intercepted traffic

intercepted [ˌɪntə'septɪd] *adj.* перехваченный.@ **intercepted data** перехваченные данные.@ **intercepted message** перехваченное сообщение.@ **intercepted traffic** перехваченная переписка.@ **intercepting equipment** аппаратура перехвата.@ **intercepting in Internet** перехват в "Интернет".

intercepting [ˌɪntə'septɪŋ] *n.* перехват.@ **intercepting requirements** требования к перехвату.@ **intercepting station** станция перехвата.

interception [ˌɪntə'sepʃən] *n.* перехват.@ **interception program** программа перехвата.

interceptor [ˌɪntə'septə] *n.* перехватчик; тот, кто осуществляет перехват; устройство перехвата.

interchange ['ɪntə'tʃeɪndʒ] *adj.* обменный.@ **interchange key (IK)** обменный ключ (предназначен для взаимного обмена сообщениями).

interface [ˌɪntə'feɪs] *n.* 1. интерфейс, стык.@ Совокупность средств и правил, обеспечивающих логическое или физическое взаимодействие устройств и/или программ вычислительной системы. 2. взаимодействие; 3. устройство сопряжения; 4. граница раздела.@ **interface board** интерфейсная плата.@ **interface computer** интерфейсная ЭВМ.@ **interface module** интерфейсный модуль, описание интерфейса.

interface device [ˌɪntə'feɪs dɪ'vaɪs] устройство сопряжения, УСО, интерфейс.@ Устройство сопряжения ЭВМ с внешним миром, сетью или другой ЭВМ.

interface specification [ˌɪntə'feɪs ˌspesɪfɪ'keɪʃən] описание интерфейса, интерфейсный модуль.@ Декларативная часть модуля программы, содержащая информацию, необходимую другим модулям для взаимодействия с ним.

interface testing [ˌɪntə'feɪs 'testɪŋ] проверка интерфейсов.@ Проверка правильности взаимодействия компонентов программной системы.

interloper *n.* = **interceptor**

intermediate [ˌɪntə'miːdjət] *adj.* промежуточный, вспомогательный; средний.@ **intermediate key** промежуточный (вспомогательный) ключ.

internal key = **inherent key**

internal [ɪn'təːnl] *adj.* 1. внутренний; 2. сокровенный.@ **internal error control (IEC) for cryptosystems** внутренний контроль за ошибками в криптосистемах.@ **internal variant cipher system** внутренняя вариантная шифрсистема.@ **internal connection (IC)** внутреннее соединение.@ **internal evidence** доказательство, вытекающее из существа дела.@ **internal file** внутренний файл.@ **internal language** внутренний язык.@ **internal number base** основание внутренней двоичной системы счисления.@ **internal number system** внутренняя система счисления.@ **internal shield (IS)** внутренний экран.@ **Internal System Number (INS)** идентификатор объекта.@ **internal timer** встроенный таймер.

internal fragmentation [ɪn'təːnl ˌfræmən'teɪʃən] внутренняя фрагментация.@ Фрагментация, возникающая в системах распределения памяти, выделяющих блоки с длиной, кратной некоторой константе; при этом в большинстве случа-

ев выделяется блок большей длины, чем запрошено, и часть выделенного блока не используется.

internal function [ɪn'tə:nl 'fʌŋkʃən] внутренняя функция.@ Функция, определенная и оформленная в теле программы.

internal interrupt [ɪn'tə:nl ɪntə'rʌpt] внутреннее прерывание.@ Прерывание, вызванное командой прерывания или ошибкой при выполнении команды.

internal memory [ɪn'tə:nl 'meməri] 1. собственная память.@ Оперативная память внешнего устройства. 2. оперативная память.

internal name [ɪn'tə:nl neɪm] внутреннее имя.@ 1. Имя, доступное только внутри модуля, в котором оно определено. 2. Имя, используемое внутри модуля, для именования некоторого внешнего объекта.

internal performance [ɪn'tə:nl pə'fɔ:məns] быстродействие процессора.@ Измеряется числом команд в секунду или тактовой частотой.

internal reference [ɪn'tə:nl 'refrəns] внутренняя ссылка.@ Использование объекта, определенного в том же модуле.

internal representation [ɪn'tə:nl ˌreprɪzen'teɪʃən] внутреннее представление.@ Представление данных в памяти ЭВМ в форме, удобной для хранения и обработки.

internal schema [ɪn'tə:nl ski:m] внутренняя схема.@ Описание физической структуры базы данных, в том числе формата хранения записей, методов доступа и распределения по внешним устройствам.

internal sort(ing) [ɪn'tə:nl sɔ:t(ɪŋ)] внутренняя сортировка.@ Сортировка, выполняемая в оперативной памяти.

internal specification [ɪn'tə:nl ˌspesɪfɪ'keɪʃən] описание реализации. @ Описание внутренней структуры программы и способа ее работы.

internally [ɪn'tə:nəli] *adv.* 1. по сути дела; 2. внутренне; внутри.@ **internally generated key** генерируемый внутри (криптографического устройства) ключ.@ **internally stored program** программа, хранимая во внутренней памяти.

international [ˌɪntə:'næʃənl] *adj.* международный.@ **international Association for Cryptologic Research (IACR)** Международная ассоциация криптологических исследований.@ **international Cryptography Experiment** Международная криптографическая инициатива (неформальная программа, целью которой является проверка соблюдения действующих в USA экспортных ограничений на экспорт стойких криптографических средств).@ **international Data Encryption Algorithm (IDEA)** Международный алгоритм зашифрования данных. Разработан в 1992 г. Авторы – сотрудники Швейцарского федерального технологического института Х. Lai, J. L. Massey.@ **International Federation for Information Processing (IFIP)** Международная федерация по обработке информации, МФОИ.@ **International Federation of Automatic Control (IFAC)** Международная федерация по автоматическому управлению.@ **International Standards Organization (ISO)** Международная организация по стандартизации, ИСО.@ **international Traffic in Arms Regulations (ITAR)** Законодатель-

ство по контролю за экспортом вооружений (свод законов USA, регулирующих продажу американского оружия за рубеж, включая шифраторы и другое криптографическое оборудование).

Internet [ɪn'tə:net] *n.* "Интернет" (глобальная компьютерная сеть).@ **Internet Secure Protocol (IPSEC)** Защищенный протокол для подключения к "Интернет" (включает средства криптографической защиты и аутентификации).@ **internet protocol** межсетевой протокол, протокол межсетевого взаимодействия.

interruptor [ɪntə'rʌptə] *n.* прерыватель.@ **interruptor letter** буква-прерыватель.@ **interruptor letter aperiodic** аperiодичный шифр многоалфавитной замены с буквой-прерывателем.

intersymbol [ɪntə'sɪmbəl] *adj.* межсимвольный.@ **intersymbol dependency** межсимвольная зависимость.@ **intersymbol interference (ISI)** межсимвольная интерференция.

inter-user [ɪntə'ju:zə] *adj.* межпользовательский.@ **inter-user key** межпользовательский ключ (предназначен для обмена сообщениями между несколькими пользователями).

intractability [ɪn'træktə'bɪlɪtɪ] *n.* неразрешимость (математической задачи) с полиномиальной сложностью.

intractable [ɪn'træktəblɪ] *adj.* 1. неразрешимый с полиномиальной сложностью (о математической задаче, для которой не существует алгоритма решения с полиномиальной сложностью); 2. стойкий.@ **intractable cryptosystem** стойкая криптосистема.

introduce a new key начать использовать новый ключ.

introduce the four rotor Enigma ввести в действие четырехроторный вариант "Энигмы"

introduce [ɪntrə'dju:s] *v.* 1. вводить; ввести в действие, начать использовать; 2. представлять, знакомить.

introduction [ɪntrə'dʌkʃən] *n.* введение.

intruder [ɪn'tru:də] *n.* злоумышленник, нарушитель; человек, незаконно присвоившим себе чужие права, «злоумышленник». @ Пользователь или программа, пытающиеся получить несанкционированный доступ к данным.

invasion [ɪn'veɪʒən] *n.* нарушение.@ **invasion of privacy** нарушение секретности (конфиденциальности).

inverse [ɪn'veɪz] *n.* 1. инверсия, обращение; 2. обратный, перевернутый; 3. противоположный; *adj.* инверсный, обратный, противоположный.@ **inverse discrete Fourier transform (IDFT)** обратное дискретное преобразование Фурье.@ **inverse function** обратная функция.@ **inverse image** прообраз.@ **inverse key** обратный ключ.@ **inverse keys** взаимно обратные ключи.@ **inverse mapping** обратное отображение.@ **inverse probability** обратная вероятность.@ **inverse Pseudo-Hadamard transform (IPHT)** обратное псевдопреобразование Адамара.@ **inverse ratio** отношение обратных величин, обратное отношение.@ **inverse relation** обратная зависимость.

inverse matrix ['ɪn'və:s 'meɪtrɪks] обратная матрица. @ Квадратная матрица B , которая при умножении на данную квадратную матрицу A дает единичную матрицу.

invert ['ɪn'vɜ:t] *v.* 1. инвертировать; 2. опрокидывать (*фазу*); обращать; переворачивать (*фазу*); преобразовывать. @ **invert function** f обратить (инвертировать) функцию f (найти функцию, обратную к f).

inverted ['ɪn'vɜ:tɪd] *adj.* инвертированный. @ **inverted list** инвертированный список, индекс. @ **inverted output** инвертированный выход. @ **inverted file** инвертированный файл. @ Файл, снабженный индексами по вторичным ключам. @ **inverted list** инвертированный список, индекс.

inverter ['ɪn'vɜ:tə] *n.* 1. скремблер с инверсией частот; 2. инвертор.

invertible ['ɪn'vɜ:tɪbl] *adj.* обратимый. @ **invertible mapping** обратимое отображение. @ **invertible matrix** обратимая матрица. @ **invertible modulo** N . обратимый по модулю N .

invisible ['ɪn'vɪzəbl] *adj.* невидимый. @ **"invisible ink"** "невидимые" чернила.

involute ['ɪnvəlʊ:t] *adj.* сложный. @ **involute cipher** сложный шифр.

invulnerable ['ɪnvə'lu:ʃən] *adj.* неуязвимый.

irrational ['ɪræʃən] *adj.* иррациональный. @ **irrational equation** иррациональное уравнение.

irreducible ['ɪrɪ'dju:səbl] *adj.* неприводимый; несводимый. @ **irreducible over** $GF2$. неприводимый над полем $GF2$. @ **irreducible polynomial** неприводимый многочлен. @ **irreducible proof** несводимое доказательство.

irredundant ['ɪrɪ'dʌndənt] *adj.* нерезервированный. @ **irredundant form** типичная форма.

irreversible *adj.* = **one-way**

isolation ['aɪsəleɪʃən] *n.* 1. развязка, разделение, разграничение (открытой и зашифрованной информации). @ Метод предназначенный для разделения частей системы или ее базы данных с целью повышения защищенности ЭВМ. 2. изолирование.

isolog ['aɪsə'lɒg] *n.* изолог (идентичный или почти идентичный открытый текст, зашифрованный на разных ключах или с помощью разных криптосистем).

isologous ['aɪsə'lɒgəs] *adj.* изологовый. @ **isologous segments** изологовые сегменты (различные отрезки шифртекста, которым соответствует идентичный или почти идентичный открытый текст).

isologue *n.* = **isolog**

isomorphism ['aɪsə'mɔ:fɪzəm] *n.* изоморфизм. @ Взаимнооднозначное отображение.

isotopically [aɪsoʊ'tɒpɪkəli] *adv.* ненаправленно.

issue ['ɪʃu:] *v.* 1. выходить, вытекать; 2. происходить, получаться в результате (**from**); 3. выпускать, издавать; *n.* 1. выпуск; 2. вопрос; 3. результат чего-

л.; 4. проблема. # **the point at issue** предмет обсуждения (спора). # **to be at issue** быть предметом обсуждения (спора).

issuer *n.* **source**

italic [ɪ'tælɪk] *adj.* курсивный. # **in italic** курсивом.

item ['aɪtəm] *n.* 1. элемент данных. 2. пункт, вопрос; 3. предмет; 4. статья; 5. наименование; 6. деталь. @ **item design** компоновка элементов данных с целью дальнейшей эффективной обработки. @ **item size** размер элемента данных (в битах, байтах или цифрах). @ **item value** значение элемента данных.

intention [ɪn'tenʃən] *n.* намерение, цель.

intentional [ɪn'tenʃənəl] *adj.* умышленный, намеренный.

intentionally [ɪn'tenʃənəlɪ] *adv.* специально, умышленно, намеренно.

iterate [ɪtə'reɪt] *v.* повторять; итерировать. @ **iterate an operation disguising an easy knapsack** выполнять операцию сокрытия тривиального вектора ранца итеративно.

iterated [ɪtə'reɪtɪd] *adj.* повторный. @ **iterated integral** повторный интеграл. @ **I-terated** I-итеративный.

iteration [ɪtə'reɪʃən] 1. итерация. @ Повторение преобразования, приближающего к решению; 2. шаг цикла. @ **iteration body** тело цикла. @ **iteration factor** параметр цикла. @ **iteration method** метод последовательных приближений, итерационный метод. @ **iteration methods for linear systems** итерационные методы решения систем линейных уравнений. @ **iteration procedure** метод итерации, итерация. @ **iteration statement** оператор цикла.

iterative [ɪtə'reɪtɪv] *adj.* итеративный, диалоговый. @ Атрибут, с помощью которого указывается, что для системы или режима характерен отклик на вводимые оператором команды. @ **iterative instruction** 1. циклическая команда, команда организации цикла; 2. команда для выполнения последовательных приближений. @ **iterative invariant** итерационный инвариант. @ **iterative loop** цикл итерации. @ **iterative process** итерационный (итеративный) процесс. @ **iterative routine** программа реализации итеративного алгоритма.

iterator [ɪtə'reɪtə] *n.* итератор. @ Управляющая конструкция языка программирования для задания последовательности значений параметра цикла.

iterated [ɪtə'reɪtɪd] *adj.* итеративный, итерационный. @ **iterated cipher** итеративный шифр (с многократным выполнением некоторых операций процесса шифрования). @ **iterated cryptosystem** итеративная криптосистема (с многократным выполнением некоторых криптографических операций). @ **I-terated knapsack cryptosystem** I-итеративная ранцевая криптосистема (ранцевая криптосистема, в которой для сокрытия тривиального вектора ранца используются I операций умножения по модулю).

iterative cipher = product cipher

itself [ɪt'self] *prom. refl.* 1. сам, само, сама; 2. себя, -ся, -сь. # **by itself** само собой. # **in itself** само по себе, по своей природе. # **of itself** само по себе, без связи с другими явлениями.

J*

Japanese [dʒəˈpæn] *adj.* японский. @ **Japanese Navy code № 25** Японский военно-морской код № 25 (вскрытие этого кода американцами помогло им провести ряд успешных военных операций на Тихом океане во время второй мировой войны).

Jefferson cipher wheel дисковый шифр Джефферсона (шифровальное колесо Джефферсона).

Jevons's number число Джевонса (в своей книге "Трактат о логическом и научном методе", опубликованной в 1870 г., Джевонс заявил о том, что вряд ли кому-то, кроме него самого, удастся разложить на множители число 8616460799)

joy-riding [dʒɔɪˈrɪdɪŋ] *n.* использование побочных явлений для доступа к информации.

just [dʒʌst] *adv.* 1. как раз; именно; 2. только что; 3. едва; 4. совсем, прямо, просто, совершенно; *adj.* 1. справедливый; 2. обоснованный; заслуженный; 3. верный, точный. # **just as** точно так же, как.

K*

k-64 = key of length 64

kappa ['kærə] *n.* к (буква греческого алфавита). @ **kappa-test** к-тест.

Kasiski method (test) метод (тест) Казиского.

keep [ki:p] *v.* (**kept**) 1. держать, поддерживать; 2. сохранять; хранить; 3. задерживать (**down**); 4. продолжать (**on**); 5. придерживаться чего-л. (**to**); 6. поддерживать (**up**). # **in keeping with** в соответствии с. # **to keep a record** вести запись. # **to keep in mind** помнить, учитывать, иметь в виду. # **to keep in touch with** поддерживать связь с; быть в курсе (событий, действий и т. п.). # **to keep pace with** идти в ногу с; не отставать. # **to keep up with** идти в ногу с; не отставать.

keeper ['ki:pə] *n.* держатель, хранитель (напр, ключа).

Kerckhoff assumption допущение Керкхоффа (весь механизм шифрования, кроме значения секретного ключа, известен криптоаналитику противника).

Kerckhoff precept правило Керкхоффа (стойкость шифра должна определяться только секретностью ключа).

Kerckhoff requirements требования Керкхоффа (шесть условий, которым должна удовлетворять универсальная криптосистема).

key (k) [ki:] *n.* криптографический ключ. @ Параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах алгоритм шифрования известен и криптографическая стойкость шифра целиком определяется секретностью ключа. @ **key agreement protocol** протокол согласования ключа (одноключевой криптосистемы). @ **key assignment**

назначение (распределение) ключей. @ **key authentication center (КАС)** центр аутентификации ключей. @ **key backup** создание резервных копий ключей. @ **key bank** банк ключей. @ **key bit** бит ключа (ключевой последовательности). @ **key book** книга с ключами. @ **key card** ключевая перфокарта (бумажная карточка с отверстиями, используемая в качестве носителя ключевой информации). @ **key carrier** 1. ключевой носитель; устройство транспортировки ключей; 2. владелец (держатель) ключа. @ **key certification authority (КА)** полномочие на сертификацию ключей. @ **key certification center (КСС)** центр сертификации ключей. @ **key certification** сертификация (заверение подлинности) ключей. @ **key change** смена (замена) ключа. @ **key character** знак ключа. @ **key clustering** группирование ключей (при криптоанализе). @ **key compromise** компрометация ключа. @ **key delivery** доставка (транспортировка) ключей. @ **key dependency** 1. зависимость от ключа (зависимость битов шифртекста от битов ключа); 2. взаимозависимость ключей. @ **key diffusion** рассеивание ключа (распространение влияния ключа на множество знаков шифртекста). @ **key digits** цифры ключа. @ **key directory (KD)** справочник ключей. @ **key disclosure** раскрытие ключа. @ **key disk** 1. диск (дискета) для хранения ключей. @ **key distribution center (KDC)** центр распределения ключей. @ **key distribution information** информация службы распределения ключей. @ **key distribution mechanism** механизм распределения ключей. @ **key distribution node** узловой центр распределения ключей. @ **key distribution protocol (KDP)** протокол распределения ключей. @ **key distribution system (KDS)** система распределения ключей. @ **key distribution** распределение (доставка) ключей. @ **key encryption** шифрование ключей. @ **key entropy** энтропия ключей. @ **key entry procedure** процедура ввода ключа. @ **key erasure** стирание ключа (записанного в памяти). @ **key escrow system (KES)** криптосистема с депонированием ключей. @ **key escrow** депонирование ключей (передача ключей на хранение третьим лицам). @ **key exchange algorithm (KEA)** алгоритм обмена ключами. @ **key exchange system** 1. система обмена ключами; 2. система обмена информацией для выработки ключа. @ **key exchange via third party** ключевой обмен с участием третьей стороны. @ **key exchange** обмен ключами. @ **key exhaustion attack** атака путем перебора всех возможных вариантов ключа. @ **key expansion** увеличение длины ключа. @ **key exposure** раскрытие (разглашение) ключа. @ **key extraction** извлечение (выделение) ключа (например, из памяти компьютера или шифратора). @ **key field** поле ключа (в сообщении). @ **key format** формат ключа. @ **key generation function** функция генерации (порождения) ключа. @ **key generation unit** устройство генерации ключей. @ **key generation** генерация (порождение) ключей. @ **key generator** генератор ключей. @ **key hashing** хэширование ключа (преобразование исходного ключа в более короткий, на котором и производится шифрование). @ **key hierarchy** иерархия ключей. @ **key identification number (KIN)** идентификационный номер ключа. @ **key information** ключевая информация. @ **key injection** ввод ключей. @ **key injector** устройство ввода ключей. @ **key input algorithm** алгоритм ввода ключа. @ **key insertion set** комплект (набор) (устройств) для ввода ключа. @ **key insertion**

ввод ключа. @ **key installation** установка (инсталляция) ключа. @ **key installer** лицо, осуществляющее установку (инсталляцию) ключа. @ **key integrity** целостность ключа. @ **key library** библиотека ключей (собрание ключей одного пользователя или группы пользователей). @ **key life** продолжительность действия ключа. @ **key list** список (перечень) ключей (используемых в течение определенного периода времени). @ **key load button** кнопка (клавиша) загрузки (ввода) ключа. @ **key load device** устройство загрузки ключей (предназначено для хранения электронного ключа с целью его последующей установки в криптографическое оборудование). @ **key load procedure** процедура загрузки (ввода) ключа. @ **key load** загрузка (ввод) ключей. @ **key management center (KMC)** центр управления ключами. @ **key management facilities (KMF)** средства управления ключами. @ **key management information** информация службы управления ключами. @ **key management mechanism** механизм управления ключами. @ **key management procedure** процедура управления ключами. @ **key management protocol (KMP)** протокол управления ключами. @ **key management system (KMS)** система управления ключами. @ **key management** управление ключами. @ **key manager** администратор (службы) управления ключами. @ **key matrix** матрица ключей (ключевая матрица) (матрица, используемая в качестве ключа). @ **key memory** память ключей. @ **key negotiation** переговоры о выработке (общего) ключа (ключевой обмен). @ **key notarization system (KNS)** система с нотариризацией ключей. @ **key notarization** нотаризация ключей. @ **key of directory** ключ, содержащийся в справочнике. @ **key of length N** ключ длины N . @ **key pair** пара ключей (зашифрования и расшифрования). @ **key parameter** ключевой параметр (параметр ключа). @ **key period** период (повторения) ключа. @ **key phrase** ключевая фраза (используется в качестве ключа или для формирования ключа). @ **key predistribution scheme (KPS)** схема предварительного распределения ключей. @ **key processor (KP)** ключевой процессор. @ **key production key (KPK)** ключ генерации ключей (используется для инициализации генератора ключевой последовательности). @ **key program** программа генерации ключей. @ **key protection** защита ключей. @ **key purchase attack** атака с использованием купленного (напр, у курьера) ключа. @ **key receiver** получатель ключа. @ **key recovery database** база данных, используемая для восстановления ключей. @ **key recovery system** система восстановления ключей. @ **key recovery** восстановление ключей. @ **key redundancy** избыточность ключа. @ **key register** регистр для хранения ключа. @ **key reload procedure** процедура повторной загрузки (повторного ввода) ключа. @ **key reload** повторная загрузка (повторный ввод) ключа. @ **key repetition** повторное использование ключа. @ **key repository** устройство (прибор) для хранения ключей. @ **key restoration** восстановление ключа. @ **key retrieval** поиск ключа. @ **key search** поиск (неизвестного) ключа. @ **key secrecy** секретность ключа. @ **key security** защищенность ключа. @ **key seed** начальное состояние генератора ключей. @ **key-selective network** сеть с выбором ключа (для различных видов связи) (сеть с избирательностью по ключу). @ **key sequence period** период ключевой последовательности. @ **key sequence** ключевая последователь-

ность. @ **key server** сервер ключей. @ **key set** множество (набор) ключей. @ **key setting** установка (набор) ключа. @ **key setup** подготовка ключей. @ **key sharing** групповое (коллективное) пользование ключом. @ **key signature** подпись, удостоверяющая ключ (подпись под ключом). @ **key size** размер (длина) ключа. @ **key source** источник ключа. @ **key space exploration** поиск в пространстве ключей. @ **key space** ключевое пространство (количество различных ключей для данного шифра). @ **key splitting** деление ключа на части (ключ делится на составные части, которые распределяются между несколькими лицами так, что ключ может быть восстановлен в полном объеме только в том случае, если каждый из них предоставит для этого свою часть ключа). @ **key starting point** исходная (отсчетная) точка (используемой) ключевой последовательности. @ **key storage unit (KSU)** устройство хранения ключей. @ **key storage** хранение ключей (в памяти компьютера или шифратора). @ **key stream generation** генерация (порождение) ключевой последовательности (ключевого потока). @ **key stream generator** генератор ключевой последовательности (ключевого потока). @ **key stream period** период ключевой последовательности (ключевого потока). @ **key stream** ключевая последовательность (ключевой поток). @ **key string** ключевая строка (строка-ключ). @ **key structure** структура ключа. @ **key system** ключевая система. @ **key table** таблица ключей (ключевая таблица). @ **key tag** ключевая бирка (дополнительная идентификационная информация, которой снабжаются электронные ключи). @ **key tape** ключевая лента (перфорированная или магнитная лента, используемая в качестве носителя ключевой информации). @ **key text** текстовая ключевая информация (представление ключа в виде текста). @ **key theft** кража ключей. @ **key to a cipher** ключ к шифру. @ **key transfer device** устройство передачи ключей. @ **key transfer protocol** протокол передачи ключей. @ **key transport device** устройство транспортировки (доставки) ключей. @ **key transport** доставка (транспортировка) ключей. @ **key trial** проба ключа (при криптоанализе методом проб и ошибок). @ **key type** тип ключа. @ **key updating** обновление ключа (необратимый процесс смены ключа в криптографическом оборудовании). @ **key variable (KV)** ключевая переменная. @ **key wheel** ключевое колесо (шифровальной машины). @ **key word** ключевое слово. @ **key** ключевой диск (ключевая дискета). @ **key-autokey (КАК)** ключ-автоключ. @ **key-breaking efforts** усилия по вскрытию ключа. @ **key-controlled algorithm** управляемый ключом алгоритм (шифрования). @ **key-cracking computer** компьютер для вскрытия ключей. @ **key-dependent cryptalgorithm** зависящий от ключа алгоритм шифрования. @ **key-dependent depth** мощность ключевого множества (количество ключей). @ **key-encrypting key (КК, КЕК)** ключ шифрования (других) ключей (главный ключ). @ **key-guessing attack secure** защищенный от атаки с угадыванием ключа. @ **key-guessing attack** атака с угадыванием ключа. @ **key-handling procedure** процедура работы с ключом. @ **key-length** длина ключа. @ **key-minimal cipher** шифр с ключом минимальной длины (с минимальным числом ключей). @ **key's properties** свойства ключа. @ **key-schedule** 1. ключ-расписание (в

DES-алгоритме); 2. назначение (смена) ключей. @ **key-schedule cryptanalysis** вскрытие ключ-расписания.

key creation function = **key generation function**

key cycle period = **key period**

key encryption key = **key-encrypting key**

key fill device = **key load device**

key-related information = **keying information**

key loader = **key load device**

key producing unit = **key generation unit**

key reloading = **key reload**

key safeguarding = **key protection**

key-key pair = **key-pair**

keyed [ki:d] *adj.* с ключом. @ **keyed cryptoalgorithm** алгоритм шифрования с ключом.

keying ['ki:diŋ] *adj.* ключевой; *n.* ввод ключа. @ **keying information** ключевая информация. @ **keying material** ключевой материал. @ **keying variable** ключевая переменная.

keyless cipher ['ki:lis 'saɪfə] бесключевой шифр.

keyword mixed sequences ['ki:'wə:d 'mɪkst 'si:kwənsɪz] смешанные с использованием ключевого слова последовательности.

"kiss" [kɪs] *n.* "поцелуй" (совпадение открытых текстов двух криптограмм, полученных с помощью различных шифров).

knapsack (KN) ['næpsæk] *n.* 1. рюкзак, ранец; 2. вектор ранца. @ **knapsack cryptosystem** ранцевая (рюкзачная) криптосистема. @ **knapsack problem** задача об укладке ранца (о рюкзаке).

knapsack-based cryptosystem = **knapsack cryptosystem**

knowledge ['nɒlɪdʒ] *n.* 1. знание; познание; эрудиция; 2. осведомленность; 3. знакомство; 4. известие. @ **knowledge-based** интеллектуальный; использующий средства или методы искусственного интеллекта. # **to the best of our knowledge** насколько нам известно. # **to the author's knowledge** насколько известно автору. # **it is common knowledge** это общеизвестно.

knowledge acquisition ['nɒlɪdʒ ,ækwɪ'zɪʃən] сбор знаний; построение базы знаний. @ При построении экспериментальной системы или базы знаний — получение информации о предметной области от специалистов и выражение ее на языке представления знаний.

knowledge base ['nɒlɪdʒ beɪs] база знаний. @ Совокупность правил и фактов, описывающая предметную область и вместе с механизмом вывода позволяющая ответить на вопросы об этой предметной области, ответ на которые в явном виде не присутствует в база.

knowledge engineer ['nɒlɪdʒ ,en-'dʒɪniə] инженер знаний. @ Специалист по искусственному интеллекту, занимающийся построением конкретной экспериментальной системы или базы знаний.

knowledge engineering ['nɒlɪdʒ ,en'dʒɪniəriŋ] разработка интеллектуального обеспечения.

knowledge representation ['nɒ-lɪdʒ ,reprɪzen'teɪʃən] представление знаний.@ Раздел искусственного интеллекта, занимающийся средствами представления понятий, правил и фактов для построения баз знаний и экспериментальных систем.

known [noun] *adj.* известный.# **known as** известный под именем; *v.* владеть (знаниями).

known-plaintext [noun,pleɪn'tekst] *adj.* основанный на знании открытого текста.@ **known-plaintext attack secure** защищенный от атаки на основе знания открытого текста.@ **known-plaintext attack** атака на основе знания открытого текста.

known-to-be-ASCII *adj.* основанный на знании того, что открытый текст имеет кодировку ASCII.@ **known-to-be-ASCII attack** атака на основе знания того, что открытый текст имеет кодировку ASCII.

krypto- = **crypto-**

L*

lack [læk] *n.* недостаток, отсутствие чего-л. (**of**); *v.* испытывать недостаток, не хватать; отсутствовать.# **for lack of** из-за отсутствия, из-за недостатка.

language ['læŋgwɪdʒ] *n.* язык.@ Естественная или искусственная знаковая система для общения и передачи информации..@ **language characteristics** характерные черты (особенности) языка.@ **language data** языковые данные.@ **language data processing** обработка лингвистической информации.

language binding ['læŋgwɪdʒ 'baɪndɪŋ] привязка к языку.@ Средства языка программирования, обеспечивающие взаимодействие программ со стандартным пакетом.

language construct ['læŋgwɪdʒ kən'strʌkt] 1. конструкция языка.@ Синтаксическая структура для построения сложных операторов и выражений языка из более простых. 2. языковая конструкция.@ Одна или несколько синтаксических структур, используемых в языке для указания узкого класса операций.

language converter ['læŋgwɪdʒ kən'vɜ:tə] конвертор.@ Программа, выполняющая трансляцию на язык того же уровня, что и входной язык.

language processor ['læŋgwɪdʒ 'prəʊsesə] транслятор или интерпретатор.@ Программа, обрабатывающая (транслирующая или интерпретирующая) программу на языке программирования.

large ['la:ɔ] *adj.* 1. большой, обширный; 2. многочисленный; значительный; 3. широкий (о взглядах и т.п.).@ **large integer factorization** разложение большого целого числа на множители.@ **large key space** большое ключевое пространство.# **as large as** до (обычно перед цифрами).# **at large** подробно; в целом, весь; широко, вообще; имеющий широкие полномочия.# **by and large**

вообще говоря. # **half as large** в два раза меньше. # **in large** в большом (крупном) масштабе. # **twice as large** в два раза больше.

last [fa:st] *v.* продолжаться; *adj.* 1. последний; 2. прошлый. # **at last** наконец. # **last but one** предпоследний.

late [leɪt] *adj.* 1. поздний; 2. недавний; последний; 3. покойный. # **late in** в конце. # **it the late** в конце. # **as late as** только, уже. # **of late** за последнее время

latent ['leɪtənt] *adj.* скрытый (латентный). @ **latent repetition** скрытое повторение (в шифртексте). # **latent period** инкубационный период.

Latin ['læɪn] *adj.* латинский. @ **Latin square** латинский квадрат (матрица размера $n \times n$ из n символов, в которой любой столбец и любая строка не содержат повторений).

latter ['lætə] *adj.* последний (из упомянутых выше). # **the former ... the latter** первый ... последний.

lattice ['lætɪs] *n.* решетка. @ Множество, на котором задано отношение порядка такое, что для любых двух элементов A и B имеется минимальная верхняя грань и максимальная нижняя грань. @ **lattice basis reduction** (криптоаналитический) метод редукции базисов решеток. @ **lattice parameter** параметр решетки. @ **lattice sampling** решетчатая выборка. @ **lattice theory** 1. теория решеток; 2. теория структур. @ **lattice with basis** решетка с базисом.

law [lɔ:] *n.* закон; правило; принцип; формула; теорема. @ **law enforcement access field (LEAF)** поле данных правоохранительных органов (в алгоритме шифрования "Скипджек"). @ **law of double negation** закон двойного отрицания. @ **law of absorption** закон поглощения. @ **law of averages** закон больших чисел. @ **law of development** закон развертывания. @ **law of excluded middle** закон исключенного третьего. @ **law of identity** закон тождества. @ **law of large numbers** закон больших чисел. @ **law of probability** вероятностный закон. @ **law of reductio ad absurdum** закон приведения к абсурду. @ **law of small numbers** закон малых чисел, закон распределения Пуассона. @ **law of thought** закон мышления.

layer ['leɪə] *n.* 1. уровень, слой; 2. разрез (операция или преобразование в блочном шифре, выполняемая по всей длине блока).

lead ['li:d] *v.* (**led**) 1. вести; 2. приводить, заставлять; *n. pl.* провода. # **to lead to a blind alley** завести в тупик. # **to take the lead** быть впереди, возглавлять. # **to be lead to** быть вынужденным.

leak [li:k] *v.* просачиваться. @ **leak into a transmission line as a side-channel** просачиваться в линию связи, превращая ее в побочный канал.

least [li:st] *adj.* (*превосх. степень от little*) наименьший, малейший. @ **least common multiple (LCM)** наименьшее общее кратное. @ **least significant bit** самый младший бит (в двоичном представлении числа). @ **least square estimation** оценка по методу наименьших квадратов. # **at least** по крайней мере. # **not in the least** нисколько. # **to say the least** по меньшей мере.

legitimate [li'dʒɪtɪmɪt] *adj.* 1. законный; 2. допустимый; 3. правильный, разумный. @ **legitimate value** допустимое значение. @ **legitimate user** законный пользователь.

lend [lend] *v.* (**lent**) 1. давать (взаймы); 2. придавать, сообщать. # **to lend itself** быть пригодным; поддаваться; сводиться. # **to lend (give) support** оказывать поддержку; подтверждать.

length [lenθ] *n.* 1. длина. @ Число элементов; 2. длина (протяженность), продолжительность, длительность; 3. продолжительность; 4. отрезок, кусок. @ **length increasing grammar** грамматика, увеличивающая длину. @ **length of a key** длина ключа. @ **length of a shift register** длина регистра сдвига. # **at length** подробно; наконец.

lengthen [lenθn] *v.* удлинять, увеличивать длину. @ **lengthen a cryptographic key to 256 bits** увеличивать длину криптографического ключа до 256 бит.

lengthy [lenθi] *adj.* 1. растянутый, очень длинный; 2. многословный.

let [let] *v.* (**let**) 1. позволять, допускать; 2. *в повелительном наклонении употребляется как вспомогательный глагол и выражает приглашение, приказание, разрешение: let us go* идем(те). # **let him do at once** пусть он сделает это сразу. # **let alone** не говоря уже о.

letter (ltr) ['letə] *n.* 1. буква; символ; элемент алфавита; 2. письмо. @ **letter frequency count** подсчет частоты встречаемости букв (в тексте). @ **letter-by-letter** побуквенное шифрование (открытого текста). @ **letter-frequency distribution** распределение частот встречаемости (появления) букв (в тексте). @ **letter-pattern cryptanalysis** криптоанализ на основе изучения сочетания букв в тексте. # **to the letter** буквально, точно.

level ['levl] *n.* 1. уровень, ступень; 2. горизонт; *adj.* ровный; *v.* выравнивать, сглаживать. @ **level of abstraction** уровень абстракции. @ **level of addressing** уровень адресации. @ **level of authorized access to information** уровень санкционированного доступа к информации.

license ['laisəns] *n.* лицензия (разрешение, выдаваемое государственными органами на право продажи и предоставления услуг).

life ['laɪf] *n.* 1. жизнь; 2. срок службы (машины и т. п.); продолжительность действия (напр, ключа). @ **life cycle of a key** "жизненный цикл" ключа. # **life size** натуральная величина. # **still life** натюрморт.

light ['laɪt] *n.* 1. свет; освещение; лампа; *adj.* 1. светлый; 2. легкий; *v.* зажигать(ся). # **to throw (cast) light on (upon)** проливать свет на что-л.

like [laɪk] *adj.* похожий, подобный; *prp.* подобно, как; *v.* нравиться, любить. # **and the like** и тому подобное. # **shold (would) like + inf.** хотелось бы + инф.

limit (lim) ['lɪmɪt] *n.* граница; предел; *v.* ограничивать. # **within the limits** в пределах. # **to place a limit on** ограничивать.

limited ['lɪmɪtɪd] *adj.* укороченный, имеющий ограниченную длину. @ **limited key** ключ ограниченной длины (укороченный ключ).

line [laɪn] *n.* 1. строка (программы, текста, экрана дисплея); 2. линия (элемент изображения); 3. линия связи; проводник шины; 4. серия; семейство; *v.* 1. проводить линию; 2. облицовывать. @ **line eavesdropping** подслушивание на линии (связи). @ **line encryption device** линейный шифратор. @ **line level en-**

ryption шифрование на уровне линии (связи).@ **line-tapper** перехватчик, подключающийся к линии (связи).# **along the lines** в направлении; по типу, в соответствии с.# **on the lines** в направлении; по типу, в соответствии с.# **in line with** в соответствии с.# **dashed line** пунктирная линия.# **dotted line** пунктирная линия.# **solid line** сплошная линия.# **to be on the right lines** находится на правильном пути.

linear ['laɪnə] *adj.* линейный.@ **linear algebraic equation** линейное алгебраическое уравнение.@ **linear approximation of block ciphers** линейная аппроксимация блочных шифраторов.@ **linear approximation** линейное приближение.@ **linear array** линейный массив.@ **linear attack** линейная атака.@ **linear cipher** линейный шифр.@ **linear combination** линейная комбинация.@ **linear complexity profile** профиль линейной сложности (ключевого потока).@ **linear complexity** линейная сложность ключевого потока (длина самого короткого регистра сдвига с линейной обратной связью).@ **linear congruential generator (LCG)** линейный конгруэнтный генератор.@ **linear consistency test** тест на линейную согласованность (ключевого потока).@ **linear cryptanalysis** линейный криптоанализ (для описания поведения шифром использует линейные приближения).@ **linear delta modulation (LDM)** линейная дельта-модуляция.@ **linear distribution** линейное распределение.@ **linear equation** линейное уравнение.@ **linear feedback shift register (LFSR)** регистр сдвига с линейной обратной связью.@ **linear function generator** 1. генератор (блок) линейной функции; 2. линейный функциональный преобразователь.@ **linear grammar** линейная грамматика.@ **linear interpolation** линейная интерполяция.@ **linear language** линейный язык.@ **linear manifold** линейное многообразие.@ **linear mapping** линейное отображение.@ **linear multistep methods** линейные многошаговые методы.@ **linear operator** линейный оператор.@ **linear predictive coding (LPC)** линейное кодирование с предсказанием.@ **linear regression model** линейная регрессивная модель.@ **linear relation** линейная зависимость.@ **linear restricted scattering matrix (LRSM)** линейно ограниченная матрица рассеяния.@ **linear search** последовательный перебор.@ **linear space** линейное пространство.@ **linear staircase function generator** 1. генератор линейной ступенчатой функции; 2. линейно-ступенчатый функциональный преобразователь.@ **linear transformations based cipher** шифр на основе линейных преобразований.@ **linear-resistant function** линейностойкая функция (стойкая против линейного криптоанализа).

linear channel ['laɪnə 'tʃænl] линейный канал.@ Канал связи, в котором информационный сигнал аддитивно смешивается с помехой и в результате образует выходной сигнал.

linear codes ['laɪnə kəʊds] линейные коды.@ В теории кодирования линейными кодами называются коды, кодирование и декодирование которых может быть сведено к линейным операциям. Часто этот термин относится к определенным кодам с исправлением ошибок, для которых кодирование осуществляется с помощью порождающей матрицы, а декодирование — с помо-

щью матрицы проверки на четность. Поэтому линейные коды также называют кодами с проверкой на четность.

linear independence ['laɪnə ˌɪndɪˈpendəns] линейная независимость. @ Фундаментальное понятие математики.

linear logic ['laɪnə ˈlɒdʒɪk] линейная логическая схема. @ Система из комбинационных и, возможно, последовательных схем, в которой комбинационная часть состоит только из схем «исключающее ИЛИ». Такие системы иногда называют строго линейными логическими схемами в противоположность слабо линейным логическим схемам, в состав которых входят инверторы.

linear program ['laɪnə ˈprɒɡræm] линейная программа. @ Программа, не содержащая переходов.

linear programming (LP) ['laɪnə ˈprɒɡræmɪŋ] линейное программирование. @ Раздел математики, изучающий задачи оптимизации с ограничениями в виде системы линейных неравенств.

linear recurrence ['laɪnə rɪˈkʌrəns] линейное рекуррентное соотношение. @ Соотношение, задающее следующий член последовательности в виде линейной комбинации предшествующих членов последовательности.

linear structure ['laɪnə ˈstrʌktʃə] линейная структура. @ Совокупность элементов, упорядоченных по одному признаку, так что каждый элемент за исключением, возможно, первого или последнего, имеют единственного предка и единственного потомка.

linear-bounded automation (LBA) ['laɪnəˈbaʊndɪd ɔːtəˈmeɪʃən] автомат с линейно ограниченной памятью. @ Автомат (например, машина Тьюринга), которому для распознавания последовательности длины N необходима память объемом не более kN , где k – число, не зависящее от входной последовательности.

linearity ['laɪnəɪrɪti] *n.* линейность.

linearly ['laɪnəli] *adv.* линейно. @ **linearly dependent** линейно зависимый.

linearization ['laɪnəraɪˈzeɪʃən] *n.* линеаризация.

linearize ['laɪnəraɪz] *v.* линеаризовать. @ **linearize a system of non-linear equations** линеаризовать систему нелинейных уравнений.

linetap = tapping

line-tap ['laɪntæp] подключение (устройств перехвата) к линии (связи).

linguistic ['lɪŋɡwɪstɪks] *adj.* лингвистический. @ **linguistic attack** лингвистическая атака (разновидность криптоаналитической атаки).

link [lɪŋk] *n.* канал. @ **link encryption key** ключ канального шифрования. @ **link encryption** канальное шифрование (засекречивание передач по каналам связи с помощью шифрования). @ **link encryptor** канальный шифратор. @ **link key** ключ для отдельного канала (связи). @ **link-by-link encryption** поканальное шифрование (применение шифрования в каждом канале, соединяющем два узла сети связи, которые могут быть промежуточными на пути от отправителя к получателю сообщения).

link encryption device = link encryptor

link-to-encryption = link-by-link encryption

lipogram ['lɪpou'græm] *n.* липограмма (содержательный текст, состоящий из слов, в которых не встречается одна или несколько букв алфавита).

lipstick *n.* жарг = **cryptoignition key (СК)**

list [lɪst] *n.* 1. список.@ Упорядоченная последовательность произвольных элементов, в частности, других списков. 2. перечень; *v.* 1. печатать, распечатывать; 2. перечислять.@ **list insertion sort** сортировка списка методом вставок.@ **list squares approximations** аппроксимация по методу наименьших квадратов.@ **list structure** списковая структура.@ **list of instructions** список команд.@ **list of modifications** список исправлений (изменений).@ **list pointer** указатель списка.@ **list process** процесс обработки списков.@ **list representation** списочное представление, представление (*данных*) в виде списка.@ **list squares approximations** аппроксимация по методу наименьших квадратов.@ **list structure** списковая структура.

list device [lɪst dɪ'vaɪs] (логическое) устройство печати.@ Устройство, на которое выводятся результаты работы программы; устройство, связанное по умолчанию со стандартным выводом программы.

list head [lɪst hed] заголовок списка.@ Специальные головные элементы списковых структур, добавляемые к списку, а возможно, и к подпискам с целью упрощения алгоритмов управления вычислительным процессом и просмотра позиций списка.

list processing [lɪst 'prəʊsesɪŋ] обработка списков.@ Программные или (редко) аппаратные средства обработки списочных структур данных, обеспечивающие динамическое распределение памяти со сборкой мусора и операции построения и анализа списков.

list sorting [lɪst 'sɔ:tɪŋ] сортировка списков.@ Форма сортировки, при которой используется поле указателя, присутствующего в каждой записи. Сортировка методом вставок с использованием указателей – это и есть способ сортировки списков.

list squares [lɪst skweəs] метод наименьших квадратов.@ Метод оценки параметров модели путем минимизации суммы квадратов разностей наблюдаемых и истинных значений.

list structure [lɪst 'strʌktʃə] списковая структура

listening ['lɪstɪŋ] *adj.* перехватывающий, подслушивающий.@ **listening post** пост (пункт, станция) перехвата (подслушивания).

listening station = listening post

literal (lit) ['lɪtərəl] *n.* литерал, буквальная (литеральная) константа.@ Слово или символ в программе, определяющие свое собственное значение, а не имя какого-то другого элемента. Примером может служить объект, значение которого определяется самим его видом. Числа – это всегда литералы. *adj.* буквенный.@ **literal key** буквенный ключ.@ **literal equation** уравнение с буквенными коэффициентами.

little [lɪtl] *adj.* маленький; *adv.* мало. # **little by little** мало-помалу, постепенно. # **little more than** лишь. # **little or no** почти или совсем не. # **a little** немного. # **as little as** только; до (*обычно перед цифрами*).

load [ləʊd] *n.* 1. загрузка (*оборудования, системы*). @ Совокупность выполняемых работ. 2. нагрузка; *v.* 1. загружать (*программу*). @ Считывать и настраивать загрузочный модуль или сегмент перекрытий. 2. загружать (*в регистр*). @ Заносить в регистр процессора данные из оперативной памяти. 3. загружать (*в память*). @ Считывать в оперативную память данные из внешней памяти. 4. загружать, заполнять (*базу данных*). @ Записывать в базу данных предназначенную для нее информацию. 5. устанавливать (*магнитную ленту или диск на соответствующее устройство*). @ **load a key** загружать (вводить) ключ. # **dead load** собственный вес; вес конструкции. # **pay load** полезная нагрузка.

loading *n.* = **load**

"lobster" ['lɒbstə] *n.* "омар" (состояние немецкой шифровальной машины "Энигма", в котором все ее роторы поворачиваются вместе).

local ['ləʊkəl] *adj.* 1. локальный. @ 1. Об объекте программы – определенный и доступный только в текущем блоке (модуле, процедуре) программы. 2. О методе – применяемый к ограниченному участку; 3. Об устройстве подключенный непосредственно к ЭВМ, в отличие от доступного по сети. 2. местный; 3. частный. @ **local discretization error** локальная ошибка дискретизации. @ **local identifier** локальный идентификатор, локальное имя. @ **local key load** местная загрузка (местный ввод) ключей. @ **local key** локальный ключ (предназначен для отдельного конкретного устройства шифрования). @ **local master key (LMK)** локальный главный ключ (мастер-ключ). @ **local mode** автономный режим. @ **local oscillator (LO)** гетеродин. @ **local parameter** локальный параметр. @ **local periodic structure (LPS)** локально-периодическая структура. @ **local quantity** локализованная величина. @ **local randomness** локальная случайность (случайность короткой подпоследовательности, являющейся частью очень длинной последовательности). @ **local storage (LS, LSTOR)** местная память (ЗУ). @ **local storage address register (LSAR)** регистр адреса местного ЗУ. @ **local-echo mode** режим локального отображения.

local area network (LAN) ['ləʊkəl 'ɛəriə 'netwɜ:k] локальная (вычислительная) сеть, ЛВС. @ Коммуникационная система, поддерживающая в пределах одного здания или некоторой ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования.

local error ['ləʊkəl 'erə] локальная ошибка. @ Мера точности, используемая на каждом шаге отыскания численного решения обыкновенного дифференциального уравнения.

local optimization ['ləʊkəl 'ɒptɪmaɪzɪʃən] локальная оптимизация. @ 1. Оптимизация программы на уровне выбора машинных команд. 2. Нахождение локального минимума или максимума целевой функции.

local variable ['loukəl 'vɛəɪəbl] локальная переменная. @ Переменная, описываемая в данном блоке или модуле и недоступная вне его.

locally ['loukəlɪ] *adv.* локально. @ **locally-assigned key** локально назначаемый ключ.

locate [lou'keɪt] *v.* 1. находить (*местоположение данных*); 2. размещать, располагать; 3. устанавливать (*позицию курсора на экране дисплея, головки магнитного диска*); 4. обнаруживать, определять место. @ **locate a transmitter** определять местоположение передатчика.

location (loc) [lou'keɪʃən] *n.* 1. положение, местоположение, размещение, расположение; 2. ячейка памяти, адрес ячейки. @ **location counter** счетчик ячеек, счетчик команд.

location operator [lou'keɪʃən 'ɔpə'reɪtə] оператор размещения. @ Оператор в языке программирования, который выдает адрес операнда.

locator [lou'keɪtə] *n.* 1. локатор, устройство ввода позиций; 2. искатель, обнаружитель

logarithm ['lɒɡərɪθəm] *n.* логарифм.

logarithmic ['lɒɡərɪθəmɪk] *adj.* логарифмический. @ **logarithmic base** основание логарифмов. @ **logarithmic calculator** логарифмическое счетное устройство. @ **logarithmic computing instrument (LOCI)** логарифмический вычислительный прибор. @ **logarithmic equation** логарифмическое уравнение. @ **logarithmic multiplier** логарифмическое множительное устройство. @ **logarithmic scale** логарифмическая шкала, логарифмический масштаб. @ **logarithmic search algorithm** алгоритм двоичного поиска. @ **logarithmic search** двоичный поиск, поиск делением пополам.

logarithmics ['ælɡɔːrɪθmɪks] *n.* логарифметика.

logic ['lɒdʒɪk] *n.* 1. логика, логические схемы; 2. алгоритм; 3. логика (наука). @ **logic bomb** логическая бомба (тайно встроенный в программу код, предназначенный для несанкционированного доступа к открытым текстам, ключам и т.д.). @ **logic inverse** логическая инверсия. @ **logic research** исследование в области логики. @ **logic-compatible** логически совместимый.

logic analyzer ['lɒdʒɪk 'ænləɪzə] логический анализатор. @ Устройство отладки цифровых электронных устройств, позволяющее отслеживать и записывать состояния сигналов и логических элементов.

logic operation ['lɒdʒɪk ɔpə'reɪʃən] логическая операция. @ Операция, аргументы которой принимают логические значения.

logic symbols ['lɒdʒɪk 'sɪmbəls] логические символы. @ Набор символов, которые обозначают функции определенных логических вентилей в логических принципиальных схемах.

logic(al) ['lɒdʒɪk(əl)] *adj.* логический. @ **logic(al) circuit** логическая схема. @ **logic(al) computer** вычислительная машина для решения логических задач, логическая вычислительная машина. @ **logic(al) design** 1. логическая схема; 2. синтез логической схемы; 3. логический синтез. @ **logic(al) diagram** 1. логическая схема, схема выполнения логических операций; 2. блок-схема. @ **logic(al)**

element логический элемент, логическая ячейка. @ **logic(al) flowchart** логическая блок-схема. @ **logic(al) function** логическая функция. @ **logic(al) gate** логический вентиль. @ **logic(al) instruction** 1. машинная команда; 2. логическая команда. @ **logic(al) level** логический уровень. @ **logic(al) machine** логическая машина. @ **logic(al) probe** логический пробник.

logic(al) gain ['lɒdʒɪk(əl) geɪn] нагрузочный множитель. @ Измеряется числом схем, на которое может быть одновременно нагружен выход данной (логической) схемы.

logical ['lɒdʒɪkəl] *adj.* 1. логический. @ 1. Относящийся к логическим значениям. 2. Рассматриваемый с точки зрения возможных операций, а не с точки зрения реальной организации; «виртуальный» – обычно понимают большую степень абстракции; «концептуальный» и «абстрактный» относятся больше к рассуждениям и проектированию, чем к функционированию программы. 2. логичный, логический. @ Правильный с точки зрения логики. @ **logical action** логическое действие, логическая операция. @ **logical addition function** функция логического сложения. @ **logical addition** логическое сложение, дизъюнкция. @ **logical axiom** логическая аксиома. @ **logical block number** логический номер блока. @ **logical block** логический блок. @ **logical check** логическая проверка. @ **logical component** логический элемент. @ **logical connective** логическая связка. @ **logical constant** логическая константа. @ **logical data type** логический тип данных. @ **logical input/output control system (LIOCS)** логическая система управления вводом-выводом. @ **logical multiplication function** функция логического умножения. @ **logical multiplication** логическое умножение, конъюнкция. @ **logical operation** 1. логическая операция; 2. логическое действие. @ **logical operator** знак логической операции. @ **logical paradox** логический парадокс. @ **logical product** логическое произведение. @ **logical program** логическая программа. @ **logical programming** логическое программирование. @ **logical value** логическое значение. @ **logical-active function** логически активная функция. @ **logical symbol** логический символ (знак) . @ **logical test** логическая проверка, логический контроль. @ **logical unit** логическое устройство, логический элемент. @ **logical section** логический узел вычислительной машины.

logical address ['lɒdʒɪkəl ə'dres] логический адрес. @ Символический или условный адрес ячейки или области памяти, устройства или узла сети, который переводится в физический адрес соответствующим программным или аппаратным обеспечением.

logical channel number ['lɒdʒɪkəl 'tʃænl 'nʌmbə] номер логического канала. @ Идентификатор виртуального канала, используемый в пакетном интерфейсе, позволяющий нескольким виртуальным каналам одновременно использовать один физический интерфейс.

logical data base ['lɒdʒɪkəl 'deɪtə beɪs] логическая база данных. @ База данных с точки зрения прикладной программы или пользователя.

logical device ['lɒdʒɪkəl di'vaɪs] логическое устройство. @ Системная программа (драйвер), выполняющая операции ввода-вывода по запросам при-

кладных программ. Одному физическому устройству может соответствовать несколько физических или одно физическое устройство может использоваться как несколько логических. Соответствие между логическими и физическими устройствами может меняться во время работы системы.

logical device name ['lɒdʒɪkəl dɪ'vaɪs neɪm] логическое имя устройства, имя логического устройства. @ Строка символов, используемая в программе для обозначения устройства ввода-вывода. Связь с конкретным внешним устройством осуществляется во время выполнения.

logical expression ['lɒdʒɪkəl ɪks'preʃən] логическое выражение. @ Выражение, состоящее из элементарных утверждений, объединенных логическими связками.

logical file ['lɒdʒɪkəl faɪl] логический файл. @ Файл с точки зрения программы; логический файл может быть связан с физическим файлом или внешним устройством.

logical input device ['lɒdʒɪkəl 'ɪnpʊt dɪ'vaɪs] логическое устройство ввода. @ В интерактивной графике – совокупность процедур, с помощью которых прикладная программа взаимодействует с пользователем. Процедуры различных логических вводных устройств обеспечивают ввод координат одной или нескольких позиций, ввод числового значения, ввод текстовой строки, выбор сегмента изображения или пункта меню. В конкретной графической системе логическое устройство может использовать различные физические устройства.

logical name ['lɒdʒɪkəl neɪm] логическое имя. @ Имя, присвоенное объекту на время выполнения программы и используемое внутри этой программы.

logical programming language ['lɒdʒɪkəl 'prɒɡræmɪŋ 'læŋɡwɪdʒ] логические языки программирования. @ Класс языков программирования и подкласс декларативных языков, которые основаны на символической логике.

logical record ['lɒdʒɪkəl 'rekɔ:d] логическая запись. @ Запись с точки зрения ее содержимого, Одна логическая запись может состоять из нескольких физических или быть частью физической записи.

logical shift ['lɒdʒɪkəl ʃɪft] логический сдвиг. @ Операция сдвига двоичного слова вправо с заполнением освобождающихся разрядов нулями; логический сдвиг влево совпадает с арифметическим сдвигом.

logical unit number ['lɒdʒɪkəl 'ju:nɪt 'nʌmbə] логический номер устройства, номер логического устройства. @ В ряде систем программирования – число, используемое в качестве имени логического устройства.

long [lɒŋ] *adj.* 1. длинный; 2. долгий; длительный; *adv.* давно. @ **long key cipher** шифр с длинным ключом. @ **long period** большой период (рекуррентной последовательности). @ **long-term key** долговременный ключ. # **long before** задолго до (того как). # **an hour long** продолжающийся один час. # **mile long** длиною в одну память. # **any (no) longer** больше не. # **as long ago as** пока; поскольку. # **at long range** еще, уже. # **before long** вскоре, скоро. # **for long** надолго. # **in the long run** в конце концов. # **in long stading** длительный, давнишний, застарелый.

long-lived key = long-term key

look [luk] *v.* 1. смотреть (**at**); 2. следить (**after**); 3. предвидеть, предусматривать (**ahead**); 4. искать (**for**); 5. ожидать, предвкушать (**forward**); 6. исследовать (**into**); 7. считать, рассматривать (**on, upon**).@ **look into a cipher** исследовать шифр.

look ahead [luk ə'hed] 1. упреждение.@ Предоставление программе или устройству ресурса до его запроса (например, большего числа блоков, чем запрошено; выборка в сверхоперативную память команд линейного участка раньше, чем программа дойдет до них). 2. просмотр вперед.@ При генерации кода – использование при выборе команды информации о последующих действиях транслируемой программы.

lookahead [lukə'hed] предварительный просмотр.@ **lookahead unit** блок предварительного просмотра.

look-alike [luk,ə'laik] имитация.@ Программа или ЭВМ, обеспечивающие те же возможности и тот же интерфейс, что и прототип, но разработанные независимо и имеющие иную внутреннюю структуру.

look-aside registers [luk,ə'said 'redʒɪstəs] ассоциативная таблица страниц.@ Часть системы управления виртуальной памятью, отражающая соответствие физических и виртуальных страниц и выдающая номер физической страницы по заданному виртуальному адресу.

look-up ['luk'ʌp] *v.* смотреть вверх.@ **look-up operation** операция поиска.

look-up table ['luk'ʌp 'teɪbl] таблица перекодировки, таблица преобразования; справочная таблица.@ Задание отображения в виде таблицы (массива), в которой *i*-й элемент указывает значение, соответствующее *i*.

lose [lu:z] *v.* (**lost**) 1. терять, лишаться; утрачивать; 2. упустить, не воспользоваться.# **to lose sight of** потерять из виду; упустить из виду.

lost [lɒst] *adj.* утраченный, потерянный.@ **lost key** утраченный (потерянный) ключ.

lot [lɒt] *n.* 1. для; 2. участок; 3. масса; 4. партия (изделий).# **a lot of** много.# **lots of** много.

low [lou] *adj.* низкий, малый; младший.@ 1. О разряде или байте – самый правый, представляющий младшую цифру числа. 2. Об области памяти – имеющий меньший адрес.@ **low bit** нулевой бит, нулевой разряд.@ **low bound** нижняя граница (массива).@ **low capacity memory** память малой емкости.@ **low density attack** попытка вскрытия по линии малой плотности.@ **low frequency letter** редко встречающаяся буква.@ **low grade cipher** шифр низкой стойкости (легко вскрываемый шифр).@ **low level scheduler** планировщик нижнего уровня.@ **low order (LO)** младший разряд.@ **low-level implementation** реализация средствами низкого уровня.@ **low-level language** язык низкого уровня.@ **low-priority** низкоприоритетный, имеющий низкий приоритет.@ **low-resolution mode** графический режим с низким разрешением.@ **low-speed encryption** низкоскоростное шифрование.

lower [louə] *v.* понижать; *adj.* 1. нижний; 2. низший. @ **lower bound** нижняя граница. @ **lower bound** нижняя граница (*массива*). @ **lower boundary class** нижняя граница интервала. @ **lower case (ls)** строчная, нижнего регистра (*о буквах*). @ **lower radical** нижний радикал. @ **lower sideband (LSB)** нижняя боковая частота. @ **lower-priority device** устройство с более низким приоритетом.

lowest [ləʊst] *adj.* наименьший. @ **lowest common denominator** наименьший общий знаменатель. @ **lowest common multiple** наименьшее общее кратное. @ **lowest frequency letter** буква с наименьшей частотой встречаемости (в тексте).

М*

machine [mə'ʃi:n] *n.* 1. (шифровальная) машина, шифратор; 2. вычислительная машина, компьютер.

machine address [mə'ʃi:n ə'dres] 1. машинный адрес. @ Адрес в числовом виде. 2. физический адрес. @ **machine arithmetic** машинная арифметика. @ **machine check** машинный контроль. @ **machine computation** вычисление на машине. @ **machine cycle** машинный цикл. @ **machine instruction processor (MIP)** процессор обработки команд. @ **machine instruction** машинная команда, команда машины. @ **machine intelligence** искусственный интеллект. @ **machine language instruction** команда на машинном языке. @ **machine learning** машинное обучение. @ **machine processible form** форма данных, пригодная для обработки на вычислительной машине. @ **machine register** аппаратный регистр, регистр машины. @ **machine run** 1. машинный прогон; 2. работа машины, эксплуатация машины. @ **machine translation** машинный перевод. @ **machine word** машинное слово. @ **machine-independent language** машинно-независимый язык. @ **machine-oriented language** машинно-ориентированный язык. @ **machine-readable** в форме пригодной для ввода в ЭВМ. @ **machine-sensible** в пригодной для ввода в ЭВМ форме.

machine code [mə'ʃi:n koud] 1. машинный код, язык машины. @ Система команд конкретной ЭВМ. 2. машинный код. @ Программа, записанная на языке машины.

machine cryptography [mə'ʃi:n 'kriptou,ra:fi] машинная криптография.

machine error [mə'ʃi:n 'erə] машинная ошибка. @ Ошибка из-за неправильной работы машины.

machine language [mə'ʃi:n 'læŋgwɪdʒ] машинный язык, язык машины. @ Система команд ЭВМ.

machine simulation [mə'ʃi:n ,simju'leɪʃən] машинное моделирование. @ Процесс, в котором одна машина может воспроизводить поведение второй машины.

machine time [mə'ʃi:n taɪm] машинное время. @ 1. Время счета, время центрального процессора. 2. Интервал времени, в течение которого вычислитель-

ная система или терминал в системе разделения времени используются данным пользователем.

machine-dependent [mə'ʃi:n,dɪ'pendənt] машинно-зависимый.@ О программе, языке программирования или методе, которые учитывают особенности архитектуры ЭВМ и могут быть использованы только на ЭВМ определенного типа.

machine-independent [mə'ʃi:n ,ɪndɪ'pendənt] машинно-независимый.@ О программе, языке программирования или методе, не зависящих от особенностей конкретной ЭВМ и пригодных для применения на ЭВМ различных типов.

machine-oriented high-level language [mə'ʃi:n'ɔ:riəntɪd haɪ'levl 'læŋgwɪdʒ] машинно-ориентированный язык программирования высокого уровня.@ Язык программирования со структурами управляющей логики типичного языка высокого уровня, типы и структуры данных которого накладываются на архитектуру машины.

Magic intercepts перехваты "Магии"

main ['meɪn] *adj.* главный; основной.@ **main control** главное (центральное) управление.@ **main frame memory** 1. основная память; 2. оперативная память.@ **main index** главный индекс, первичный индекс.@ **main line** питающая сеть.@ **main memory address register (MMAR)** адресный регистр основного ЗУ.@ **main memory register (MMR)** регистр основного ЗУ.@ **main storage (MSTOR)** оперативная память.@ **main storage data register (MSDR)** регистр данных основного ЗУ.@ **main theorem** основная теорема.@ **main variable** главная (основная) переменная.# **in the main** в основном.

main loop ['meɪn lu:p] основной цикл.@ Самый внешний цикл программы.

main memory ['meɪn 'meməri] оперативная память, основная память, ОЗУ.@ Запоминающее устройство, непосредственно связанное с центральным процессором и предназначенное для данных, непосредственно участвующих в его операциях.

main program ['meɪn 'prəʊgræm] основная программа.@ Часть программы, получающая управление при запуске и вызывающая другие подпрограммы.

main routine ['meɪn ru:'ti:n] основная программа.@ Часть программы, получающая управление при запуске и вызывающая другие подпрограммы.

maintenance ['meɪntɪnəns] *n.* 1. сопровождение, обслуживание.@ Поддержание работоспособности системы и ее модификация в соответствии с изменением предъявляемых к ней требований. 2. содержание; 3. уход; ремонт; 4. эксплуатация.@ **maintenance bit** служебный (дополнительный) двоичный разряд.@ **maintenance key** эксплуатационный ключ (используется для проведения профилактических работ с криптографическим оборудованием).@ **maintenance routine** программа профилактического обслуживания.@ **maintenance standby** дежурство.

major ['meɪdʒə] *adj.* 1. главный; основной; 2. более важный; 3. старший.@ **major control data** управляющие данные высшего уровня.@ **major cycle** главный цикл работы машины.@ **major failure** существенная неисправность.@

major heading основной заголовок. @ **major product** старшие разряды производства.

major key ['meɪdʒe ki:] 1. главный ключ. @ При сортировке по нескольким ключам – ключ, по которому записи упорядочиваются в первую очередь. 2. первичный ключ.

majority ['meɪdʒerɪti] *n.* большинство. @ **majority function** мажоритарная функция, функция «большинства». @ **majority principle** мажоритарный принцип, принцип большинства. @ **majority rule** правило большинства.

majority element (gate) ['meɪdʒerɪti 'elɪmənt (deɪt)] мажоритарный элемент. @ Логический элемент с нечетным числом входов, выход которого согласуется с большинством входов.

make [meɪk] *v.* (**made**) 1. делать; 2. заставлять; 3. способствовать (**for**); 4. компенсировать (**up for**); 5. составлять (**up**); *n.* конструкция; марка @ **make a code** создавать код. @ **make an attack of a cipher** подвергать шифр криптоанализу. # **in the making** в процессе создания (становления, развития). # **it makes all the difference (in the word)** это существенно меняет дело; это очень важно. # **to make allowance for** учитывать; делать допуск (поправку) на что-л. # **to make a long story short** короче говоря. # **to makes itself felt** это дает о себе знать, проявляться. # **to make appearance** появляться. # **to make certain** удостовериться, убедиться. # **to make sure** удостовериться, убедиться. # **to make comparisons** проводить аналогию. # **to make mention of** упоминать о. # **to make provision for** предусматривать; обеспечивать; принимать меры. # **to make sense** иметь смысл. # **to make the best of** использовать что-л. наилучшим образом. # **to make use of** использовать.

manipulate [mə'nɪpju'leɪt] *v.* манипулировать.

manipulation [mə'nɪpju'leɪʃən] *n.* 1. обработка; операции; 2. манипуляция.

manner ['mænə] *n.* 1. способ, метод; образ действий; 2. стиль; манера; 3. *pl.* обычаи, нравы. # **after (in) the manner** по способу. # **all manner of** всевозможные. # **in a manner** в некотором смысле; до известной степени. # **in a broad manner** вообще. # **in such a manner** таким образом; так, чтобы

manual ['mænjuəl] *n.* 1. руководство, описание; справочник; *adj.* ручной; физический. @ **manual aperiodic polyalphabetic substitution cipher** ручной аperiодичный шифр многоалфавитной замены. @ **manual computation** ручное вычисление. @ **manual cryptosystem** ручная криптосистема (все операции по зашифрованию и расшифрованию выполняются вручную). @ **manual encryption** ручное шифрование. @ **manual key distribution** распределение ключей вручную. @ **manual of cryptography** руководство по криптографии. @ **manual remote rekeying** ручной удаленный ввод ключа (процедура, применяемая для смены ключа в расположенном на удалении криптографическом оборудовании и требующая участия в ней местного обслуживающего персонала). @ **manual word generator** устройство задания слов в ручную.

manual control ['mænjuəl kən'troul] ручное управление.@ Управление вычислительной системой, осуществляемое человеком, который может вмешаться в работу в любой момент или в моменты, предусмотренные программой.

manually ['mænjuəlɪ] *adv.* вручную

manufacturer [ˌmænju'fæktʃə] *n.* изготовитель, производитель.@ **manufacturer-installed key** ключ изготовителя (производителя) (шифраппаратуры).

manufacturer's key = manufacturer-installed key

many ['mæni] *adj.* (**more, most**) многие, многочисленные, много; *n.* множество, многие.# **a good many** порядочное количество.# **a great many** громадное количество, множество.# **as many as** столько же, сколько; до (*обычно перед инф.*).# **not so many as** меньше, чем.

map cipher картографический шифр (разновидность шифра замены, в котором в качестве букв шифралфавита используются символы, обычно применяемые для условных обозначений на географических картах)

map [mæp] *n.* географическая карта; *v.* отображать, устанавливать соответствие.

mapping ['mæpɪŋ] *n.* отображение

market ['ma:kɪt] *n.* рынок (сбыта).@ **market for cryptography** рынок криптографических средств.

Markov cipher шифр Маркова

masking [ma:sk] *adj.* маскирующий

masking [ma:skɪŋ] *n.* маскирование.@ Выделение разрядов слова, соответствующих единичным разрядам маски. *adj.* маскирующий.@ **masking cipher** маскирующий шифр.@ **masking effect** эффект маскировки.@ **masking technique** 1. метод масок, метод трафаретов; 2. техника масок, трафаретная техника; 3. технология изготовления масок или трафаретов.

masquerade [ˌmæskə'reɪd] *n.* маскировка, подмена (поведение нарушителя, пытающегося выдать себя за законного пользователя); *v.* маскироваться, выдавать себя за.@ **masquerade as a legitimate user** выдавать себя за легального пользователя.@ **masquerade attack** атака с маскировкой (подменой).

masquerader [ˌmæskə'reɪdə] *n.* имитатор действий законного пользователя

master ['ma:stə] *n.* 1. хозяин; глава; 2. великий художник, мастер; 3. мастер, квалифицированный рабочий; 4. магистр (ученая степень); *v.* овладевать; *adj.* главный.@ **master control** 1. главное управление; 2. центральный пульт управления.@ **master control center (MCC)** главный центр управления.@ **master control routine** 1. главная управляющая программа; 2. основная часть программы управления.@ **master crypto-ignition key** главный ключ инициирования криптографических операций (электронное устройство для добавления новых ключей в набор ключей, используемых для инициирования криптографических операций).@ **master data** основные данные.@ **master interrupt** прерывание от главной управляющей программы.@ **master key (M-key, MK)** мастер-ключ, главный ключ.@ **master mode** привилегированный режим.@ **master mode** режим работы с использованием мастер-ключа (главного ключа)

ча).@ **master program** главная программа.@ **master record** главная запись.@ **master scheduler** главный планировщик.@ **master-slave system** несимметричная система; конфигурация "главный - подчиненный".

master file ['ma:stə faɪl] основной файл.@ Файл, содержащий относительно постоянную информацию о предметной области.

master index ['ma:stə 'indeks] главный индекс, первичный индекс.@ В системе двухуровневой индексации элементы главного индекса указывают, в каком вторичном индексе содержатся ключи соответствующего диапазона.

master tape ['ma:stə teɪp] 1. основная лента.@ Магнитная лента, на которой записан основной файл или его часть. 2. эталонная лента.@ Магнитная лента, на которой записан эталонный вариант программы или данных и с которой делаются копии для распространения или модификации.

match [mætʃ] *v.* 1. сравнивать; 2. сопоставлять (отождествлять).@ В языках обработки списков и языках логического программирования – сравнивать образец с данными; образец может включать элементы, которые должны точно совпадать с соответствующими компонентами данных, элементы, задающие условия, которым должны удовлетворять соответствующие компоненты данных, и элементы, указывающие переменные, которым присваиваются соответствующие компоненты данных при успешном отождествлении. 3. совпадать, соответствовать; отождествляться; 4. подбирать под пару; *n.* 1. пара; ровня; 2. соответствие; 3. состязание, матч.@ **match indicator** индикатор совпадения.@ **match merge operation** операция выборочного слияния данных.@ **match(ed) condition** 1. условие согласования; 2. условие соответствия; 3. условие совпадения в ассоциативном запоминающем устройстве.@ **match/mismatch register** регистр совпадения – несовпадения.

match-all pattern [mætʃ'ɔ:l 'pætən] универсальный образец.@ Элемент образца, отождествляющийся с любой составляющей данных.

match-all symbol [mætʃ'ɔ:l 'sɪmbəl] универсальный образец.@ Элемент образца, отождествляющийся с любым символом.

matched [mætʃt] согласованный.@ **matched filter (MF)** согласованный фильтр.@ **matched spatial filter (MSF)** согласованный пространственный фильтр.

matching ['mætʃɪŋ] *n.* 1. сравнение; 2. сопоставление; отождествление; 3. совпадение, соответствие; 4. согласование, приведение в соответствие (ключей) *adj.* согласованный; соответствующий.@ **matching components** соответствующие компоненты.@ **matching key pair** пара согласованных ключей (для зашифрования и расшифрования сообщений).@ **matching key** согласованный ключ (напр, ключ расшифрования, соответствующий ключу шифрования).@ **matching parentheses** парные скобки.@ **matching word** слово с совпадающим признаком (*при обращении к ассоциативной памяти*).

mathematical [mæθɪ'mætɪkəl] *adj.* математический.@ **mathematical approach** математическое моделирование.@ **mathematical check** математический контроль.@ **mathematical logic** математическая логика.@ **mathematical**

problem математическая задача (проблема).@ **mathematical cryptanalysis** математический криптоанализ.@ **mathematical cryptography** математическая криптография (для шифрования сообщений использует сложные математические операции, напр, такие как возведение очень больших чисел в чрезвычайно высокие степени по модулю произведения двух простых чисел).@ **mathematical-related keys** математически связанные ключи.

mathematical model [ˌmæθɪ'mætɪkəl 'mɒdl] математическая модель. @ Абстрактная или знаковая модель, построенная средствами математики (например, в виде системы уравнений, графа, логической формулы, картинной логики и т. п.).

mathematical programming [ˌmæθɪ'mætɪkəl 'prɒɡræmɪŋ] математическое программирование.@ Область математики, занимающаяся задачами оптимизации.

mathematically [ˌmæθɪ'mætɪkəlɪ] *adv.* математически.

matrix ['meɪtrɪks] *n.* 1. матрица. @ Двумерная таблица, двумерный массив. 2. дешифратор; 3. сетка из регистров; 4. трафарет; 5. кристаллическая решетка.@ **matrix adder** матричный сумматор.@ **matrix address selection system** матричная система выборки адреса.@ **matrix algebra** алгебра матриц, матричная алгебра.@ **matrix calculation** вычисление матриц, матричное вычисление.@ **matrix calculus** матричное исчисление.@ **matrix cipher** матричный шифр.@ **matrix computation** вычисление матриц.@ **matrix formula** формула матричного преобразования.@ **matrix gate** дешифратор.@ **matrix grammar** матричная грамматика.@ **matrix iteration** итерации матрицы.@ **matrix key distribution scheme** матричная схема распределения ключей.@ **matrix norm** норма матрицы.@ **matrix notation** матричная запись.@ **matrix of coupling** матрица соединений (связей) .@ **matrix of the coefficient** матрица коэффициентов.@ **matrix point** ячейка матрицы.@ **matrix power converter (MPC)** матричный преобразователь.@ **matrix representation** матричное представление, матричное выражение.@ **matrix row** строка матрицы.@ **matrix technique** матричный метод.@ **matrix wire** провод матрицы.@ **matrix-updating methods** методы матричных преобразований.

matrix inversion ['meɪtrɪks 'ɪn'vɜːʃən] обращение матрицы.@ Нахождение обратной матрицы.

matter ['mætə] *n.* 1. вещество; 2. материя (*филос.*); 3. предмет, вопрос, дело; *v.* иметь значение.# **as a matter of convenience** для удобства.# **as a matter of course** как нечто само собой разумеющееся.# **as a matter of experience** исходя из опыта.# **as a matter of fact** фактически, на самом деле.# **as a matter of record** на основании полученных данных.# **as matters stand** при существующем положении (дел).# **for that matter** что касается этого, в этом отношении; в связи с этим.# **in a matter of seconds (minutes)** за несколько секунд (минут).# **it is a matter of common knowledge** это общеизвестно.# **no matter** независимо от того, безразлично.# **subject matter** сущность, содержание; предмет (обсуждения и т. п.).# **to put the matter another way** другими словами.

maximal ['mæksiməl] *adj.* максимальный. @ **maximal length sequence (ML-sequence)** последовательность максимальной длины. @ **maximal length shift register (MLSR)** регистр сдвига максимальной длины. @ **maximal period generator** генератор псевдослучайной последовательности с максимальным периодом.

maximize ['mæksimaɪz] *v.* максимизировать.

maximum ['mæksiməm] *n.* максимум, наибольшее значение, максимальное количество; *adj.* максимальный. @ **maximum likelihood estimate (MLE)** оценка методом максимального правдоподобия. @ **maximum likelihood method** метод максимального правдоподобия. @ **maximum principle** принцип максимума. @ **maximum-length sequence** последовательность максимальной длины. @ **maximum a posteriori probability estimation** оценка по методу максимальной апостериорной вероятности. @ **maximum likelihood detector** критерий (детектор) максимального правдоподобия. @ **maximum order complexity of a pseudo-random sequence** сложность максимального порядка псевдослучайной последовательности.

maximally ['mæksiməli] *adv.* максимально. @ **maximally correlation-immune combiner** максимально корреляционностойкий смеситель.

mean [mi:n] *v.* (**meant**) 1. значить, означать; 2. иметь в виду, намериваться; 3. предназначать(ся); 4. подразумевать(ся); *n.* 1. среднее (значение), средняя величина; 2. *pl.* средство, средства; *adj.* средний. # **by means of** посредством. # **by all means** во что бы то ни стало; безусловно. # **by any means** каким бы то ни было образом. # **by no means** никоим образом, ни в коем случае. # **by some means or other** тем или иным образом. # **by which means** посредством чего.

meaning ['mi:nɪŋ] *n.* смысл; значение. # **with meaning** многозначительно.

meaningful ['mi:nɪŋfʊl] *adj.* осмысленный; содержательный (имеющий смысл). @ **meaningful decryption** дешифрование дающее содержательный текст.

meantime ['mi:n'taɪm] *adv.* тем временем. # **in the meantime** тем временем.

measure ['meɪʒə] *n.* 1. мера, масштаб; 2. делитель; 3. критерий; *v.* 1. мерить, измерять; 2. оценивать, определять; 3. иметь размеры. # **in a (some) measure** отчасти, до некоторой степени. # **to take measures** принимать меры.

mechanism ['mekənɪzəm] *n.* 1. механизм (физическое устройство); 2. механизм (логическая концепция машины, которая может быть реализована на практике как физическое устройство или как последовательность логических команд, выполняемых физическим устройством).

mechanistic ['mekənɪstɪk] *adj.* механический. @ **mechanistic cryptography** механическая криптография (для шифрования сообщений использует машины или механизмы, собранные из многих относительно простых компонентов и узлов, которые в совокупности реализуют очень сложное шифрующее преобразование).

medium ['mi:djəm] *n.* 1. носитель (данных). 2. среда передачи данных; 3. среднее число; 4. средство, способ; 5. атмосфера; *adj.* средний, промежуточный. # **through the medium** через, посредством.

medium-speed ['mi:dʒəm'spi:d] *adj.* среднескоростной.@ **medium-speed encryptor** среднескоростной шифратор.

meet [mi:t] *v.* (**met**) 1. встречать(ся); 2. удовлетворять (требование, желание); 3. преодолевать (трудности); 4. пересекать.@ **meet-in-the-middle (MITM)** сведение к середине.@ **meet-in-the-middle attack (MITMA)** атака методом сведения к середине (предложенный американскими криптологами Р. Мерклем, М. Хеллманом метод вскрытия суперпозиций шифров).# **to meet the case** отвечать предъявленным требованиям.

mega- (M) [megə] мега..., М, 10^6 ; в сложных и сложносоставных словах имеет значение мега- (превышение основной единицы измерения в миллион раз).

megabyte (Mbyte) [megə'bait] *n.* мегабайт, Мбайт (2^{20} байт = 1048576 байт).@ **megabyte data encryption** шифрование данных со скоростью ... мегабайт в секунду.

megabit (Mbit) [megə'bit] *n.* мегабит.@ **megabit data encryption** шифрование данных со скоростью ... мегабит в секунду.

memorize ['meməraɪz] *v.* помещать в память (в запоминающее устройство) (компьютера или шифратора).@ **memorize a key** помещать ключ в память (в запоминающее устройство).

memorized ['meməraɪzd] *adj.* запоминаемый, хранимый в памяти (в запоминающем устройстве) (компьютера или шифратора).@ **memorized key** запоминаемый (хранимый и памяти) ключ.

memory ['meməri] *n.* память; оперативная память; запоминающее устройство.@ **memory access controller (MAC)** контроллер доступа к памяти.@ **memory address register** регистр адреса памяти.@ **memory address test (MAT)** проверка адреса ЗУ.@ **memory address** адрес запоминающего устройства.@ **memory capacity** объем памяти.@ **memory cell** 1. ячейка памяти. 2. запоминающий элемент.@ **memory cycle** цикл памяти, цикл обращения к памяти.@ **memory data register (MDR)** регистр данных запоминающего устройства.@ **memory device** накопитель, запоминающее устройство.@ **memory dump** дампы памяти.@ **memory element** элемент памяти, запоминающий элемент, элемент запоминающего устройства.@ **memory expansion card** плата расширения памяти, дополнительная плата памяти.@ **memory fill** заполнение памяти, роспись памяти.@ **memory guard** защита памяти.@ **memory hierarchy** иерархия памяти.@ **memory interface (MI)** интерфейс ЗУ.@ **memory key** ключ (защиты) памяти.@ **memory location** 1. ячейка памяти. 2. адрес ячейки памяти.@ **memory lockout register** регистр блокировки обращений к памяти.@ **memory management unit (MMU)** диспетчер памяти, устройство управления памятью.@ **memory management** распределение памяти.@ **memory map** карта (распределения) памяти.@ **memory matrix** матрица памяти, матрица запоминающего устройства.@ **memory module** модуль (куб) памяти.@ **memory operation** операция в памяти машины или накопителе.@ **memory page** страница памяти, лист памяти.@ **memory pair** запоминающая пара.@ **memory plane** матрица запоминающего устройства.@ **memory protection interrupt** прерыва-

ние по защите памяти. @ **memory register** регистр памяти. @ **memory selection register** 1. регистр выбора блока (модуля) памяти; 2. регистр адреса памяти. @ **memory speed** быстродействие памяти. @ **memory stored control** управление при помощи программы, хранимой в памяти. @ **memory test computer (MTC)** ЭВМ для проверки памяти (ЗУ). @ **memory unit** 1. запоминающее устройство; 2. ячейка памяти. @ **memory upgrade** дополнительная память. @ **memory-map list** список распределения памяти. @ **memory-reference instruction** команда обращения к памяти. @ **memory-to-memory instruction** команда типа «память – память». @ **memory-to-memory move instruction (MOV)** команда пересылки данных из памяти в память.

memory allocation ['meməri 'æləkeɪʃən] распределение памяти. @ Действия транслятора или исполняющей системы для выделения областей памяти объектам (переменным) программы.

memory array ['meməri 'eɪrɪ] массив памяти, область памяти. @ Массив, размещаемый в оперативной памяти.

memory bank ['meməri bæŋk] банк памяти. @ Плата, выполняющая функции запоминающего устройства.

memory compaction ['meməri 'kɒmpækʃən] уплотнение памяти. @ При динамическом распределении памяти – перемещение занятых блоков для объединения мелких свободных блоков в крупные.

memory cycle stealing ['meməri 'saɪkl 'sti:lɪŋ] занятие цикла памяти. @ Приостановка обработки команды процессором на один или несколько тактов для обращения к памяти при обмене или регенерации.

memory interleaving ['meməri ,ɪntə'li:vɪŋ] расслоение памяти. @ Размещение элементов памяти с последовательными адресами в физически разных блоках памяти.

memory lock ['meməri lɒk] замок памяти. @ Код в дескрипторе сегмента или страницы виртуальной памяти, используемый системой защиты памяти для ограничения доступа; к сегменту могут обращаться только процессы, имеющие в своем дескрипторе соответствующий ключ.

memory mapping ['meməri mæ-pɪŋ] управление памятью. @ В архитектуре ЭВМ с оперативной памятью, большей адресного пространства, – средства аппаратного отображения адресного пространства на различные области физической оперативной памяти; средства отображения могут программно включаться и отключаться.

memory paragraph ['meməri 'pærəgrɑ:f] параграф памяти. @ Единица адресации и управления памятью меньшая, чем страница; обычно параграф равен 16 байт.

memory protection ['meməri prə'tekʃən] защита памяти. @ При обращении к памяти – проверка принадлежности слова к адресному пространству задачи.

memoryless ['memərɪles] *adj.* без запоминания.

mention [menʃən] *v.* упоминать; упоминать о; ссылаться на что-л. # **not to mention** не говоря уже о. # **to mention (name) only (but) a few** не говоря уже о многих других. # **to make mention of** упоминать о

MERCURY = CHALET

mere [mie] *adj.* сущий; явный; простой. # **the mere (fat etc.)** один лишь (*факт и т. н.*).

Merkle's channels каналы Меркля (множество открытых каналов связи: телефонных, телексных, радиовещательных, телевизионных, почтовых и т.д.).

Merkle's puzzle "шарада" Меркля.

Mersenne prime простое число Мерсена (простое число вида 2^{n-1}).

message (MSG) ['mesɪdʒ] *n.* 1. сообщение. @ Блок данных, представляющий для пользователя единое целое. 2. запрос. @ В объектно-ориентированном программировании – имя операции и список фактических параметров; соответствует вызову процедуры в процедурном программировании. 3. посылка, сигнал. @ **message authenticating code key** ключ с кодом аутентификации сообщения. @ **message authenticating code (MAC)** код аутентификации сообщения. @ **message authentication code (MAC)** код сообщения с паролем. @ **message beginning character** признак начала сообщения. @ **message digest (MD)** сжатие (хэширование) сообщения. @ **message digit** разряд (место) в сообщении, символ в сообщении. @ **message entropy** энтропия сообщений. @ **message exchange** 1. аппаратура обмена сообщениями; 2. аппаратура сопряжения. @ **message exhaustion attack** атака путем перебора всех возможных вариантов сообщения. @ **message expansion** расширение сообщения (при зашифровании). @ **message format** формат сообщения. @ **message indicator** индикатор сообщения (битовый набор, передаваемый по каналу связи для синхронизации работы криптографического оборудования). @ **message key (MK)** разовый ключ. @ **message keying element** элемент ключа, изменяемый для каждого сообщения. @ **message passing** передача сообщений. @ **message preparation for encryption** подготовка сообщения к зашифрованию. @ **message residue class** класс вычетов сообщений. @ **message Security Protocol (MSP)** Протокол безопасности сообщений. @ **message source** источник сообщений. @ **message space** пространство сообщений. @ **message substitution** подмена сообщений (тип угрозы в теории аутентификации информации). @ **message transmission rate** скорость передачи информации. @ **message wiretapping** перехват сообщений с подключением к проводной линии связи (перехват сообщений по отводному каналу).

message header ['mesɪdʒ 'hedə] заголовок сообщения. @ Начальная часть сообщения, содержащая его описание: коды адреса и источника, длину, время отправления.

message queuing ['mesɪdʒ 'kju:ɪŋ] организация очередей сообщений. @ Процесс хранения сообщения в сетевом узле коммутации сообщений в период занятости имеющихся ресурсов на передаче другого сообщения следующему узлу по маршруту к пункту назначения.

message switching ['mesɪdʒ 'swɪtʃɪŋ] коммутация сообщений.@ Метод переключения каналов передачи данных, который не требует физических каналов между отправителем и получателем до того как установится связь.

message trailer ['mesɪdʒ 'treɪlə] завершитель сообщения.@ Часть сообщения, указывающая на его окончание и содержащая контрольную информацию (например, контрольную сумму).

message reordering attack = ordering attack

messaging ['mesɪdʒɪŋ] *n.* обмен сообщениями, передача сообщений.

meteorological [ˌmi:tjərə'lɒdʒɪkəl] *adj.* метеорологический.@ **meteorological code** метеорологический код (применяется специально для кодирования сводок и прогнозов погоды).

method ['meθəd] *n.* 1. метод; 2. правило.@ В языке Smalltalk и в объективно-ориентированном программировании – описание действия, выполняемого при реакции на запрос. 3. система, порядок; 4. способ.@ **method of comparison** способ сравнения.@ **method of elimination** способ исключения неизвестных.@ **method of encipherment** метод шифрования.@ **method of images** метод изображений.@ **method of least squares** метод наименьших квадратов.@ **method of steepest descent** метод скорейшего спуска.@ **method of successive approximations** метод последовательных приближений, итерационный метод.@ **method of successive correction** метод (способ) последовательных поправок.@ **method of successive substitutions** метод последовательных подстановок.@ **method of undetermined coefficients** метод неопределенных коэффициентов.

method of selected point ['meθəd əv sɪ'lektɪd pɔɪnt] метод выборочных точек.@ Метод построения кривых по выборочным точкам.

method of encryption = method of encipherment

microdot ['maɪkrou'dɒt] *n.* микроточка (многократно уменьшенная фотокопия документа).

microprocessor (unit) (MPU, μ P) ['maɪkrou'prəʊsesə ('ju:nɪt)] *n.* микропроцессор.@ Большая интегральная схема (БИС), способная выполнять функции центрального процессора.@ **microprocessor control unit (MCU)** микропроцессорное устройство управления.@ **microprocessor-based cryptosystem** крипто-система с микропроцессором (для выполнения криптографических преобразований).

Microsoft (MS) Challenge Handshake Authentication Protocol (MS CHAP) Протокол аутентификации типа вызов-рукопожатие корпорации "Майкрософт".

Microsoft Point-to-Point Encryption protocol (MPPE) криптографический протокол корпорации "Майкрософт" для одноранговых сетей.

middle person = meet-in-the-middle

middle ['mɪdl] *n.* середина; *adj.* средний; *v.* поместить в середину.@ **middle wheel** средний шифрдиск (второй по счету шифрдиск в трехдисковой модификации "Энигмы").

military ['militəri] *adj.* военный.@ **military cryptanalysis** военный криптоанализ.

mimic ['mimik] *v.* имитировать; *adj.* имитирующий.@ **mimic resistance** имитостойкость.@ **mimic the action of a cipher machine** имитировать работу шифратора.

mind [maɪnd] *n.* 1. ум; 2. память; 3. мнение; *v.* возражать.# **to bear (to have, to keep) in mind** помнить, учитывать, иметь в виду.# **to my mind** по моему мнению.# **with this in mind** имея это в виду.

minimal ['minɪml] *adj.* минимальный.@ **minimal cover time** минимальное время защиты (минимальное время, которое шифрсистема противостоит попыткам ее вскрыть для всех возможных атак против нее).@ **minimal key-length** минимальная длина ключа.@ **minimal polynomial** минимальный полином.

minimum ['mɪnɪmə] *n.* минимум.@ **minimum mean square error estimation** оценка по минимуму среднеквадратичной ошибки.

minimum disclosure proof = zero knowledge proof

minuend cryptosystem *n.* = **subtractive cryptosystem**

mixed ['mɪkst] *adj.* смешанный.@ **mixed cipher alphabets** смешанные шифралфавиты.@ **mixed cipher alphabets recovery** восстановление смешанных алфавитов.

mixing ['mɪksɪŋ] *n.* смешение.@ **mixing-key cryptoalgorithm** криптоалгоритм смешения ключевого и информационного потока.

mnemonic [nɪ:'mɒnɪk] *adj.* легко запоминаемый.@ **mnemonic code** мнемонический код.@ **mnemonic diagram** мнемоническая (графическая) схема.@ **mnemonic symbol** мнемонический знак (символ).@ **mnemonic key** легко запоминаемый ключ.

mode [moʊd] *n.* 1. режим (работы); 2. мода.@ Характеристика дискретной случайной величины, равная наиболее часто применяемому значению. 3. метод, способ; 4. форма, вид; 5. вид колебаний.@ **mode of operation** режим работы (шифратора).

modem (modulator and demodulator) ['moʊdəm] (['mɒdju'leɪtə ænd di:'mɒdju'leɪtə]) *n.* модем, модулятор-демодулятор.@ Устройство, преобразующее цифровые сигналы в аналоговую форму и обратно для передачи их по линии связи аналогового типа, например, по телефону.@ **modem-encryptor** модем с шифратором.

modern ['mɒdə] *adj.* современный; новый.@ **modern cryptanalysis** современный криптоанализ.

modification [ˌmɒdɪfɪ'keɪʃən] *n.* изменение (модификация), определение, видоизменение.@ **modification attack** атака с целью изменения (содержания) сообщения.@ **modification detection encryption algorithm** алгоритм шифрования с обнаружением изменений (в шифртексте).@ **modification of a cipher machine** модификация шифратора.

modified ['mɒdɪfaɪd] *adj.* модифицированный, измененный.@ **modified one-time key (mot-key)** модифицированный одноразовый ключ.

modify ['mɒdɪfaɪ] *v.* изменять (модифицировать), переадресовать.@ **modify messages from a legitimate transmitter** изменять сообщения законного передатчика.

modular ['mɒdjulə] *adj.* модульный.@ **modular arithmetic cipher** шифр на основе модульной арифметики.@ **modular arithmetic** арифметика в остаточных классах.@ **modular block (MB)** модульный блок; модуль.@ **modular concept** 1. модульный принцип (способ) конструирования; 2. модульный счетчик.@ **modular design** модульная (блочная) конструкция.@ **modular exponentiation** модульное возведение в степень.@ **modular hardware** 1. модульная конструкция; 2. модульная аппаратура.

modular programming ['mɒdjulə 'prɒɡræmɪŋ] модульное программирование.@ Организация программы в виде совокупности модулей со строгим соблюдением правил их взаимодействия; описание модуля состоит из описания интерфейса и описания реализации.

modulator ['mɒdjulətə] *n.* модулятор.

module ['mɒdju:l] *adv.* по модулю; *n.* модуль.@ 1. Относительно независимая часть программы. 2. Секция внешнего запоминающего устройства, содержащая один том данных.@ **module invariant** инвариант модуля.@ **module specification** точное определение результатов, достижение которых требуется от программного модуля.@ **module strength** прочность модуля.@ **module test mode (MTM)** режим испытаний на уровне модуля.@ **module under test (MUT)** испытуемый модуль.@ **modulo 2 adder** сумматор по модулю 2.@ **modulo 2 multiplier** умножитель по модулю 2.@ **modulo n arithmetic** арифметика по модулю n.@ **modulo n check** контроль по модулю n.@ **modulo n counter** счетчик по модулю n.@ **modulo n divider** схема пересчета по модулю n.@ **modulo product** произведение по модулю.@ **modulo-adding** суммирование по модулю.@ **modulo-exponentiation** возведение в степень по модулю.@ **modulo-L Vernam system** система Вернама по модулю L (одноразовый шифровальный блокнот).

modulo operation ['mɒdju:lə ɔpə'reɪʃən] операция по модулю.@ Арифметическая операция, в которой результатом является остаток от деления одного целого числа на другое.

modulus ['mɒdju:ləs] *n.* модуль (числа или конгруэнтности), основание системы счисления, показатель степени, коэффициент.@ **modulus of a complex number** модуль комплексного числа.@ **modulus of a congruence** модуль сравнения.@ **modulus of congruence** модуль конгруэнтности.@ **modulus of continuity** модуль непрерывности.@ **modulus of natural logarithms** модуль натуральных логарифмов.

"mole" [maʊl] *n.* "крот", "двойной" агент (перевербованный сотрудник спецслужбы).

monalphabetic *adj.* = **monoalphabetic**

moment ['moumənt] *n.* 1. момент, миг; 2. важность, значение.# **of great moment** имеющий большое значение; важный.# **of little moment** имеющий небольшое значение; неважный.# **the moment** в тот момент, когда.@ **moment of a frequency distribution** момент распределения.

momentum [mou'məntəm] *n.* (*pl.* **momenta**) 1. скорость движения; 2. толчок; импульс; движущая сила; 3. движущая сила; 4. инерция (движения тела); 5. кинетическая энергия.# **because of momentum** по инерции; по привычке.# **to gain momentum** развивать скорость; усиливаться.# **to grow in momentum** развивать скорость; усиливаться.

monitor ['mɒnɪtə] *n.* 1. управляющая программа, монитор; 2. дисплей; 3. монитор.@ В языках программирования – высокоуровневый механизм взаимодействия и синхронизации процессов, обеспечивающий организацию доступа к неразделенным ресурсам. Монитор состоит из процедур доступа к ресурсу, каждая из которых может быть вызвана только из одного процесса одновременно. Процесс, пытающийся обратиться к процедуре монитора, когда монитор обслуживает другой процесс, ставится в очередь ожидания; *v.* наблюдать за радиообменом, вести радиоперехват; наблюдать, следить.@ **monitor counter** контрольный счетчик.@ **monitor communications** наблюдать за сообщениями.@ **monitor program** управляющая программа.

monitoring ['mɒnɪtərɪŋ] *n.* проверка, контроль, мониторинг.

monoalphabetic [ˌmɒnə'ælfəbetɪk] *adj.* моноалфавитный.@ **monoalphabetic cipher** моноалфавитный шифр.

monofigure [ˌmɒnə'fɪɡə] *n.* одна цифра.@ **monofigure-dinome cipher system** одно-двухцифровая шифрсистема (при зашифровании одна часть символов открытого текста заменяется на одну цифру, а другая – на две).

monofigure-dinome = **monofigure-dinome cipher system**

monographic [ˌmɒnə'græfɪk] *adj.* монографический, однобуквенный.@ **monographic cipher** монографический шифр (осуществляет побуквенное преобразование открытого текста в зашифрованный).@ **monographic Phi test** однобуквенный ф-тест.

more [mɔ:] *adj.* (*сравнит. степень от much, many*) 1. большой; 2. еще; *adv.* 1. более; 2. еще.# **more often than got** нередко.# **more recently** совсем недавно.# **more than once** не раз, неоднократно.# **all the more** тем более.# **any (no) more** больше не.# **once more** еще раз.# **(all) the more so** тем более (что).# **so much the more** тем более (что).

most [məʊst] *adj.* (*превосх. степень от much, many*) наибольший; *adv.* больше всего; очень; *n.* большинство; большая часть.@ **most frequently occurring letter in a language** наиболее часто встречаемая буква языка.@ **most significant character** самый старший знак.# **most directly** сразу.# **most probably** по всей вероятности.# **a most interesting book** очень (весьма) интересная книга.# **at most** самое большее; в лучшем случае.

motion ['mouʃən] *n.* 1. движение; 2. побуждение; 3. предложение (*на собрании*).# **to bring (put) forward a motion** вносить предложение.# **to carry the motion** при-нять предложение.# **to reject the motion** отклонить предложение.

mount [maunt] *v.* 1. подниматься; 2. монтировать; 3. предпринимать, организовывать; *n.* 1. установка; монтирование; 2. крепление, опора.@ **mount a cryptanalytic attack** предпринимать (организовывать) криптоаналитическую атаку.

much [mʌtʃ] *adj.* (**more; most**) много; *adv.* 1. очень много, значительно; 2. почти.# **much (about) the same** почти одно и то же; почти такой же.# **much as** как бы много ... ни; почти так же ... как.# **much of** большая (значительная часть) чего-л.# **much of a size (a height etc.)** почти такого же размера (той же высоты и т. п.).# **much more likely** по всей вероятности.# **as much** столько же.# **as much as** до (*обычно перед цифрами*); столько же, сколько.# **as much as to say** равносильно тому, что сказать.# **however much** сколько бы ни.# **in as much as** поскольку; ввиду того, что.# **so much for (the theory)** это все, что касается (теории).# **so much the better** тем лучше.# **so much the more** тем более (что).# **so much the worse** тем хуже.

multi- ['mʌlti] в сложных и сложносоставных словах имеет значение много-; мульти-.@ **multi-algorithmic encryption** мультиалгоритмическое шифрование (с использованием нескольких алгоритмов).@ **multi-algorithmic** мультиалгоритмический.@ **multi-channel encryption** многоканальное шифрование.@ **multi-channel** многоканальный.@ **multi-dimensional encryption** шифрование с многомерными преобразованиями.@ **multi-dimensional** многомерный.@ **multi-encryption** многократное шифрование (на разных ключах).@ **multi-function encryptor** многофункциональный шифратор.@ **multi-function** многофункциональный.@ **multi-key** многоключевой.@ **multi-key memory** память для хранения ключей различного назначения.@ **multi-level encryption** многоуровневое шифрование.@ **multi-level key distribution** многоуровневое распределение ключей.@ **multi-level key management** многоуровневое управление ключами.@ **multi-level** многоуровневый.@ **multi-nomial** многочленный, полиномиальный; *n.* многочлен, полином.@ **multi-party** состоящий из нескольких участников.@ **multi-party protocol** протокол обмена сообщениями между несколькими абонентами.@ **multi-sequence shift register** регистр сдвига, порождающий несколько последовательностей.

multiliteral ['mʌlti'litərəl] *adj.* многозначный, многобуквенный.@ **multiliteral cipher alphabet** многозначный шифралфавит (служит для замены одного знака открытого текста на несколько знаков шифрованного).@ **multiliteral cipher system** многобуквенная шифросистема (при зашифровании каждый символ открытого текста заменяется на несколько символов шифрованного).

multiple ['mʌltipl] *adj.* многократный; *n.* кратное число @ **multiple encryption method** метод многократного шифрования (на различных ключах).@ **multiple iterated knapsack cryptosystem** ранцевая криптосистема с многократными итерациями.@ **multiple mapping** многократное отображение.@ **multiple**

substitution cipher шифр многократной замены. @ **multiple substitution (multi-substitution)** многократная замена.

multiple ['mʌltɪpl] в сложных и сложносоставных словах имеет значение много-, мульти-. @ **multiple-instruction (multiple-data) (MIMD)** характеризующийся наличием многих потоков команд (многих потоков данных) в компьютерной архитектуре. @ **multiple-key** многоключевой; имеющий несколько ключей. @ **multiple-key cipher** многоключевой шифр. @ **multiple-key encryption** шифрование на нескольких ключах. @ **multiple-polynomial** мультиполиномиальный. @ **multiple-polynomial Quadratic Sieve (MPQS)** квадратичное решето (один из алгоритмов разложения целого числа на множители). @ **multiple-stage** многоступенчатый. @ **multiple-stage encryption** многоступенчатое шифрование.

multiplexer (MUX, mux, MPX) ['mʌltɪpleksə] *n.* мультиплексор; концентратор. @ Устройство, обеспечивающее одновременную работу нескольких абонентов (устройств) по одному каналу, группируя сигналы нескольких подканалов и посылая их в один канал с более высокой пропускной способностью. На другом конце происходит «демультиплексирование», для выделения сигналов отдельных каналов. «Концентратор» обычно подразумевает использование для подключения нескольких терминалов по одному физическому каналу.

multiplexing ['mʌltɪpleksɪŋ] *n.* мультиплексирование, уплотнение. @ Передача данных для нескольких устройств (подканалов) по одному физическому каналу.

multiplexor channel ['mʌltɪpleksə 'tʃænl] мультиплексный канал.

multiplicand [ˌmʌltɪplɪ'kænd] *n.* множимое. @ **multiplicand gate** вентиль множимого. @ **multiplicand register** регистр множимого.

multiplication [ˌmʌltɪplɪ'keɪʃən] *n.* 1. умножение; 2. усиление. @ **multiplication algebra of an algebra** алгебра умножений алгебры. @ **multiplication by constant** умножение на постоянную величину. @ **multiplication factor** 1. коэффициент усиления; 2. коэффициент умножения. @ **multiplication of series** умножение рядов.

multiplication time [ˌmʌltɪplɪ'keɪʃən taɪm] время умножения. @ Время, за которое процессор выполняет команду умножения.

multiplicator [ˌmʌltɪplɪ'keɪtə] *n.* мультипликатор.

multiplicity [ˌmʌltɪ'plɪsɪti] *n.* кратность, разнообразие, многообразие, многочисленность.

multiplier ['mʌltɪplaɪə] *n.* 1. множитель, сомножитель; 2. устройство умножения. @ **multiplier quotient register** регистр множителя частного. @ **multiplier register** ['mʌltɪplaɪə 'redʒɪstə] регистр множителя.

multiply ['mʌltɪplaɪ] *v.* 1. множить, умножить; 2. увеличивать; 3. умножать (by). @

multiply connected ['mʌltɪplaɪ kə'nektɪd] многосвязанный. @ Свойство узла сети связи, который имеет линии цепи или каналы, соединяющие его с бли-

жайшими узлами (одним или несколькими). Если происходит какое-либо нарушение одного соединения, узел остается работоспособным благодаря возможности связи по другим каналам.

multiplying ['mʌltɪplaɪŋ] *n.* умножение; *adj.* множительный, умножающий.@ **multiplying circuit** схема умножения.@ **multiplying instruction** команда умножения.@ **multiplying order** команда умножения.

multipoint ['mʌltɪpɔɪnt] *adj.* многоточечный.

multipoint connection ['mʌltɪpɔɪnt kə'nekʃən] многоточечное соединение.@ Параллельное соединение нескольких терминалов.

multipoint line ['mʌltɪpɔɪnt laɪn] многоточечная линия, моноканал.@ Линия передач данных, которая соединяет более двух точек (станций, узлов и т. п.).

multiplicative ['mʌltɪplɪ'keɪtɪv] *adj.* мультипликативный.@ **multiplicative cipher** мультипликативный шифр.@ **multiplicative inverse element** обратный элемент по умножению.@ **multiplicative knapsack cryptosystem** мультипликативная ранцевая криптосистема.

multiprocessor ['mʌltɪ'prəʊsesə] *adj.* мультипроцессорный, многопроцессорный; *n.* мультипроцессор (компьютер, имеющий больше одного процессора).

multiregister ['mʌltɪ'redʒɪstə] *adj.* многорегистровый.@ **multiregister generator** многорегистровый генератор (ключевой/шифрующей последовательности).

multisignature ['mʌltɪ'sɪɡnətʃə] *n.* (цифровая) подпись нескольких лиц (пользователей).

multistep ['mʌltɪ'steɪp] *adj.* многошаговый.@ **multistep key generator** многошаговый генератор ключей.

multiuser ['mʌltɪ'juːzə] *adj.* многопользовательский.@ **multiuser cryptographic techniques** многопользовательские криптографические методы.

mutual ['mjuːtʃuəl] *adj.* взаимный.@ **mutual information** взаимная информация.@ **mutual key** взаимный ключ (общий для нескольких участников сеанса связи).

mutual exclusion ['mjuːtʃuəl ɪks'kluːʒən] взаимное исключение.@ Отношение между процессами, характеризующее тем, что определенная часть каждого из них называемая критической секцией, не должна выполняться, пока выполняется критическая секция другого процесса.

MH knapsack cryptosystem ранцевая криптосистема Меркля-Хеллмана.

N*

name [neɪm] *n.* 1. имя.@ Строка символов, идентифицирующая: адрес, файл, программу, переменную, тип, константу, устройство, пользователя или другой объект. 2. имя, название, наименование (алгоритма шифрования); *v.* на-

зывать. @ **name the enemy ciphers after sea creatures** давать шифрам противника имена морских тварей. # **to name (mention) only a few** не говоря уже о других.

named [neɪmt] *adj.* амер. безномерной. @ **named key** безномерной ключ (предназначен для отдельной криптографической операции или для конкретного узла шифратора).

nastygram ['næstɪ'græm] *n.* мерзограмма (сообщение, которое используется для взлома криптографического протокола).

national ['neɪʃənəl] *adj.* национальный.

National Bureau of Standards (NBS) Национальное бюро стандартов (USA).

National Computer Security Center (NCSC) Национальный центр защиты компьютеров (американское государственное ведомство, занимающееся внедрением защищенных компьютерных систем в правительственных учреждениях USA, а также координирующее разработку и анализ таких систем).

National Institute of Standards and Technology (NIST) Национальный институт стандартов и технологии (USA).

National Security Agency Scientific Advisory Board (NSASAB) Научно-консультационный совет Агентства национальной безопасности (USA).

National Security Agency (NSA) Агентство национальной безопасности (Национальное агентство безопасности) (правительственное ведомство USA, занимающееся перехватом и дешифрованием сообщений). @ **NSA cryptographer** криптограф из NSA. @ **NSA domestic intelligence activity** разведывательная деятельность NSA внутри USA. @ **NSA employee** сотрудник NSA. @ **NSA Research Group** Исследовательская группа NSA. @ **NSA staff** штат служащих NSA. @ **NSA supplier** поставщик NSA. @ **NSA-provided algorithm** алгоритм, предоставленный NSA. @ **NSA-sponsored** финансируемый NSA.

National Cryptologic Museum Национальный музей криптологии (USA).

native ['neɪtɪv] *adj.* внутренний. @ **native key** внутренний (для криптографического устройства) ключ. @ **native mode** режим работы в собственной системе команд. @ **native-mode language** язык, транслируемый в собственную систему команд.

native-mode compiler ['neɪtɪv'məʊd kəm'paɪlə] «родной» транслятор. @ Транслятор, порождающий объектный код в собственной системе команд той машины, на которой выполняется трансляция.

nature ['neɪtʃə] *n.* 1. природа; 2. сущность; 3. характер; 4. натура; 5. род, сорт, тип. # **by nature** по природе; по натуре. # **in (of) the nature** напоминающий, такого же рода, как; имеющий характер. # **in the nature of things** в силу природы вещей; естественно, неизбежно. # **in the course of nature** при естественном ходе вещей. # **true to nature** реалистический; как живой. # **to be of a similar nature** носить одинаковый характер.

Navaho *n.* = **Navajo**

Navajo code код навахо (использование вооруженными силами USA языка индейского племени навахо для засекречивания военных радиопередач во время первой и второй мировых войн).

Navajo *n.* навахо (североамериканские индейцы).

naval ['neɪvəl] *adj.* военно-морской. @ **naval cipher** военно-морской шифр.

near [niə] *adv., prp.* близко, около; *adj.* близкий. # **near by** рядом, близко.

necessity [nɪ'sesɪti] *n.* 1. необходимость; 2. неизбежность. # **of necessity** неизбежно, обязательно; по необходимости.

negligible ['neglɪdʒəbl] *adj.* незначительный, ничтожный, пренебрежимо малый. @ **negligible probability** пренебрежимо малая вероятность.

negligibly ['neglɪdʒəblɪ] *adv.* незначительно.

negotiate [nɪ'gəʊʃieɪt] *v.* договариваться. @ **negotiate separate keys** договариваться об использовании различных ключей.

negotiation [nɪ'gəʊʃi'eɪʃən] *n.* согласование. @ Диалог между двумя виртуальными терминалами сети передачи данных для согласования параметров, которые будут использоваться в дальнейшей работе.

negotiated *adj.* = **agreed-upon**

network (NET, net) ['netwɜ:k] *n.* 1. сеть. @ 1. Сеть ЭВМ, сеть передачи данных. Выбор термина «сеть ЭВМ» или «сеть передачи данных» зависит от рассматриваемых функций сети, а не от свойств сети. 2. Связной ориентированный граф. 2. схема. @ **network attack cryptosystem** сетевая криптосистема. @ **network attack subscriber** абонент сети. @ **network attack** сетевая атака (для вскрытия ключа шифра используются вычислительные ресурсы распределенной компьютерной сети). @ **network attack** сетевой ключ. @ **network calculator** схемный анализатор. @ **network control protocol** протокол управления сетью. @ **network data base system** сетевая система управления базами данных (СУБД). @ **network description language (NDL)** язык описания схем. @ **network file system (NFS)** сетевая файловая система. @ **network generation** генерация сетевых средств (*при генерации операционной системы*). @ **network interconnection** объединение сетей. @ **network processor** сетевой процессор. @ **network virtual** виртуальный терминал сети.

network (layer) protocol ['netwɜ:k ('leiə) 'prəʊtɜ:kɔl] протокол сетевого уровня, сетевой протокол. @ Уровень протокола сети передачи данных, регламентирующий обмен порциями данных (пакетами) между двумя станциями сети.

network address ['netwɜ:k ə'dres] сетевой адрес. @ Адрес узла сети ЭВМ.

network architecture ['netwɜ:k 'a:kɪtektʃə] архитектура сети ЭВМ; архитектура сети передачи данных. @ Общее описание сети, включающее топологию сети, способ кодирования и передачи информации, методы адресации.

network data base ['netwɜ:k 'deɪtə beɪs] сетевая база данных. @ База данных, основным понятием которой является связь типа «один-ко-многим», причем один и тот же объект может участвовать в произвольном числе таких связей. Сетевая база данных состоит из записей, объединенных в наборы.

network delay ['netwə:k dɪ'leɪ] сетевая задержка.@ Время передачи по сети.

network front-end ['netwə:k end frɒnt] сетевой процессор.@ Вспомогательный процессор или ЭВМ, обеспечивающие связь вычислительной системы с сетью ЭВМ.

network layer ['netwə:k 'leiə] сетевой уровень.@ Основной уровень взаимодействия в сети передачи данных, реализующий обмен порциями данных (пакетами) между двумя станциями сети. Размер пакета ограничен надежностью и составляет, как правило, от 100 до 50 байтов. На сетевом уровне происходит маршрутизация, обеспечивающая передачу пакетов через несколько каналов по одной или нескольким сетям. Сетевой уровень выполняет обработку адресов, а также мультиплексирование.

network protocol ['netwə:k 'prəʊtəkɒl] сетевой протокол.@ Совокупность правил, регламентирующих передачу информации в сети.

network structure ['netwə:k 'strʌktʃə] сетевая структура.@ Организация записей, при которой на одну порожденную запись может ссылаться несколько исходных.

network topology ['netwə:k tə'pɒlədʒɪ] топология сети, конфигурация сети.@ Схема связей между узлами передачи данных.

network attack-based cryptosystem = **network attack cryptosystem**

never ['nevə] *adv.* никогда.# **never before** никогда еще.# **never more** никогда.

new [nju:] *adj.* 1. новый, обновленный; 2. иной, другой; *adv.* ново-, свежее, вновь, недавно (*обычно в сложных словах*).@ **new DES** обновленный DES-алгоритм.@ **"New directions in cryptography"** "Новые направления в криптографии" (статья американских криптологов У. Диффи и М. Хеллмана, публикация которой в 1975 г. ознаменовала наступление эры криптологии с открытыми ключами).# **new-born** возрожденный; новорожденный.# **new-built** вновь выстроенный.

next [nekst] *adj.* следующий, ближайший; *adv.* затем; *prp.* около.# **next but one** предыдущий.# **next to nothing** почти ничего.# **next to the last** предпоследний.

no [nou] *adj.* никакой; означает запрет.@ **no foreigners (NOFORN)** иностранцам вход воспрещен (применяется в USA для ограничения доступа иностранных граждан в секретные зоны на американских станциях перехвата, расположенных за рубежом).# **no longer** больше не.# **no more** больше не.# **no matter** безразлично, неважно.# **no sooner ... than** как только.

node [nəʊd] *n.* 1. вершина (*дерева или графа*); 2. узел (*сети передачи данных или сети ЭВМ*).@ **node computer** ЭВМ – узел сети.@ **node encryption** шифрование в узлах (сети связи) .@ **node key** узловой ключ.@ **node splitting** расщепление узлов.@ **node-to-node encryption** межузловое шифрование.

noise [nɔɪz] *n.* шум, помехи.@ Любой сигнал, который возникает в системе и не является передаваемым полезным сигналом.@ **noise sequence** шумовая

последовательность. @ **noise digit** цифра в освобождающемся при сдвиге разряде. @ **noise factor (NF)** коэффициент шума. @ **noise generator (NSGN)** шумовой генератор. @ **noise immunity** помехоустойчивость. @ **noise limiter (NL, NLT)** ограничитель шумов. @ **noise margin** запас помехоустойчивости. @ **noise meter (NM)** измеритель относительного уровня шумов. @ **noise pattern** картина шумов. @ **noise power ratio (NPR)** относительный уровень собственных шумов канала. @ **noise reduction (NR)** шумопонижение. @ **noise reduction system (NRS)** система шумопонижения. @ **noise sequence** шумовая последовательность; случайная последовательность. @ **noise source** источник помех. @ **noise suppression circuit (NSC)** схема шумоподавления. @ **noise-equivalent power (NEP)** эквивалентная мощность шума. @ **noise-equivalent temperature (NET, net)** эквивалентная шумовая температура. @ **noiseless channel** канал без помех. @ **noiseless coding** помехоустойчивое кодирование. @ **noise-to-signal ratio (NSR)** отношение шумсигнал. @ **noisy channel** канал с помехами.

noise mode ['nɔɪz moʊd] шумовой метод. @ Режим работы, который иногда применяется при нормализации чисел с плавающей запятой.

nomenclator ['noumen,kleitə] *n.* номенклатор (гибридная криптографическая система, являющаяся наполовину кодом, наполовину шифром).

non- ['nɒn-] *pref.* обозначает отрицание. @ **non von Neumann computer** не-фон-неймановская ЭВМ. @ **non-alphanumeric** небуквенно-цифровой. @ **non-cryptographic** некриптографический. @ **non-deterministic Turing machine** недетерминированная машина Тьюринга. @ **non-deterministic** недетерминированный. @ **non-disclosure** неразглашение (секретной информации); невозможность вскрытия (шифра). @ **means for data transmission** средства передачи данных, исключаящие их перехват. @ **non-error expanding cipher** шифр без размножения ошибок. @ **non-expanding** не расширяющий. @ **non-expanding encipherer** не расширяющий шифратор (не увеличивает объем текста при шифровании). @ **non-interceptible** исключаящий перехват; неподдающийся перехвату. @ **non-iterative zero-knowledge proof (NIZK)** неитеративное доказательство с нулевым разглашением (конфиденциальной информации). @ **non-iterative** неитеративный. @ **non-linear algorithm** нелинейный алгоритм. @ **non-linear feedback shift register (NLFSR)** регистр сдвига с нелинейной обратной связью. @ **non-linear feedback** нелинейная обратная связь. @ **non-linear mapping** нелинейное отображение. @ **non-linear order of a function** степень нелинейности функции. @ **non-linear** нелинейный. @ **non-linearity criteria for cryptographic functions** критерий нелинейности криптографических функций. @ **non-linearity** *n.* нелинейность. @ **non-prime number** непростое число. @ **non-prime** непростой. @ **non-recallable key** неизвлекаемый (из криптографического устройства) ключ. @ **non-recallable** неизвлекаемый (из криптографического устройства). @ **non-redundant source of messages** безызбыточный источник сообщений. @ **non-redundant** безызбыточный. @ **non-repetitive cipher** неповторяющийся шифр. @ **non-repetitive key** неповторяющийся ключ. @ **non-repetitive pseudo-random number (PRN) generator** генератор неповторяющихся псевдослучайных чисел. @ **non-repetitive** неповторяющийся. @ **non-**

truncated congruential generator неусеченный конгруэнтный генератор.@ **non-truncated** неусеченный.@ **non-uniform diplomatic communications (NDC)** неамериканские дипломатические каналы связи.@ **non-uniform distribution** неравномерное распределение.@ **non-uniform** неравномерный.@ **non-US** неамериканский.@ **non-verbal traffic** неречевой трафик.@ **non-verbal** неречевой.@ **non-volatile key** ключ, хранимый в энергонезависимой памяти.@ **non-volatile** хранимый в энергонезависимой памяти.

non von Neumann architecture ['nɒn vɒn nemɪən 'a:kitektʃə] не-фоннеймановская архитектура.@ Любой способ организации ЭВМ, принципиально отличающийся от классической фон-неймановской архитектуры. Предлагаемые варианты не-фон-неймановской архитектуры включают: организацию ЭВМ либо без счетчика команд и с непосредственным выполнением команд, либо без памяти с многократной записью.

non-cooperative remote rekeying = automatic remote rekeying

non-error propagating cipher *n.* = **non-error expanding cipher**

non-invertible *adj.* = **one-way**

non-repeating *adj.* = **non-repetitive**

non-secret encryption = **public-key encryption**

none [nʌn] *pron.* никто, ничто; ни один; *adj.* никакой; *adv.* нисколько, совсем не.# **none but** никто кроме.# **none the less** тем не менее.

notarization *n.* нотаризация (заверение открытых ключей пользователя цифровой подписью администратора безопасности).

notarized *adj.* заверенный.@ **notarized key** заверенный ключ.

note [nəʊt] *v.* 1. делать заметки; записывать; 2. отмечать; упоминать.# **of note** выдающийся, известный.# **it will be noted** следует отметить.# **worthy of note** заслуживающий внимания.# **to be noted for** быть известным чем-л..# **to take note of** обращать внимание на что-л.

nothing ['nʌθɪŋ] *pron.* ничто, ничего.# **nothing but** только лишь.# **nothing else than** не что иное как.# **to have nothing to do with** не иметь ничего общего с.

notice ['nəʊtɪs] *v.* замечать; отмечать; обращать внимание; *n.* извещение, уведомление; объявление; предупреждение.# **on a short notice** сразу, без предупреждения.# **to bring to one's notice** доводить до сведения.# **to take notice of** обращать внимание на что-л.

now [naʊ] *adv.* 1. теперь, сейчас; 2. и так; *conj.* когда, раз.# **now and again** иногда, время от времени.# **now and then** иногда, время от времени.# **now that** теперь, когда.# **by now** в дальнейшем.# **just now** только что.# **up to now** до сих пор.# **up till now** до сих пор.

null [nʌl] *adj.* 1. пустой, фиктивный; 2. пустой указатель.@ В языке Си – зарезервированное значение ссылочного типа, обозначающее, что указатель не ссылается ни на какой объект.@ **null (empty) list** пустой список.@ **null attribute** неопределенный атрибут.@ **null character** символ пробела.@ **null cipher** пустышечный шифр.@ **null circuit** нулевая схема.@ **null hypothesis** "нулевая" (основная) гипотеза.@ **null information** отсутствие информации.@ **null in-**

struction нулевая (фиктивная) команда.@ **null link** фиктивная связь, нулевая связь.@ **null representation** машинное представление нуля.@ **null sequence** нулевая последовательное п., (двоичная последовательность из нулей) .@ **null statement** пустой оператор.

null (zero) matrix [nʌl ('ziərou) 'meɪtrɪks] нулевая матрица.@ Квадратная матрица, все элементы которой равны нулю.

null string [nʌl strɪŋ] пустая строка.@ Строка нулевой длины.

number ['nʌmbə] *n.* 1. число, количество; 2. номер; *v.* нумеровать.# **a number of** ряд (некоторое количество); целый ряд.@ **number address code** код адреса числа.@ **number code** код числа.@ **number converter** преобразователь чисел из одной системы счисления в другую.@ **number cruncher** сверхбыстродействующая ЭВМ, супер-ЭВМ.@ **number generator** генератор чисел.@ **number language** числовой язык программирования с нумерованными строками.@ **number normalization** нормализация числа.@ **number of possible keys** количество возможных ключей.@ **number range** диапазон чисел.@ **number register** регистр числа.@ **number representation** система счисления, система представление чисел.@ **number sequence** числовая последовательность.@ **number system base** основание системы счисления.@ **number theory** теория чисел.@ **number to frequency converter** преобразователь кода в частоту.@ **number to position converter** преобразователь кода в положение.@ **number-theoretic cryptalgorithm** криптоалгоритм на основе теории чисел.# **the number of** число, количество.# **quite a number** значительное количество.

number designation ['nʌmbə də'zɪɡ'neɪʃən] запись числа.@ Буквальная числовая константа, записываемая в виде последовательности цифр; одно и то же число может быть записано в программе различными способами.

number system ['nʌmbə 'sɪstɪm] система счисления.@ Способ записи чисел в виде последовательности цифр.

numeric adj. = **numerical**

numeric character [nju:'mɛrɪk 'kærɪktə] цифра.@ **numeric concept** 1. выражаемое числителем; 2. числовое понятие.@ **numeric field** числовое поле.@ **numeric word** 1. машинное слово, представляющее число; 2. цифровое слово.

numeric keypad [nju:'mɛrɪk 'ki:pæd] числовая клавиатура, цифровая клавиатура.@ Небольшая клавиатура или специальная часть клавиатуры для ввода цифр.

numeral ['nju:mɜəl] *n.* 1. запись числа; 2. (десятичная) цифра; *adj.* числовой; цифровой.

numerical [nju:'mɛrɪkəl] *adj.* численный.@ О методе решения математической задачи, как правило, приближенных вычислений.@ **numerical aperture (NA)** числовая апертура.@ **numerical computation** вычисление численными методами.@ **numerical constant** числовая постоянная.@ **numerical control (NC)** числовое программное управление.@ **numerical data** числовые данные.@ **numerical differentiation** численное дифференцирование.@ **numerical information** цифровая числовая информация.@ **numerical integration** численное интегрирование.@ **numerical key** цифровой ключ.@ **numerical linear algebra**

численные методы линейной алгебры. @ **numerical message** цифровое сообщение. @ **numerical method** численный метод. @ **numerical position** позиция числа. @ **numerical representation** представление в числовой форме.

numerical stability устойчивость численного решения. @ **numerical system** цифровая система (напр. арабская). @ **numerical value** численное значение.

numerical code [nju:'mærikəl koud] числовой код. @ Код, алфавит которого содержит только цифры или наборы цифр.

numeral analysis ['nju:məɹəl ə'næəsɪz] численный анализ. @ Область математики, относящаяся к численным методам задач, поставленных и изучаемых другими областями.

numerical analysis [nju:'mærikəl ə'næləsɪz] численный анализ. @ Область математики, относящаяся к численным методам решения задач, поставленных и изучаемых другими областями математики. В практическом плане численный анализ предполагает создание эффективных и надежных стандартных программ для решения широкого круга задач.

numerically [nju:'mærikəli] *adv.* в цифровом выражении.

numeration [nju:mə'reɪʃən] *n.* 1. исчисление; 2. нумерация. @ **numeration system** система счисления.

numerator register ['nju:məreɪtə 'redʒɪstə] регистр делимого.

numerous ['nju:mərəs] *adj.* многочисленный.

nut [nʌt] *n.* помешанный. @ **"nut file"** "файл для помешанных" (жаргонное название специального файла NSA USA, в котором хранятся сведения о шифр-системах представленных их авторами на рассмотрение американского правительства).

O*

object ['ɒbdʒɪkt] *n.* 1. объект. 2. объектный, целевой. 3. объектный, выходной. 4. предмет; 5. цель. # **the object in view** поставленная цель; *v.* возражать.

objection [əb'dʒækʃən] *n.* возражение. # **open to objection** сомнительный; уязвимый.

observation [ˌɒbzə:'veɪʃən] *n.* 1. наблюдение; 2. наблюдательность; 3. замечание, высказывание.

observe [əb'zə:v] *v.* 1. наблюдать, замечать; 2. отмечать; 3. соблюдать (законы и т. п.).

observer [əb'zə:və] *v.* наблюдатель.

observation Service = B-Dienst

occurrence [ə'kʌrəns] *n.* 1. вхождение; экземпляр; 2. случай; 3. событие; 4. наличие; 5. местонахождение; распространение; 6. проявление; 7. встречаемость. @ **occurrence of bigrams in English** встречаемость биграмм в английском языке.

octal (oct) ['ɒktəl] *adj.* 1. восьмеричный; 2. восьмиугольный. @ **octal multiplication** умножение в восьмеричной системе счисления (восьмеричное умножение). @ **octal representation** восьмиричное представление.

octal notation ['ɒktəl nou'teɪʃən] восьмеричная запись. @ Запись числа в восьмеричной системе счисления.

octet *n.* = byte

odd [ɒd] *adj.* 1. нечетный; 2. странный; 3. лишний, сверх нормы; 4. неспаренный; 5. случайный. # **od-dly to say** как ни странно. # **twenty odd** двадцать с лишним.

off [ɒf, ɔ:f] *adv.* указывает на удаление, отделение, отклонение от нормы, расстояние, прекращение действия и т. п., например: **some distance off** на некотором расстоянии. @ **off-line** автономный; предварительный. @ **off-line crypt-analysis** автономный криптоанализ (не в реальном масштабе времени). @ **off-line cryptosystem** автономная криптосистема (шифрование и расшифрование сообщений производится независимо от их передачи по каналам связи). @ **off-line encryption device** прибор предварительного (автономного) шифрования. @ **off-line mode** автономный режим работы. # **off and on** время от времени, нерегулярно. # **off hand** без подготовки, сразу. # **off the point** не по существу. # **far off** отдаленный. # **to give off** выделять. # **to put off** откладывать. # **to read off** отсчитывать. # **to take off** снимать. # **to turn (switch) off** выключать.

off-line cipher device = **off-line encryption device**

off-network *adj.* = **off-line**

once [wʌns] *cj.* раз, раз уж, если; как только; если только; *adv.* 1. (один) раз; 2. некогда, когда-то; однажды. # **once again** еще раз, снова. # **once and again** несколько раз, неоднократно; иногда. # **once (and) for all** раз (и) навсегда. # **once in a while (way)** редко, изредка. # **once more** еще раз. # **all at once** неожиданно. # **at once** сразу, немедленно. # **for once** на этот раз. # **more than once** не раз, неоднократно.

one [wʌn] *num.* один; *pron.* употребляется в неопределенно-личный предложениях. Например: **One must observe rules.** Следует соблюдать правила; *n.* заменяет ранее упомянутое существительное. # **one another** друг друга. # **one of** один из. # **for one** например. # **for one thing** во-первых, прежде всего. # **to be at one** быть заодно, действовать единодушно.

one- [wʌn] в сложных и сложносоставных словах имеет значение одно-. @ **one-part** состоящий из одной части, одночастевой. @ **one-part cipher** одноразовый шифр. @ **one-part code** одночастевой код (код, в котором элементы открытого текста и соответствующие им кодовые группы упорядочены по алфавиту или каким-либо другим образом, чтобы их перечисление могло служить одновременно и для кодирования, и для декодирования). @ **one-part cryptosystem** одноразовая криптосистема. @ **one-part encryption** одноразовое шифрование. @ **one-part key encryption** шифрование на ключе одноразового использования. @ **one-part key** одноразовый ключ. @ **one-part pad** одноразовый шифровальный блокнот. @ **one-part signature scheme** схема одноразовой цифровой подписи. @ **one-part tape** одноразовая перфоленга (перфорированная бумаж-

ная лента, используемая в качестве носителя ключевой информации и предназначенная для однократного применения).@ **one-time** одноразовый.@ **one-to-many** неоднозначный, многозначный.@ **one-to-many mapping** неоднозначное (многозначное) отображение.@ **one-to-one** взаимно однозначный.@ **one-to-one mapping** взаимно однозначное отображение.@ **one-to-one substitution cipher** шифр простой замены.@ **one-way** односторонний.@ **one-way cipher** односторонний шифр (шифр на основе односторонней функции).@ **one-way function (OWF)** односторонняя функция.@ **one-way hash function (OWHF)** односторонняя хэш-функция (функция хеширования) (вычислительно невозможно найти два разных аргумента, для которых ее значения совпадают).@ **one-way key** ключ только для зашифрования или расшифрования.@ **one-word** состоящий из одного слова.@ **one-word key encryption** шифрование на ключе из одного слова.@ **one-word key** ключ из одного слова (ключ-слово).@ **on-line** (работающий) в реальном масштабе времени |в темпе поступления информации); оперативный; линейный.@ **on-line certificate status protocol (OCSP)** линейный протокол статуса сертификата.@ **on-line cryptanalysis** криптоанализ в реальном масштабе времени.@ **on-line cryptography configuration** конфигурация, предусматривающая одновременное включение криптографического оборудования на обоих концах канала связи.@ **on-line cryptosystem** линейная криптосистема (шифрование и расшифрование сообщений производится согласованно с их передачей по каналам связи).@ **on-line encryption device** устройство линейного (оперативного) шифрования.@ **on-line key management** управление ключами в реальном масштабе времени.

one-key *adj.* = **single-key**

on-line cipher device = **on-line encryption device**

one-part hash = **message digest (MD)**

only ['ounli] *adj.* единственный; *adv.* только, исключительно; *conj.* но.# **only that** если бы не то, что.# **if only** хотя бы.

on-the-air [ɒn'ði:'eə] по радио.@ **on-the-air key load** загрузка (ввод) ключей по радио.

on-the-fly [ɒn'ði:'flaɪ] немедленный, непрерывный.@ О действиях, выполняемых без видимого прерывания основной работы.@ **on-the-fly encryption** оперативное (линейное) шифрование.@ **on-the-fly error recovery** оперативное устранение ошибок.@ **on-the-fly garbage collection** параллельная очистка памяти, параллельная сборка мусора.

open ['oʊpən] *v.* 1. открывать (файл); 2. открывать(ся); *adj.* расширяемый, открытый. *n.* разрыв.@ **open circuit (OC)** разомкнутый контур; разомкнутая цепь.@ **open loop control** управление (регулирование) по разомкнутому циклу.@ **open loop transfer function (OLTF)** передаточная функция разомкнутой системы.@ **open shop** вычислительный центр с доступом пользователей к ЭВМ.@ **open subroutine** открытая подпрограмма, подставляемая подпрограмма.@ **open system** открытая система; расширяемая система.@ **open systems architecture (OSA)** архитектура открытых систем.# **to be open to criticism (question, speculation)** вызывать сомнения; быть спорным, быть сомнительным.

open a file ['oʊpən ə faɪl] открывать файл.@ Операция, связывающая переменную типа файл или номер логического канала с конкретным файлом файловой системы. Файл должен быть открыт, прежде чем к нему можно обращаться операциям записи и чтения.

open function ['oʊpən 'fʌŋkʃən] «открытая» функция.@ Функция, вычисляемая по открытой подпрограмме.

open loop (OL) ['oʊpən lu:p] 1. разомкнутый цикл.@ Организация обработки данных, при которой обратная связь идет через оператора или пользователя. 2. разомкнутая петля; разомкнутый контур; 3. разомкнутая система.

open systems interconnection (OSI) ['oʊpən 'sɪstɪms ɪntə'kənekʃən] взаимодействие открытых систем.@ Предложенный ISO проект стандарта сетевого и межсетевого взаимодействия, определяющий семь уровней взаимодействия компонентов сети: физический, канальный, сетевой, транспортный, сеансовый, уровень представления данных и прикладной. Для каждого уровня разрабатывается один или несколько протоколов, которые обеспечат сетевое взаимодействие широкого класса устройств.

open-ended ['oʊpən'endɪd] открытый, расширяемый.@ О системе, для которой определены и описаны используемые форматы данных и процедурный интерфейс, что позволяет подключать к ней независимо разработанные компоненты.

operation [ˌɒpə'reɪʃən] *n.* 1. операция (вычислительной системы), команда.@ Действия, в совокупности составляющие выполнение команды процессора. 2. операция; 3. действие; функционирование; режим работы.@ **operation and maintenance phase** промышленная эксплуатация.@ **operation declaration** описание операции.@ **operation decoder** дешифратор команд.@ **operation field** поле команды, поле кода команды.@ **operation of decryption** операция расшифрования.@ **operation of encryption** операция зашифрования.@ **operation per minute (OPM)** число операций в минуту.@ **operation register** 1. регистр операции; 2. регистр команд.@ **operation testing** испытания в реальных условиях; опытная эксплуатация.@ **operation time** время выключения операции.

operation code (Op Cd) [ˌɒpə'reɪʃən kɒd] код операции; код команды, состав команды.@ 1. Часть командного слова, определяющая какая операция должна быть выполнена по данной команде. 2. Набор частей командных слов конкретной ЭВМ и определяющий множество операций, которые способна выполнять эта ЭВМ.

operation on sets [ˌɒpə'reɪʃən ɒn sɛts] операции на множествах.@ Простейшие операции, которые могут быть выполнены на множествах: объединение, пересечение, образование дополнения, разность множеств.

operational [ˌɒpə'reɪʃənəl] *adj.* 1. работающий; сданный в эксплуатацию; 2. операционный; 3. рабочий; 4. практический.@ **operational attack** практическая атака (криптоаналитическая атака, которая может быть успешно осуществлена на практике).@ **operational calculus** операционное исчисление.@ **operational characteristic** рабочие параметры.@ **operational cipher** действующий шифр.@

operational cryptanalyst криптоаналитик-практик. @ **operational decoder** дешифратор операции. @ **operational factor** эксплуатационные (рабочие) параметры (характеристики), действующие параметры. @ **operational failure** эксплуатационный отказ. @ **operational grammar** операционная грамматика. @ **operational key** рабочий ключ (используется для шифрования служебной информации передаваемой по каналам связи). @ **operational label** маркировочная метка, маркировочный знак для идентификации файла на магнитной ленте. @ **operational method** операторный метод. @ **operational order** операционная команда. @ **operational readiness and reliability test (ORRT)** проверка эксплуатационной готовности и надежности. @ **operational research** исследование операций. @ **operational symbol** операционный символ. @ **operational system (OS)** операционная система.

operational semantics [ˌɒpə'reɪʃənəl si'mæntiks] операционная семантика. @ Способ задания семантики языка с помощью описания абстрактной машины, интерпретирующий его.

operator (op) ['ɒpəreɪtə] *n.* 1. знак операции; операция. @ Подразумевает не столько действия для выполнения операции, сколько обозначение операции в тексте. 2. оператор. @ Человек, обслуживающий или использующий ЭВМ. 3. оператор. @ **operator error** ошибка оператора. @ **operator routine** служебная программа, выполняемая оператором. @ **operator variable** операторная переменная. @ **operator-oriented language** язык, ориентированный на оператора.

operator command ['ɒpəreɪtə kə'ma:nd] команда оператора. @ Команда операционной системе, введенная с операторского терминала.

opponent cryptanalyst = enemy cryptanalyst

opponent [ə'pounənt] *n.* противник; оппонент.

opportunity ['ɒpə'tjuniti] *n.* возможность; удобный случай. # **to take the opportunity** воспользоваться случаем.

oppose [ə'prouz] *v.* 1. противопоставлять (**with, against**); 2. возражать; 3. оказывать сопротивление, сопротивляться, противиться; 4. мешать, препятствовать. # **as opposed to** в противоположность.

opposed [ə'prouzd] *adj.* 1. противоположный, противный; 2. встречающий сопротивление.

optimal ['ɒptɪməl] *adj.* оптимальный. @ Наилучший в заданных условиях. Качество оценивается с помощью критерия оптимальности, а условия задаются в виде ограничения на дополнительные критерии. Оптимизация – центральная идея кибернетики.

optimal binary search tree ['ɒptɪməl 'baɪnəri sə:tʃ tri:] оптимальное двоичное дерево поиска. @ Двоичное дерево поиска, построенное в расчете на обеспечение максимальной производительности при заданном распределении вероятностей местоположения требуемых данных.

optimization ['ɒptɪmaɪzɪʃən] *n.* оптимизация. @ 1. Преобразование программы, сохраняющее ее семантику, но уменьшающее ее размер или время

выполнения. **2.** Поиск значения параметров, оптимизирующих значение заданного функционала. @ **optimized code** оптимизированная программа.

optimizer ['ɒptɪmɪzə] *n.* 1. оптимизатор. @ Оптимизирующий транслятор 2. оптимизатор, блок оптимизации. @ Компонент транслятора, выполняющий оптимизацию.

optimizing computer ['ɒptɪmɪzɪŋ kəm'pjʊ:tə] оптимизирующий транслятор. @ Транслятор, выполняющий эквивалентные преобразования программы, приводящие к получению более быстрой или более компактной программы. Оптимизация включает однократное вычисление общих подвыражений, вынос из цикла не зависящих от повторения операций, уничтожение лишних присваиваний или проверок и другие преобразования.

optimum (opt) ['ɒptɪmə] *n.* наиболее благоприятные условия; *adj.* оптимальный. @ **optimum allocation** оптимальное распределение объектов в выборке. @ **optimum programming** оптимальное программирование. @ **optimum scale integration** 1. интеграция оптимального уровня; 2. с оптимальным уровнем интеграции.

option ['ɒpʃən] *n.* 1. необязательный параметр; 2. вариант; 3. дополнительное средство; 4. право выбора (замены). @ **option list** список дополнений.

optional ['ɒpʃənl] *adj.* необязательный; произвольный; дополнительный. @ **optional information** факультативная (необязательная) информация. @ **optional interrupt** необязательное прерывание. @ **optional label** необязательная метка. @ **optional modification** дополнительная модификация (одобренная NSA USA модификация криптографического оборудования, которая может производиться по требованию пользователей этого оборудования). @ **optional parameter** необязательный параметр. @ **optional product** факультативное произведение. @ **optional retention** необязательное членство. @ **optional word** необязательное ключевое слово.

or [ɔ:] *conj.* или; в противном случае, иначе; и (*после отрицания*); то есть (*после запятой*). # **or else** или же. # **or so** около того. # **and/or** по отдельности или оба вместе.

orange ['ɒrɪndʒ] *adj.* оранжевый. @ **"orange Book" (O-book)** "Оранжевая книга" (сокращенное название американского стандарта DoD 520028-STD). @ **orange machine** "оранжевая" машина (условное наименование, данное американскими криптоаналитиками японской шифровальной машине).

order [ɔ:'dɜ] *n.* 1. порядок, упорядоченность; способ упорядочения; 2. порядок, степень; 3. разряд; 4. порядок чисел; 5. порядок действий; 6. машинная команда; 7. команда; 8. кратность; 9. степень; 11. директива; заказ; 12. инструкция; 13. ордер; 14. очередность; 15. последовательность; 16. расстановка; 17. регламент; 18. упорядоченность; *v.* 1. командовать; 2. предписывать; 3. распоряжаться; 4. упорядочивать. @ Расставлять в соответствии с заданным отношением порядка. @ **mth order correlation immunity** корреляционная стойкость порядка **m** (отсутствие статистической зависимости между выходной последовательностью и любыми **t** элементами входной последовательности); **kth order product** произведение порядка **k** (произведение **k** сомножителей).

лей).# **in order** для того, чтобы.# **in order that** для того, чтобы.# **in order to** для того, чтобы.# **to be in order** быть в порядке; быть уместным.

ordering [ɔ:'dɔ:rn] *n.* определение порядка следования, упорядочение, упорядочивание, упорядоченное расположение, порядок, расстановка.@ **ordering register (OR)** регистр команд.

ordering relation [ɔ:'dɔ:rn rɪ'leɪʃən] способ упорядочения; отношение порядка.@ Отношение, обладающее свойствами рефлексности, антисимметричности и транзитивности.

ordinal ['ɔ:dɪnl] *adj.* исходный, первоначальный; порядковый; *n.* порядковое или трансфинитное число.@ **ordinal relation** прямая зависимость.@ **ordinal type** перечисленный тип.@ **original key** исходный (первоначальный) ключ.@ **original plaintext** исходный открытый текст.

ordinary ['ɔ:dnri] *adj.* обычный, заурядный.@ **ordinary differential equation** обыкновенное дифференциальное уравнение.

originate [ə'rɪdʒineɪt] *v.* отправлять (сообщение).

originator [ə'rɪdʒineɪtə] *n.* отправитель (сообщения).@ **originator's key** ключ отправителя (сообщения).

other ['ʌðə] *adj.* другой, иной; *pron.* другой; *adv.* иначе.# **other than** помимо, кроме; а не; любой кроме; кроме как.# **other things (conditions) being equal** при прочих равных условиях.# **the other way (round)** и наоборот.# **each other** друг друга.# **on the other hand** с другой стороны.# **somehow or other** так или иначе.# **some time or other** когда-нибудь, рано или поздно.

otherwise ['ʌðəwaɪz] *adv.* 1. иначе, иначе говоря; 2. или же, в противном случае; 3. в остальном, в других отношениях, в других случаях; 4. *переводится значением, противоположным только что высказанному, например: the presence or otherwise of* присутствие или отсутствие.# **except when otherwise stated (specified, indicated etc.)** за исключением тех случаев, когда это оговорено особо.# **unless (if) otherwise stated (indicated, mentioned, noted, specified)** если не указано (оговорено) особо.# **under otherwise equal (identical) conditions** при прочих равных условиях.

outline ['aʊtlaɪn] *n.* 1. схема текста, план.@ Иерархическая структура текста (членение на части, главы, параграфы) и перекрестные ссылки между его отдельными частями. 2. очертание, контур (*часто pl.*); *v.* описывать (в общих чертах).# **in outline** в общих чертах.

out-of-date ['aʊt'ɔv'det] *adj.* устаревший, недействительный.@ **out-of-date key** устаревший (недействительный) ключ (с истекшим сроком годности).

out-of-phase ['aʊt'ɔv' feɪz] *adj.* несовпадающий по фазе.@ **out-of-phase autocorrelation** несовпадающая по фазе автокорреляция.

output ['aʊtpʊt] *adj.* выходной; *n.* 1. вывод данных; 2. выходные данные, результаты; 3. выводное устройство, устройство вывода; 4. выходной сигнал; 5. выводить данные.@ Отображать данные на экране дисплея или бумаге, записывать их в файл или передавать по линии связи.@ **output alphabet** выходной алфавит.@ **output area** буфер вывода.@ **output assertion** выходное утвер-

ждение. @ **output block feedback (OBFB)** обратная связь по выходному блоку (один из режимов использования DES-алгоритма). @ **output block** выходное устройство. @ **output buffer (OB)** буфер вывода. @ **output buffer register** регистр выходного буфера, выходной буферный регистр. @ **output data** выходные данные, результаты. @ **output feedback (OFB)** обратная связь по выходу (один из режимов использования DES-алгоритма). @ **output file** выходной файл, файл результата. @ **output generator (OG)** выходной генератор. @ **output highway (OHW)** выходной тракт дискретной информации. @ **output information** выходная информация, выходные данные. @ **output listing** распечатка, контрольная печать программы. @ **output medium** 1. среда для записи выходных данных; 2. способ вывода данных. @ **output order** выходная команда. @ **output parameter** выходной параметр, параметр-результат. @ **output primitive** графический примитив, элемент отображения, выходной примитив. @ **output program** программа вывода. @ **output register** выходной регистр. @ **output routine** программа вывода. @ **output section** выходная область памяти. @ **output sequence** выходная последовательность. @ **output transformation** выходное преобразование. @ **output unit** выводное устройство, устройство вывода. @ **output variable** выходная переменная. @ **output-bound task** задача, скорость выполнения которой ограничена скоростью вывода данных.

output format ['aʊtput 'fɔrmæt] выходной формат. @ Формат результата работы программы.

output queue ['aʊtput kju:] очередь вывода. @ Список выходных файлов, подлежащих печати.

output stream ['aʊtput stri:m] выходной поток. @ Файл или устройство, куда направляются выходные данные заданий пакета.

output subroutine ['aʊtput səb.ru:'tɪn] подпрограмма вывода. @ Подпрограмма подготовки выходных данных.

output-limited process ['aʊtput'limitɪd 'prəʊses] ограниченный по выводу процесс. @ Процесс, скорость выполнения которого лимитируется скоростью вывода данных.

outset ['aʊtset] *n.* начало. # **at the outset** в начале. # **from the outset** с самого начала.

outside ['aʊtsaɪd] *adj.* наружный, внешний; *adv.* 1. снаружи, вне; 2. помимо.

outsider ['aʊtsaɪdə] *n.* посторонний, чужой (человек).

over ['oʊvə] *pref.* передается приставками *сверх-, над-, пере-; prep.* 1. над, через; по; 2. свыше; 3. в пределах; в течение; 4. по сравнению; *adv.* 1. через; 2. повсюду, кругом; 3. слишком; 4. снова. # **over and above** сверх, в добавлении; к тому же. # **over much of** на протяжении большей части чего-л. # **over and over again** много раз, повторно, неоднократно. # **over (within) the range** в пределах, в диапазоне. # **well over** значительно выше (больше). # **to be over** заканчивается.

overall ['oʊvəɹɔ:l] *adj.* полный. @ **overall diffusion** полная диффузия (любой бит блока на выходе блочного шифра является функцией каждого бита со-

ответствующего входного блока, при этом изменение одного бита на входе приводит к изменению всех выходных бит с вероятностью 05).

override ['ouvəraɪd] *v.* (**overrode**, **overridden**) 1. отменять; замещать. @ Задавать значения параметров, отличные от принимаемых по умолчанию. 2. преобладать; подавлять; 3. отвергать, не принимать во внимание. # **to be overridden with difficulties** представлять большие трудности.

override ['ouvəraɪd] *n.* отмена.

over-the-air ['ouvə'di:'eə] *adj.* эфирный. @ **over-the-air key distribution (OTAD)** эфирное распределение ключей (ключ, посылаемый по каналу связи, шифруется с помощью того же самого ключа, который используется для шифрования сообщений, передаваемых по этому каналу). @ **over-the-air key transfer (OTK)** эфирная передача ключей. @ **over-the-air rekeying (OTAR)** эфирный ввод ключа (процедура, применяемая для смены ключа в расположенном на удалении криптографическом оборудовании, при этом новый ключ пересылается по тому же самому каналу связи, что и сообщения, которые предполагается шифровать при помощи этого ключа).

own [oun] *adj.* собственный; *v.* владеть, обладать. # **in one's own (right)** в своем праве; по праву. # **on one's own (account)** самостоятельно; сам по себе. # **it stands on its own** это говорит само за себя. # **to come into one's (right)** вступить в права.

owner ['ounə] *n.* 1. владелец. @ При защите данных и контроле доступа - пользователь, имеющий неограниченные права по отношению к файлу или другой информации. 2. владелец набора. @ **owner key** ключ владельца (криптографического устройства).

owner type ['ounə taɪp] тип владельца. @ В сетевых базах данных – часть описания набора, задающая тип владельца набора.

P*

package ['pækɪdʒ] *n.* 1. пакет (программ). @ Совокупность программ, объединенных общим приложением. 2. корпус; 3. блок; 4. модуль. @ **packet encryption** пакетное шифрование, шифрование пакетов (текста).

package body ['pækɪdʒ 'bɒdɪ] тело пакета. @ Описание реализации пакета.

package generator ['pækɪdʒ 'dʒenəreɪtə] генератор пакетов прикладных программ. @ Программа, настраивающая пакет прикладных программ на конкретный класс задач.

package specification ['pækɪdʒ ,spesɪfɪ'keɪʃən] описание пакета, спецификация пакета. @ Описание интерфейса пакета.

packed ['pækt] *adj.* упакованный. @ О типе данных, для переменных которого транслятор выполняет оптимизацию по памяти.

packed decimal ['pækt 'desiməl] упакованное десятичное (число).@ О представлении чисел в двоично-десятичной системе, при котором в каждом байте хранится две десятичные цифры.

packet ['pækit] *n.* 1. пакет.@ Блок данных в сети передачи данных, имеющий строго определенную структуру, включающую заголовок и поле данных. Сообщение может быть разбито на несколько пакетов. Размер пакета составляет 100 – 500 байтов. 2. пучок; 3. микросгусток.@ **packet assembler/dis-assembler** устройство сборки – разборки пакетов.@ **packet assembly and disassembly (PAD)** формирование и разборка пакетов.@ **packet assembly** формирование пакета.@ **packet disassembly** разборка пакета.@ **packet of encrypted data** пакет с шифрованными данными.@ **packet switched data service** служба коммутации пакетов данных.

packet interleaving ['pækit ,intə'li:vɪŋ] чередование пакетов.@ Способ передачи данных, при котором по одному физическому каналу последовательно передаются пакеты разных сообщений.

packet switching ['pækit 'swɪtʃɪŋ] коммутация пакетов.@ Метод динамического распределения коммутационных ресурсов между многочисленными взаимодействующими объектами.

packet switching network (PSN) ['pækit 'swɪtʃɪŋ 'netwɜ:k] сеть коммутации пакетов.@ Сеть передачи данных, в которой передаваемое сообщение разбивается на несколько специально оформленных порций – пакетов, каждый из которых передается независимо.

packet-mode terminal ['pækit'moud 'tə:mɪnl] пакетный терминал. @ Терминал, взаимодействующий с ЭВМ через сеть коммутации пакетов.

packing density ['pækiŋ 'densɪti] 1. плотность компонентов.@ Количество электронных устройств на единицу площади интегральной схемы. 2. плотность размещения.@ Количество информации на единицу емкости запоминающей среды.@ **packing factor** плотность упаковки информации.

pad [pæd] *n.* 1. вспомогательная клавиатура; 2. (графический) планшет; шифровальный блокнот; *v.* дополнять, дополнять холостым заполнением.@ Заполнять поля записи, не содержащие полезной информации, пустыми кодами (например, пробелами).

pad character [pæd 'kærɪktə] символ-заполнитель.@ Символ, дополняющий поле записи или управляющую последовательность до требуемого формата.

padded [pædɪd] *adj.* дополненный холостым заполнением.@ **padded message** сообщение, дополненное холостым заполнением (ничего не значащей или фальшивой информацией).

padding [pædɪŋ] *n.* холостое заполнение (ничего не значащая или фальшивая информация, добавляемая в передаваемое сообщение).@ **padding character** знак (символ)-заполнитель.

page [peɪdʒ] *n.* 1. страница памяти, лист памяти.@ Совокупность ячеек памяти с одинаковыми старшими разрядами адреса, являющейся единицей, с ко-

торой работает система управления памятью. 2. страница. @ Лист бумаги или элемент описания формата документа. @ **page address** адрес страницы. @ **page fault** отсутствие страницы, обращение к отсутствующей странице. @ **page heading** заголовок страницы. @ **page pool** множество свободных страниц. @ **page printer** постранично печатающее устройство с печатью одновременно целой страницы. @ **page sorter view** раскладка страниц. @ **page system** страничная система, система со страничной организацией (виртуальной) памяти. v. нумеровать страницу.

page fault interrupt [peɪdʒ fɔ:lt ,ɪntə'rɒpt] прерывание по отсутствию страницы. @ В системах с виртуальной памятью – аппаратное прерывание, вызванное обращением к ячейке виртуальной памяти, расположенной на странице, отсутствующей в данный момент в физической оперативной памяти.

page footer [peɪdʒ 'fʊtə] нижний колонтитул. @ Текст, повторяющийся в нижней части каждой страницы текста.

page frame [peɪdʒ freɪm] страничный блок, страница. @ Страница памяти с точки зрения системы управления виртуальной памятью. «Страничный блок» означает либо сегмент физической оперативной памяти, в котором может быть размещена страница виртуальной памяти, либо копию содержимого страницы виртуальной памяти на внешнем запоминающем устройстве.

page header [peɪdʒ 'hedə] колонтитул, шапка (*страницы*). @ Текст, повторяющийся в верхней части каждой страницы текста.

page locking [peɪdʒ 'lɒkɪŋ] фиксация страницы. @ Запрещение откачки страницы виртуальной памяти.

page table [peɪdʒ 'teɪbl] таблица страниц. @ Структура данных операционной системы, связывающая виртуальные адреса с номерами страниц и указывающая, какие страницы виртуальной памяти находятся в оперативной памяти.

pager [peɪdʒə] n. пейджер. @ **pager Identification and Message Extraction System** Система перехвата пейджинговых сообщений.

paging ['peɪdʒɪŋ] n. замещение страниц, подкачка. @ Перемещение активных страниц виртуальной памяти и с диска в оперативную память и пассивных – из оперативной памяти на диск. *adj.* пейджинговый. @ **paging signals** пейджинговые сигналы.

paging policy ['peɪdʒɪŋ 'pɒləsɪ] алгоритм замещения страниц, алгоритм подкачки. @ Алгоритм системы управления виртуальной памятью, определяющий, какие страницы оперативной памяти следует освободить и какие страницы виртуальной памяти следует загрузить.

painstaking ['peɪnz'steɪkɪŋ] *adj.* старательный, усердный; 2. тщательный, кропотливый. @ **painstaking encryption** кропотливое шифрование.

pair [pɛə] n. пара; *adj.* парный. # **pairwise** 1. попарно; 2. парный. @ **pairwise key** 1. парный ключ (в криптосистеме с открытым ключом); 2. ключ, назначенный двум пользователям (недоступный для других пользователей). @ **pairwise traffic encryption keys** парный трафик ключей шифрования.

paper ['peɪpə] *adj.* бумажный; *n.* 1. статья; 2. работа; научный доклад; 3. бумага. @ **paper-tape key** ключ, записанный на бумажной перфоленте.

par [pɑ:] *n.* равенство. # **at par** по номинальной стоимости. # **on a par with** наравне, на равных началах. # **par example** например. # **par excellence** по преимуществу, преимущественно.

parameter [pə'reɪmɪtə] *n.* 1. параметр. @ Объект, над которым выполняется процедура или от которого зависит ее выполнение. 2. параметр, характеристика. @ **parameter qualifier** ключ параметра.

parameter mismatch [pə'reɪmɪtə mɪs'mætʃ] несоответствие параметров. @ При обращении к подпрограмме – несоответствие числа или типов фактических параметров числу или типам формальных параметров.

parameter passing [pə'reɪmɪtə 'pa:sɪŋ] передача параметров. @ Операции и структуры данных, используемые вызывающей программой для указания вызываемой процедуре объектов и значений, над которыми должны выполняться действия.

parameter passing by name [pə'reɪmɪtə 'pa:sɪŋ baɪ neɪm] передача параметров по наименованию. @ Способ передачи параметров, при котором выражение задающее фактический параметр, вычисляются заново при каждом обращении к параметру в теле процедуры так, как если бы текст фактического параметра подставлялся вместо каждого вхождения соответствующего формального параметра.

parameter passing by reference [pə'reɪmɪtə 'pa:sɪŋ baɪ 'refrəns] передача параметров по ссылке. @ Способ передачи параметров, при котором вызываемой процедуре передается адрес объекта; выполняемые процедурой действия воздействуют на объект в вызвавшей программе. Передача по ссылке соответствует изменяемым параметрам.

parameter passing by value [pə'reɪmɪtə 'pa:sɪŋ baɪ 'vælju:] передача параметров по значению. @ Способ передачи параметров, при котором вызываемой процедуре передается только копия значения объектов; производимые подпрограммой изменения не отражаются на объекте в вызвавшей программе. Передача по значению соответствует входным параметрам.

parameter specification [pə'reɪmɪtə ,spesɪfɪ'keɪʃən] описание параметров, спецификации параметров. @ Описание типа и способа передачи параметров и, возможно, ограничений, которым они должны удовлетворять.

parametric [pə'reɪmɪtrɪk] *adj.* параметрический. @ **parametric device** параметрический элемент. @ **parametric equation** параметрическое уравнение. @ **parametric representation** параметрическое представление.

parametrically [pə'reɪmɪtrɪkəli] *adv.* параметрически. @ **parametrically Extensible Algorithmic Key (PEAK)** Параметрически расширяемый алгоритмический ключ (название криптосистемы).

part [pɑ:t] *n.* 1. часть; участок; 2. участие, доля в работе; роль; *v.* разделять(ся). # **in part** частично; отчасти. # **in large part** в значительной степени. #

on the part of со стороны кого-л. # **to play part** играть роль. # **to take part** принимать участие.

partial ['pa:ʃəl] *adj.* частичный; частный; парциальный. @ **partial key recovery** частичное восстановление ключа. # **partial equation** уравнение в частных производных.

partially ['pa:ʃəli] *adj.* частично. @ **partially linear** частично линейный. @ **partially-known plaintext cryptanalysis** криптоанализ с использованием частично известного открытого текста.

participant [pa:'tɪsɪpənt] *n.* пользователь.

particular [pə'tɪkjələ] *adj.* 1. особый; особенный; 2. отдельный, частный; данный; конкретный; именно; *pl.* 1. подробности; 2. обстоятельства. @ **particular key** конкретный ключ. # **in particular** в особенности, в частности. # **to go into particulars** вдаваться в подробности.

pass [pa:s] *n.* проход. @ При многопроходной обработке каждый проход последовательно обрабатывает входной файл; выходной файл одного прохода обрабатывается следующим проходом. *v.* 1. передавать (*управление, параметры*). 2. проходить; 3. переходить; 4. пропускать; 5. передавать (**on**); 6. принимать (закон, резолюцию и т. п.). @ **pass in the clear** передавать (сообщение) открытым текстом. @ **pass keying information to an enemy** передавать ключевую информацию противнику. # **in passing** мимоходом; между прочим. # **it is a matter of passing interest** между прочим, можно отметить.

passive ['pa:sɪv] *adj.* пассивный. @ **passive eavesdropping** пассивный перехват (у противника имеется возможность только наблюдать за обменом сообщениями, не оказывая на него никакого влияния).

passive star ['pa:sɪv sta:] пассивная звезда. @ Звездообразная топология сети ЭВМ, в которой центральный узел выполняет только ретрансляцию сигналов и, возможно, коммутацию.

passive wiretap = passive eavesdropping

passphrase ['pa:sfreɪz] *n.* парольная фраза, фраза-пароль (в отличие от пароля, состоит из нескольких слов).

password ['pa:swə:d] *n.* пароль. @ Последовательность символов, которую должен выдавать пользователь или программа для получения доступа к какому-либо ресурсу. @ **password authentication** проверка пароля; аутентификация пользователя по паролю. @ **password encryption key (PEK)** ключ шифрования паролей (используется для дополнительного шифрования информации о пользовательских паролях в операционной системе Windows NT 40 американской корпорации "Майкрософт"). @ **password encryption** шифрование паролей. @ **password protection** защита с использованием пароля. @ **password-protected key** защищенный паролем ключ.

patent ['peɪtənt] *adj.* явный, очевидный. @ **patent repetition** явное повторение (в шифртексте).

pattern ['pætən] *n.* 1. образец, шаблон. 2. образ, изображение; диаграмма; 3. копия, рисунок, картина, узор (*напр. в электростатических запоминающих трубках*); 4. структура; схема; 5. характер, стиль; 6. кристаллическая решетка;

7. комбинация, сочетание.@ **pattern analysis** анализ образцов.@ **pattern inventory** опись конфигураций; ряд, перечисляющий конфигурации.@ **pattern matching** сопоставление с образцом, отождествление.@ **pattern recognition programming** программирование опознаванием образов.

pattern of recognition ['pætən əv rɪ'kɒgnɪʃən] распознавание образов. @ Процесс обнаружения определенной конфигурации в сигнале или приписывания ей вероятности появления.

pay [peɪ] *v.* (**paid**) 1. платить; 2. окупаться, быть выгодным; *n.* оплата.# **it pays** стоит, имеет смысл.# **to pay (turn) attention to** обращать внимание на.

peculiar [pɪ'kjuːliə] *adj.* 1. особый; специфический; своеобразный; 2. свойственный (to).# **to be peculiar** быть характерным.

pending ['pendɪŋ] *adj.* нерешенный, ожидающий решения; очередной.@ **pending key** очередной ключ (предназначенный для замены действующего ключа).@ **pending interrupt** отложенное прерывание. *prp.* 1. в продолжение, в течение; 2. до, в ожидании.

pending job ['pendɪŋ dʒɒb] повисшее задание, повисшая задача.@ Задание, процесс или задача, ждущие наступления события, которое не может произойти в результате ошибки в программе или в вычислительной системе (например, задача может повиснуть в результате обращения к выключенному устройству).

pending request ['pendɪŋ rɪ'kwɛst] ждущий запрос; отложенный запрос.@ Необработанный запрос к операционной системе.

penetrate ['penɪtreɪt] *v.* 1. проникать; 2. вскрывать.@ **penetrate diplomatic codes** вскрывать дипломатические коды.@ **penetrate KDC** проникать в KDC.

penetration ['penɪtreɪʃən] 1. проницаемость; 2. проникновение (успешное преодоление средств защиты системы); 3. преодоление защиты.@ Способ оценки степени защищенности.

pentagram ['pentəgræm] *n.* пентаграмма (пять символов текста).@ **pentagram count** маркировка пентаграмм.@ **pentagram frequency** частота встречаемости (появления) пентаграмм (в тексте).

pentagram counting = count

pentagraph *n.* = **pentagram**

per ['pɜː] *prp.* в, на, за.# **per annum** в год.# **per capita** на человека, на душу населения.# **per centum** процент, на сотню.# **per hour** в час.# **per se** сам по себе, по существу.# **as per** согласно.

perfect ['pɜːfɪkt] *adj.* 1. совершенный, идеальный; 2. законченный.@ **perfect authenticity** совершенная аутентичность.@ **perfect forward secrecy** совершенная форвардная стойкость (про криптосистему говорят, что она обладает совершенной форвардной стойкостью, если сгенерированный с ее помощью шифртекст не позволяет противнику получить какую-либо информацию о соответствующем открытом тексте, кроме, может быть, длины последнего).@ **perfect nonlinear function** (двоичная функция от *n* входных переменных, которая меняет свой выход с вероятностью 1/2 всякий раз, когда ее *i* входов,

$1 < i < n$, изменяют свои значения на противоположные).@ **perfect protection** совершенная защита.@ **perfect security** совершенная стойкость.@ **perfect shuffle** совершенное тасование (разновидность перестановки).

perfect codes ['pɜ:fɪkt kouds] совершенные коды.@ 1. По Хеммингу это коды с исправлением ошибок, в которых шары Хемминга с центром в кодовых словах заполняют все пространство Хемминга, не пересекаясь. Все эти шары имеют радиус e (т. е. код способен исправлять e ошибок), а их центры (кодированные слова) отделены один от другого расстоянием $(2e + 1)$; при этом шары не соприкасаются между собой (т. е. не имеют общих слов), их поверхности находятся на минимальном расстоянии друг от друга, и этот промежуток не содержит других точек. 2. По теории многомерных цифро-векторных множеств совершенные коды это систематические коды со 100% исправлением, например всех одиночных ошибок, которые содержат информационную и контрольную части кода, а во всех ячейках многомерного цифрового пространства этого кода располагаются штатные цифры и соответствующие им цифры с одной ошибкой в информационной или контрольной его частях. Причем в каждой из ячеек располагается только одна цифра.

perfect secrecy = perfect security

perfectly ['pɜ:fɪktli] *adv.* совершенно.@ **perfectly random key** совершенно случайный ключ.

period ['piəriəd] *n.* период, точка (знак препинания).@ **period determination** определение периода.@ **period of group element** порядок элемента группы.@ **period of repeating decimal** период дроби.

periodic(al) ['piəriədɪk(əl)] *adj.* периодический.@ **periodic cipher** периодический шифр.@ **periodic key** периодически сменяемый ключ.@ **periodic polyalphabetic substitution cipher** шифр периодической многоалфавитной замены.@ **periodic sequence** периодическая последовательность.@ **periodic shifted alphabet cipher** шифр (замены) с периодическим смещением алфавита.

periodic *n.* = **periodic polyalphabetic substitution cipher**

periodically ['piəriədɪkəli] *adv.* периодически.

periodicity ['piəriədɪsɪti] *n.* периодичность.@ **periodicity of a sequence** периодичность последовательности.

permanent ['pɜ:mənənt] *adj.* 1. постоянный; неизменный; 2. постоянный ключ; 3. монументальный.@ **permanent error** систематическая ошибка.

permutation [ˌpɜ:mju:'teɪʃən] перестановка, подстановка.@ Перегруппировка элементов множества, изменяющая порядок следования компонентов заданного вектора).@ **permutation box (P-box)** блок перестановок.@ **permutation code (PC)** перестановочный код.@ **permutation matrix** матрица перестановок.

permutation group [ˌpɜ:mju:'teɪʃən gru:p] группа перестановок.@ Подгруппа группы, которая сформирована из множества S_n всех подстановок n отдельных элементов и на которых определена операция композиции функций.

permute [pɜ'mju:t] *v.* переставлять, производить перестановку.

permuter [pə'mju:tə] *n.* блок перестановок, пермутатор (специализированный криптографический узел, используемый для изменения порядка, в котором содержимое регистра сдвига подается на вход других криптографических узлов).

Pers Z *n.* "Отделение Z" (название криптоаналитического бюро МИЛ Германии в 20-е – 40-е годы).

per-session [pə:'seʃən] *adj.* сеансовый. @ **per-session key** сеансовый ключ.

personal ['pə:snl] *adj.* персональный. @ **personal communications system** система персональной связи (включает мобильные телефоны, пейджеры и беспроводные линии сити персональных компьютеров). @ **personal identification number (PIN)** персональный идентификационный номер.

pertinent ['pə:tinənt] *adj.* 1. уместный; подходящий; 2. имеющий отношение, относящийся к (**to**); соответствующий. # **to be pertinent to** иметь отношение к; являться существенным для.

phase ['feɪz] *n.* 1. фаза; 2. период, стадия. # **phasing out** постепенное прекращение серийного производства

phi function = Euler function

phi [faɪ] *n.* фита (буква греческого алфавита Φ). @ **phi test** фита-тест.

phone [fəʊn] *n.* телефон. @ **phone-tapping** перехват разговоров по телефону путем подключения к телефонной линии.

phoney *adj.* = **phony**

phony ['fəʊni] *adj.* ложный, фальшивый. @ **phony public-key** фальшивый открытый ключ.

phrase ['freɪz] *n.* фраза.

phreak ['fri:k] *n.* фрик (специалист в области фриканья).

phreaking ['fri:kɪŋ] *n.* фриканье, фрикинг (наука и искусство несанкционированного подключения к телефонным и другим сетям).

physical (layer) protocol ['fɪzɪkəl ('leiə) 'prəʊtəkɒl] физический протокол. @ Уровень протокола сети передачи данных, регламентирующий механические, электрические, функциональные и процедурные характеристики интерфейса между вычислительной машиной, участвующей во взаимодействии, и средой передачи сигналов.

physical ['fɪzɪkəl] *adj.* физический. @ Имеющий отражение в структуре устройства, в отличие от логического или виртуального. @ **physical block number** физический номер блока. @ **physical device** физическое устройство. @ **physical layer encryption** шифрование на физическом уровне (семиуровневой модели взаимодействия открытых систем).

physical address ['fɪzɪkəl ə'dres] физический адрес. @ 1. Число, идентифицирующее ячейку или область физической памяти. 2. Код, задающий физическое положение данных на внешнем устройстве. Для диска физический адрес имеет вид (номер поверхности, номер дорожки, номер сектора).

physical block ['fɪzɪkəl blɒk] физический блок. @ Порция физического обмена с внешним устройством (обычно диском); участок носителя, на котором размещается порция обмена.

physical data base ['fɪzɪkəl 'deɪtə beɪs] физическая база данных.@ База данных с точки зрения ее представления на физических запоминающих устройствах (обычно дисках).

physical interface ['fɪzɪkəl ɪntə'feɪs] 1. физический интерфейс; 2. сопряжение, физическое подключение.@ Наличие и способ физической связи.

physical layer ['fɪzɪkəl 'leɪə] физический уровень.@ Уровень взаимодействия в сети передачи данных, обеспечивающий интерфейс между вычислительной машиной, участвующей во взаимодействии, и средой передачи сигналов.

physical record ['fɪzɪkəl 'rekɔ:d] физическая запись.@ Порция обмена с внешним устройством. Физическая запись может содержать одну логическую запись, несколько логических записей или часть логической записи.

physical storage ['fɪzɪkəl 'stɔ:ɹɪdʒ] физическая память.@ Внешняя или оперативная память вычислительной системы, реализуемая определенным запоминающим устройством.

physically ['fɪzɪkəli] *adv.* физически.@ **physically random sequence** физически случайная последовательность (получена с помощью генератора, в основе работы которого лежит некое физическое явление).@ **physically random sequence** физически случайная последовательность (получена с помощью генератора, в основе работы которого лежит некое физическое явление).@ **physically secure key** физически защищенный ключ.

picket fence cipher ['pɪkɪt fens 'saɪfə] шифр с отдельным шифрованием четных и нечетных букв алфавита.

piece [pi:s] *n.* 1. кусок; часть; участок; 2. отдельный предмет; штука; 3. произведение, пьеса, картина; 4. деталь.# **piece by piece** по кускам; постепенно.# **all of a piece** сходный, одного качества.# **to be of a piece** образовать единое целое.

pin [pɪn] *n.* штифт; штырь; контактная иглолка.

pinch ['pɪntʃ] *n.* любой украденный у противника объект, который помогает при вскрытии вражеской криптосистемы; *v.* похищать криптографические материалы (ключи, описания шифровальных алгоритмов, схемы шифраторов).@ **pinch pinwheel rotor** цевочный ротор.@ **pinch pinwheel** цевочное колесо.# **pinch-off** отсечка, смыкание.

place ['pleɪs] *n.* место; *v.* помещать.# **in place of** вместо.# **in the first (second etc.) place** во-первых (во-вторых и т. д.).# **in the next place** затем.# **out of place** неуместный, неподходящий.# **to place (lay) emphasis on** выделять, придавать значение, подчеркивать.# **to place hope on** возлагать надежду на.# **to place (set) the limit** установить предел; положить конец.# **to place (put) a premium** поощрять.# **to place reliance on (upon)** полагаться на.# **to place restriction** ограничивать, налагать ограничения.# **to give place to** уступать место.# **to take place** иметь место.

plain [pleɪn] *adj.* 1. ясный; 2. простой; 3. ровный; 4. незашифрованный, открытый.@ **plain code (placode)** код без перешифровки.@ **plain language message** сообщение открытым текстом, нешифрованное сообщение.@ **plain-crypto changeover** переключение с открытой на зашифрованную связь.@ **plain-to-**

crypto 1. преобразование открытого текста в шифрованный; 2. = **plain-crypto changeover**.

plain language = **plaintext** (P)

plaintext (P) ['pleɪn'tekst] открытый текст.@ Сообщение в незашифрованной форме.@ **plaintext alphabet** алфавит открытого текста.@ **plaintext attack secure** защищенный от атаки на основе знания открытого текста.@ **plaintext attack** атака на основе знания открытого текста.@ **plaintext block chaining (PBC)** сцепление блоков открытого текста.@ **plaintext character** знак открытого текста.@ **plaintext cryptanalysis secure** защищенный от криптоанализа на основе знания открытого текста.@ **plaintext cryptanalysis** криптоанализ на основе знания открытого текста.@ **plaintext feedback (PFB)** обратная связь по открытому тексту.@ **plaintext letter frequencies** частоты встречаемости букв в открытом тексте.@ **plaintext letter** буква (буквенный знак) открытого текста.@ **plaintext message** открытое (незашифрованное) сообщение.@ **plaintext recognition** распознавание открытого текста.@ **plaintext restoration** восстановление открытого текста (по имеющемуся шифртексту).@ **plaintext telegram** незашифрованная телеграмма.@ **plaintext unit** отрезок открытого текста.@ **plaintext-cipher-text pair** пара открытый-шифрованный текст.@ **plaintext-ciphertext relation** зависимость между открытым и шифрованным текстом.

plan [plæn] *n.* план, схема; *v.* планировать (выбирать объекты и цели радиоразведывательной деятельности).

planning [plæniŋ] *n.* планирование (выбор объектов и целей радиоразведывательной деятельности).

plant [plɑ:nt] *n.* 1. самомодификация программы; 2. завод; 3. объект; 4. лаборатория; 5. установка оборудования 6. растение; *v.* встраивать, внедрять, вмонтировать.@ **plant collection device** встраивать (внедрять, вмонтировать) устройство для сбора информации.

play [pleɪ] *v.* 1. играть; 2. действовать, приходить в движение; 3. исполнять; *n.* 1. игра; 2. пьеса.# **to bring (call) into play** приводить в действие, осуществлять.# **to come into play** начать действовать.

Playfair cipher шифр Плейфейера.

plenty ['plenti] *n.* изобилие; множество.# **plenty of** много.

plug [plʌg] *n.* разъем; *v.* вставлять в разъем, подключать.# **plug up** блокировать.

plugged control [plʌgd kən'troul] коммутационное управление.

plug-board (PB) ['plʌg,bɔ:d] *n.* коммутатор, штепсельная панель (один из основных узлов немецкой шифровальной машины "Энигма").@ **plug-board connections** соединения коммутатора.@ **plug-board less Enigma** бескоммутаторная "Энигма".@ **plug-board settings** установки коммутатора (в "Энигме").

point [pɔɪnt] *n.* 1. точка, пункт, запятая; 2. пункт, место; 3. вопрос, дело, момент; 4. смысл; 5. точка зрения; 6. острие; *v.* указывать, ссылаться, отмечать (out).@ **point-of-sale encryption** шифрование для обеспечения защиты торговых автоматов.# **point by point** постепенный, последовательный.# **point of view** точка зрения.# **the point at issue** предмет обсуждения (спора).# **the point**

is дело в том, что.# **at all points** во всех отношениях.# **at this point** на данном этапе; здесь.# **from the point of view of** с точки зрения.# **in point** рассматриваемый.# **in point of** в отношении.# **in point of fact** фактически, действительно.# **off the point** не на тему, не по существу.# **on the point of** близкий к чему-л.# **point-to-point** 1. сквозной, межконцевой, оконечный, абонентский; 2. взаимно однозначный.# **to the point** по существу.# **to the point of** до такой степени, что.# **to the point that** до такой степени, что.# **up to this point** до сих пор.# **yield point** предел текучести.# **to be on the point of** + *герундий* собираться сделать что-л.# **to make a point of** + *герундий* настаивать на чем-л.; брать себе за правило.# **to serve one's point** выполнять свое назначение.

poker ['poukə] *n.* покер (карточная игра).@ **poker test** покерный тест (используется для проверки случайности двоичной последовательности).

police (P) [pə'li:s] *n.* полицейский.@ **police channel** полицейский канал связи.

poll [poul] *v.* 1. опрашивать; 2. объединять в общий фонд; *n.* 1. объединение; 2. опрос.# **to poll the experience** делиться опытом, обобщать опыт.# **to poll (the) interests** действовать, сообщать.

polyalphabetic [ˌpɒli'ælfəbetɪk] *adj.* многоалфавитный.@ **polyalphabetic substitution cipher** шифр многоалфавитной замены.

polyalphabetic *n.* = **polyalphabetic substitution cipher**

polycipher *n.* = **polyalphabetic substitution cipher**

polygram [ˌpɒli'græm] *n.* полиграмма (набор из двух и более символов).@ **polygram substitution cipher** шифр полиграммной замены (производит замену полиграмм открытого текста на полиграммы шифрованного текста).

polygraphic [ˌpɒliɡ'ræfɪk] *adj.* полиграфический.@ **polygraphic cipher** полиграфический шифр (осуществляет одновременное преобразование сразу нескольких букв открытого текста в шифрованный).@ **polygraphic substitution cipher system** полиграфический шифр замены.

polynomial [ˌpɒli'noumjəl] *adj.* полиномиальный, многочленный; *n.* полином, многочлен.@ **polynomial multiplication** умножение полиномов.@ **polynomial over GF2** полином над полем GF2.@ **polynomial ring** кольцо полиномов.@ **polynomial transformation of degree n** полиномиальное преобразование степени *n*.

poor [puə] *adj.* 1. бедный; 2. плохой; нестойкий.@ **poor key** нестойкий ключ.

poorly-selected *adj.* = **poor**

Porta Table cipher табличный шифр Porta

position [pə'zɪʃən] *n.* 1. позиция, место цифры, разряд числа; 2. положение; состояние; *v.* 1. ставить на место; 2. определять местоположение.@ **position code** позиционный код.@ **position indicator (PI)** индикатор положения.@ **position tree** дерево положений.# **to be in a position** иметь возможность; быть в состоянии.

positional [pə'zɪʃənəl] *adj.* позиционный. @ **positional representation** позиционное представление. @ **positional system** позиционная система счисления.

positional notation [pə'zɪʃənəl nou'teɪʃən] позиционная нотация, позиционная запись, позиционная система счисления, позиционное представление (числа). @ Представление чисел, при котором значение цифры зависит от ее положения в числе.

positional parameter [pə'zɪʃənəl pə'ræmɪtə] позиционный параметр. @ Параметр, значение которого задается в определенной позиции списка параметров.

positional-independent [pə'zɪʃənəl,ɪndɪ'pendənt] переместимый. @ О программе или структуре данных, которая может быть размещена в любом месте памяти без настройки адресов.

positional-independent code [pə'zɪʃənəl,ɪndɪ'pendənt koud] 1. программа в носительных адресах. @ Программа, которая может быть размещена в любой области памяти, так как все ссылки на ячейки памяти сделаны относительно счетчика команд. 2. непозиционный код. @ Код, в котором местоположение разряда числа не определяет его вес.

positionally [pə'zɪʃənəlɪ] *adv.* позиционно. @ **positionally dependent cipher** шифр, зависящий от положения знаков (текста).

post [pɒst] *n.* пост, станция, пункт (перехвата). @ **post-encryptor** *n.* устройство окончного шифрования.

power ['paʊə] *n.* 1. степень, показатель степени; 2. (**p**, **pwr**) мощность, энергия; 3. способность, возможность; 4. власть; 5. держава; 6. полномочие; 7. степень (*mat.*); *adj.* силовой, энергетический; *v.* снабжать энергией. @ **power function** степенная функция. # **to the ninth (tenth etc.) power** в девятой (десятой и т. д.) степени. # **to the power nine (tenth etc.)** в девятой (десятой и т. д.) степени. # **resolving power** разрешающая способность. # **to raise to the power** возводить в степень.

powerful ['paʊəfʊl] *adj.* стойкий. @ **powerful encryption** стойкое шифрование.

practical ['præktɪkəl] *adj.* 1. практический, основанный на опыте; 2. практический; целесообразный; 3. действительный; фактический. @ **practical security** практическая стойкость. # **by practical consideration** путем эксперимента, опытным путем.

practically ['præktɪkəlɪ] *adv.* практически. @ **practically unbreakable cipher** практически невскрываемый шифр.

practice ['præktɪs] *n.* 1. практика; практическая деятельность; применение; действие; 2. привычка; обыкновение; установившийся порядок. # **in practice** на практике; на деле. # **to put into practice** осуществлять; применять.

preamble [pri:'æmbəl] *n.* преамбула (специальный заголовок, предваряющий текст сообщения).

prearranged [pri:ə'reɪndʒd] *adj.* заранее (предварительно) согласованный. @ **prearranged key** заранее (предварительно) согласованный ключ.

precomputation [pri:kəmpju:'teɪʃən] *n.* предварительные вычисления, пред-вычисления.

precomputed [pri:kəm'pju:tɪd] *adj.* заранее вычисленный. @ **precomputed trial encryption** заранее выполненное пробное шифрование

precomputer [pri:kəm'pju:tə] *adj.* докомпьютерный. @ **precomputer cryptography** докомпьютерная криптография.

predetermined [pri:dɪ'tə:rmɪnt] *adj.* предварительно назначенный, заранее определенный; predetermined. @ **predetermined key** предварительно назначенный (заранее определенный) ключ.

preliminary [pri:'lɪmɪnəri] *adj.* предварительный. # **preliminary to** до. # **to be a preliminary to** предшествовать.

preloaded [pri:'ləʊdɪd] *adj.* заранее (предварительно) загруженный (введенный). @ **preloaded key** заранее (предварительно) загруженный (введенный) ключ.

preloading [pri:'ləʊdɪŋ] *n.* предварительный ввод (ключа); ввод (ключа) до начала работы.

prescientific [pri: ,saɪən'tɪfɪk] *adj.* донаучный. @ **prescientific cryptology** донаучная криптология.

premium ['pri:mjəm] *n.* награда. # **to be at premium** находиться в выгодном положении; быть в большом спросе. # **to place (put) a premium on** поощрять.

present [prə'zent] *adj.* 1. присутствующий; 2. настоящий; современный; 3. имеющийся; данный. # **present-day** современный. # **at present** в настоящее время. # **for the present** на этот раз; пока. # **to be present** присутствовать.

pretty ['prɪti] *adj.* 1. привлекательный; 2. значительный, изрядный; *adv.* вполне, достаточно довольно. @ **pretty Good Privacy (PGP)** "Довольно хорошая секретность" (программа шифрования). # **pretty much** очень; в большой степени; почти.

pretty print ['prɪti prɪnt] структурная распечатка программы. @ Распечатка текста программы в удобном для чтения и анализа виде: каждый оператор размещается на отдельной строке, вложенность блоков, операторов и описаний отмечается сдвигом вправо.

pretty printer ['prɪti 'prɪntə] программа структурированной распечатки. @ Программа, которая принимает текстовый файл и готовит листинг или копию этого файла в формате, удовлетворяющем некоторому набору условий, предъявляемому к внешнему виду текста.

prevent an attack предотвращать атаку.

prevent [prɪ'vent] *v.* 1. предотвращать, предупреждать; 2. мешать, препятствовать (from). @ **prevent an attack** предотвращать атаку.

preventive [prɪ'ventɪv] *adj.* профилактический; предупредительный. @ **preventive maintenance** профилактика, профилактическое обслуживание.

previous ['pri:vjəs] *adj.* 1. предыдущий (**to**); 2. предварительный; *adv.* до, ранее (**to**).@ **previous carry** перенос из предыдущего разряда.@ **previous key** предыдущий ключ.

previously ['pri:vjəslɪ] *adv.* предварительно, заранее.

price [praɪs] *n.* цена.# **at the price** за счет.

primality ['praɪmlɪtɪ] *n.* простота (числа).@ **primality problem** задача проверки простоты числа.@ **primality test** проверка простоты числа.

primary ['praɪməɹɪ] *adj.* 1. главный, основной, имеющий первостепенное значение; 2. первичный, первоначальный.@ **primary alphabet** первичный (исходный) алфавит.@ **primary colors** основные цвета.@ **primary control program (PCP)** первичная управляющая программа.@ **primary failure** независимый отказ.@ **primary implicant** простая импликанта.@ **primary index** основной индекс.@ **primary key** основной ключ.@ **primary type** 1. простой тип. 2. встроенный простой тип.

primary key ['praɪməɹɪ ki:] первичный ключ.@ 1. В базах данных – ключ, о котором в схеме базы данных указано, что он является первичным для данного типа записи. Как правило, система управления базой данных обеспечивает эффективный доступ к записям по первичному ключу. 2. В методах доступа – поле записи, по которому определяется ее положение в файле.

primary memory (main) ['praɪməɹɪ 'meməɹɪ ('meɪn)] первичная память, основная память.@ Оперативная память, та ее часть, которая используется в качестве среды для хранения команд и данных, необходимых для текущего процесса в процессоре.

primary record ['praɪməɹɪ 'rekə:d] первичная запись.@ Запись, ссылка на которую имеется в индексе и через которую осуществляется доступ к записям расширения.

primary station ['praɪməɹɪ 'steɪʃən] первичная станция.@ Станция HDLC, формирующая команды и интерпретирующая ответы одной или нескольких вторичных станций.

primary storage ['praɪməɹɪ 'stɔ:ɪdʒ] 1. основная память.@ В системе управления виртуальной памятью – оперативная память, в которую отображаются блоки виртуальной памяти.

prime [praɪm] *adj.* 1. первичный; 2. основной; 3. превосходный, лучший; *n.* простое число.@ **prime about 1000 bits in length** простое число длиной около 1000 бит.@ **prime attribute** первичный атрибут.@ **prime field GF(p)** простое поле GF(p) (поле GF(p) называется простым, если число p - простое).@ **prime formula** элементарная формула.@ **prime generation** генерация (порождение) простых чисел.@ **prime number** простое число.@ **prime product ring** кольцо по модулю произведения простых чисел.

prime number generation = prime generation

primeness *n.* = **primality**

priming ['praɪmɪŋ] *adj.* первичный, начальный.@ **priming key** первичный (начальный) ключ.

primitive ['prɪmɪtɪv] *adj.* 1. первобытный; 2. простой, несложный; грубый; примитивный; базовый элемент, примитив. @ Элемент, который нельзя разложить на простые формы. @ **primitive attribute** элементарный атрибут. @ **primitive element of the finite field GF(p)** примитивный элемент конечного поля GF(p). @ **primitive element** примитивный элемент. @ **primitive element mod p** примитивный элемент по модулю p. @ **primitive period** основной период. @ **primitive polynomial** примитивный многочлен. @ **primitive recursive scheme** примитивно рекурсивная схема. @ **primitive root** первообразный корень. @ **primitive symbol** исходный символ.

primitive data type ['prɪmɪtɪv 'deɪtə taɪp] базисный тип данных. @ Тип данных (например, целые, вещественные, логические и символьные числа), которые может использовать пользователь какого-либо конкретного типа вычислительного оборудования.

primitive recursive function ['prɪmɪtɪv rɪ'kə:sɪv 'fʌŋkʃən] примитивно рекурсивная функция. @ Функция, которая может быть получена из определенных исходных функций конечным числом применений операций композиций и рекурсии.

primitive type ['prɪmɪtɪv taɪp] простой тип. @ Тип данных, значения которого не содержат компонент (например, целое или символ, в отличие от массива или записи).

principle ['prɪnsəpl] *n.* 1. аксиома; 2. закон, правило; 3. принцип. # **in principle** в принципе; по существу. @ **principle of duality** принцип двойственности. @ **principle of reflection** принцип зеркальной симметрии. @ **principle of superposition** принцип суперпозиции. @ **principle value** главное значение. # **of principle** принципиальный.

printed ['prɪntɪd] *adj.* представленный в печатном виде. @ **printed key** ключ, представленный в печатном виде.

prior [praɪə] *adj.* прежний, предшествующий; предварительный; *adv.* раньше, до. # **prior (to)** до.

privacy ['praɪvəsi] *n.* личная тайна, конфиденциальность. @ **privacy Enhanced Mail (PEM)** Почта повышенной секретности (набор программных средств для обеспечения конфиденциальности сообщений, отправляемых электронной почтой). @ **privacy homomorphism** обеспечивающий секретность гомоморфизм (функция зашифрования, которая предоставляет возможность выполнения ряда требуемых операций над открытым текстом путем выполнения соответствующих операций над шифртекстом). @ **privacy problem** проблема сохранения тайны.

privacy lock ['praɪvəsi lɒk] замок секретности. @ В базах данных – код, связанный с набором, областью или другой группой данных для ограничения доступа к ним.

private ['praɪvɪt] *adj.* 1. приватный, закрытый. 2. частный, закрытый. @ Об информации или информационной системе, доступ к которой открыто только ограниченной группе пользователей (обычно ее владельцу). @ **private circuit** частный канал; выделенный канал. @ **private Communication Technology** Тех-

нология конфиденциальной связи (криптографический протокол, разработанный американской корпорацией "Майкрософт" для обеспечения конфиденциальности сообщений, передаваемых по компьютерной сети "Интернет").@ **private cryptographic algorithm** частный криптоалгоритм (алгоритм, принадлежащий частному лицу или фирме).@ **private data base** частная база данных, закрытая база данных.@ **private exponent** секретный показатель степени.@ **private key distribution** распределение секретных ключей.@ **private key encryption** шифрование с помощью секретных ключей.@ **private key operation** операция с открытым ключом.@ **private key** личный ключ (отдельного пользователя).@ **private library** личная библиотека, библиотека пользователя.@ **private private** секретный ключ (в криптосистеме с открытым ключом).@ **private session key** личный сеансовый ключ (отдельного пользователя).

private data ['praɪvɪt 'deɪtə] 1. приватные данные, закрытые данные. 2. частные данные, частная информация; личные данные, личная информация.@ Данные, доступные только их владельцу.

private type ['praɪvɪt taɪp] приватный тип.@ Тип данных, представление которого скрыто от пользователя и с переменными которого можно работать только экспортируемыми процедурами.

private key cryptosystem = secret-key cryptosystem

pro- [prɒu-] *pref.* со значением за, про-, замещающий, вместо.# **pro and con (pro et contra)** (лат.) за и против.# **pro forma** (лат.) проформа, ради формы, для вида.# **pro rate** (лат.) пропорциональный, пропорционально.# **pro rector** (лат.) проректор, заместитель ректора.

probabilistic [ˌprɒbə'bɪlɪstɪk *adj.* вероятностный.@ **probabilistic approach** вероятностный подход.@ **probabilistic coding** вероятностное кодирование.@ **probabilistic correlation attack** вероятностная корреляционная атака.@ **probabilistic encryption** вероятностное шифрование (открытому тексту сообщения ставится в соответствие множество шифртекстов и делается это таким образом, что получение даже частичной информации об открытом тексте этого сообщения противником, при условии наличия у него одного только шифрованного текста, является труднорешаемой задачей).@ **probabilistic key generation** вероятностная генерация ключей.@ **probabilistic proof** вероятностное доказательство.@ **probabilistic relaxation** вероятностная релаксация (метод вскрытия шифра многоалфавитной замены).

probabilistic logic [ˌprɒbə'bɪlɪstɪk 'lɒdʒɪk] вероятностная логика.@ Логика, в которой истинностные значения представляются вероятностями.

probability [ˌprɒbə'bɪlɪtɪ] *n.* вероятность.@ **probability bound** предельная вероятность.@ **probability calculus** исчисление вероятностей.@ **probability computer** вероятностная вычислительная машина.@ **probability density** плотность вероятности.@ **probability distribution** распределение вероятностей.@ **probability limit** вероятностный предел.@ **probability of error** вероятность ошибки.@ **probability of failure** вероятность сбоя.@ **probability of survival** вероятность безотказной работы.@ **probability of deception** вероятность обмана (введения в заблуждение).@ **probability of successful attack** вероятность

успешной атаки.@ **probability theory** теория вероятности.@ **probability value** вероятность.

probability distribution [ˌprɒbəˈbɪlɪtɪ dɪsˈtrɪbjʊːʃən] распределение вероятностей.@ Теоретическая формула для вероятности того, что наблюдаемая величина примет какое-то конкретное значение или попадет в определенный диапазон значений.

probable [ˌprɒbəbl] *adj.* вероятный.@ **probable key** вероятный ключ (при криптоанализе).@ **probable message cryptanalysis** криптоанализ с использованием вероятного сообщения.@ **probable word cryptanalysis** криптоанализ с использованием вероятных слов.

problem [ˈprɒbləm] *n.* 1. проблема.@ 1. Проблема развития – неудовлетворительное состояние системы, изменение которого к лучшему является непростым делом. 2. Проблема функционирования – удовлетворительное состояние системы, сохранение которого требует постоянных и непростых усилий (например, проблема выживания). 2. задача, вопрос; 3. трудность; *adj.* прикладной.# **to attack the problem** приступить к разрешению проблемы.# **to face the problem** столкнуться с проблемой.# **go get around the problem** разрешить вопрос (проблему).# **to solve (tackle) the problem** разрешить вопрос (проблему).

procedure [ˌprəʊˈsiːdʒə] *n.* 1. методика проведения, процедура; 2. процесс; 3. алгоритм; метод, способ; 4. методика.@ **procedure for key generation** процедура генерации ключей.@ **procedure declaration** описание процедуры.@ **procedure heading** заголовок процедуры.@ **procedure identifier** идентификатор процедуры.@ **procedure parameter** параметр процедуры.@ **procedure statement** оператор процедуры.@ **procedure-oriented programming** процедурное программирование.

procedure body [ˌprəʊˈsiːdʒə ˈbɒdi] тело процедуры.@ Исполнительная часть процедуры; описание реализуемого процедурой алгоритма.

procedure call [ˌprəʊˈsiːdʒə kɔːl] вызов процедуры, обращение к подпрограмме.@ Подразумевается оператор или действия вызывающей программы.

procedure declaration [ˌprəʊˈsiːdʒə ˌdekləˈreɪʃən] описание процедуры.@ Описание процедуры состоит из заголовка процедуры, задающего ее имя и список формальных параметров с их типами, и тела процедуры, определяющего выполняемые при вызове процедуры действия.

procedure division [ˌprəʊˈsiːdʒə dɪˈvɪʒən] раздел процедур.@ Часть программы, содержащая описания исполняемой части программы.

procedure head(er) [ˌprəʊˈsiːdʒə ˈhed(ə)] заголовок процедуры.@ Часть описания процедуры, задающая имя процедуры и определяющая число, тип, форму задания и способ передачи параметров.

procedure invocation [ˌprəʊˈsiːdʒə ˌɪnvəʊˈkeɪʃən] вызов процедуры.@ Действия и данные, связанные с конкретным обращением к подпрограмме.

procedure-oriented language [ˌprəʊˈsiːdʒə ˈɔːrɪəntɪd ˈlæŋɡwɪdʒ] процедурный язык.@ Императивный язык программирования, основанный на понятиях процедуры и переменной. Процедура выполняет некоторое действие, используя и

изменяя значения переменных, являющихся ее параметрами, а также глобальных и локальных переменных. Действия процедуры описываются последовательностью более простых действий, выполняемых обращениями к другим процедурам и базовыми операторами языка. Процедурными языками являются Паскаль, Ада и др.

process ['prouses] *n.* 1. процесс.@ Последовательность операций при выполнении программы или части программы и данные, используемые этими операциями. «Процесс» является единицей диспетчеризации и потребления ресурсов системы. 2. технологический прием; 3. состояние; *v.* 1. обрабатывать; 2. выполнять *v.* обрабатывать.@ **process communications** обрабатывать сообщения (преобразовывать в форму, пригодную для получения разведывательной информации).@ **process chart** диаграмма потоков данных через машину или систему, блок-схема процесса.@ **process state** состояние процессора.@ **process status word (PSW)** слово состояния процессора.@ **process variable** регулируемый параметр процесса.@ **process variable** регулируемый параметр процесса.

process descriptor ['prouses dis'kriptə] описатель процесса; дескриптор процесса.@ Совокупность сведений, определяющих состояние ресурсов, предоставленных процессу.

process image ['prouses 'imɪdʒ] образ процесса.@ Содержимое оперативной памяти, относящейся к процессу, записываемое на диск при выгрузке процесса.

processing ['prousesɪŋ] *n.* обработка (преобразование перехваченных сообщений в форму, пригодную для получения разведывательной информации).@ **processing element** элементарный процессор (*многопроцессорной ЭВМ*).@ **processing gain (PG)** усиление в процессе обработки сигналов.@ **processing interrupt** прерывание отработки.@ **processing loss** потери времени при обработке данных.

processor ['prousesə] *n.* процессор.@ 1. Устройство, выполняющее команды; центральный процессор. 2. Программа, обрабатывающая данные определенного типа.@ **processor interrupt** 1. прерывание процессора; 2. прерывание от процессора.@ **processor state** состояние процессора.@ **processor status word (PSW)** слово состояния процессора.@ **processor time** время счета.@ **processor-active task** текущая задача.@ **processor-flag attack** атака со знанием содержимого регистров процессора (осуществляющего шифрование данных в соответствии с некоторым криптографическим алгоритмом).

processor allocation ['prousesə 'æləkeɪʃən] распределение процессорных ресурсов.@ Определение объемов ресурсов процессора, необходимых каждому процессу.

processor defined function ['prousesə di'faɪnd 'fʌŋkʃən] встроенная машинно-зависимая функция, предопределенная машинно-зависимая функция.@ Функция, которая имеется во всех вариантах системы программирования для разных ЭВМ, но работа которой зависит от конкретной используемой ЭВМ.

processor flags ['prousesə flægs] флаги процессора.@ Разряды слова состояния процессора, описывающие результат выполнения последней команды и режим работы процессора.

processor-bound task ['prousesə 'baund ta:sk] счетная задача.@ Программа, скорость выполнения которой определяется быстродействием процессора.

produce [prɒ'dju:s] *n.* 1. продукция, продукт; 2. результат; *v.* 1. производить, получать; 2. вызывать, быть причиной.@ **produce ciphertext** вырабатывать шифртекст.

product ['prɒdəkt] *adj.* составной, производный, композиционный; *n.* 1. произведение, композиция, суперпозиция (шифров); 2. изделие, продукт.@ **product accumulator** накапливающий сумматор произведений.@ **product cipher** суперпозиция шифров (составной; производный; композиционный шифры).@ **product moment** смешанный момент.@ **product of sets** пересечение множеств.@ **product of sums expression (POS expression)** логическая функция, выражаемая через произведение ее дизъюнктивных членов.@ **product of two ciphers** произведение двух шифров.@ **product operation** операция повторного шифрования (шифрованного сообщения).@ **product portability** переносимость разрабатываемых программ.@ **product register** 1. регистр произведения; 2. счетчик результатов.@ **product row** правило умножения.@ **product space** 1. произведение множеств; 2. область пересечения.@ **product with embedded cryptography** продукт со встроенным криптографическим средством.# **by product** побочный продукт.

product term ['prɒdəkt tə:m] конъюнктивный член, произведение.@ Логическое произведение переменных, взятых с отрицанием или без отрицания, реализуемых с помощью операции И.

production (PROD) ['prɒdəkʃən] 1. продукция, правило вывода, порождающее правило; 2. производство, порождение; 3. постановка; *adj.* промышленный, сданный в эксплуатацию.@ **production formula** формула, приведенная к виду, удобному для логарифмирования.@ **production rule** правило вывода, порождающее правило.

production run ['prɒdəkʃən rʌn] 1. производственный счет; эксплуатация.@ Работа программного обеспечения в реальных промышленных условиях, в отличие от отладки или опытной эксплуатации. 2. рабочий прогон отлаженной программы.

production-rule system ['prɒdəkʃən'ru:l 'sistim] система производственных правил; система продукций.@ Согласованная система правил, в каждом из которых определяется условие его применения и действие, которое должно быть предпринято, когда правило применимо.

productions system ['prɒdəkʃəns 'sistim] система продукций.@ Форма представления знаний или неформального описания программы в виде множества правил (продукций) вида «если А, то В», где А – некоторое условие, а В – соответствующее действие, причем В может содержать переменные, используемые в А. На каждом шаге выполнения программы, заданной в виде системы

продукций, выбирается одно или несколько правил, условия которых истинны, и выполняются соответствующие действия.

productive time ['prɒdɒktɪv taɪm] полезное время.@ Время, затраченное на производственный счет.

productivity ['prɒdɒktɪvɪtɪ] производительность.@ **productivity tools** вспомогательные средства.

professional [prə'fɛnʃənəl] *adj.* профессиональный; *n.* профессионал.@ **professional cryptanalyst** криптоаналитик-профессионал.

program ['prəʊgræm] *n.* 1. программа.@ 1. Последовательность операций или несколько параллельных последовательностей операций, выполняемых ЭВМ для достижения определенной цели; 2. Описание действий, выполняемых ЭВМ, на языке программирования или машинном коде. 2. программировать, составлять программу; *v.* программировать, записывать информацию в ППЗУ.@ **program control** программное управление.@ **program address** программный адрес, адрес программы.@ **program breakpoint** контрольная точка

program check контроль программы.@ **program checkout** 1. отладка программы; 2. испытания программы при сдаче в эксплуатацию.@ **program competition** конкуренция программ, межпрограммная конкуренция.@ **program control unit** блок программного управления.@ **program design** проектирование программы.@ **program development** разработка программ.@ **program error** ошибка в программе.@ **program flowchart** блок-схема программы.@ **program generator** 1. генерирующая программа, программа-генератор; 2. генератор (датчик) программы измерений или контроля.@ **program head** вводная часть программы.@ **program input** входные данные.@ **program instruction** команда программы.@ **program interrupt** 1. программное прерывание; 2. прерывание программы.@ **program language** программный язык.@ **program library** библиотека программ.@ **program loader** загрузчик программ.@ **program location** местоположение (размещение) программы в памяти.@ **program loop** цикл программы, программный цикл.@ **program origin** начальный адрес программы (*в машинном коде или на языке ассемблера*).@ **program parameter** параметр программы.@ **program profile** профиль программы.@ **program proving** доказательство правильности программы.@ **program register** регистр команд.@ **program sensitive malfunction** сбой, обнаруживаемый программой.@ **program status word (PSW)** слово состояния программы.@ **program stop light** индикатор остановки программы.@ **program testing time** время отладки программы.@ **program testing** тестирование программы.@ **program unit** модуль (программы).@ **program verification** верификация программ, доказательство правильности программ.@ **program-control instruction** 1. команда перехода; 2. управляющая конструкция.@ **program-controlled interrupt** программно-управляемое прерывание.@ **program-driven** программно-управляемый.

program background ['prəʊgræm 'bækgraʊnd] фон программы.@ Время, когда программа находится в состоянии ожидания и не занимает центральный процессор.

program body ['prougræm 'bɒdi] тело программы. @ Исполнительная часть программы.

program compatibility ['prougræm kəm.pætə'bɪlɪti] программная совместимость. @ Свойство системы, позволяющее эффективно использовать программы в общей системной среде.

program correctness proof ['prougræm kə'rektnɪs pru:f] доказательство правильности программ. @ Формальное математическое подтверждение того, что семантика программы соответствует предъявленным требованиям, изложенным в спецификации этой программы.

program counter (PC, P-counter) ['prougræm 'kauntə] 1. счетчик команд. @ Регистр процессора, содержащий адрес выполняемой команды или адрес команды, следующей за выполняемой. 2. программный счетчик

program decomposition ['prougræm di'kɒmpə'zɪʃən] декомпозиция программы. @ Разбиение готовой программы на множество составных частей, обычно называемых модулями.

program design language (PDL) ['prougræm dɪ'zain 'læŋɡwɪdʒ]. @ Язык, используемый при разработке программ и имеющий много общего с обычным языком программирования высокого уровня, но больше ориентированный на структуру и содержание, а не на удобство использования программ, написанных на этом языке.

program development system (PDS) ['prougræm dɪ'veləpmənt 'sɪstɪm] система разработки программ. @ Совокупность программных средств, состоящая из редакторов программ, систем подготовки документации, трансляторов, библиотекаря, компоновщика, отладчика и, возможно, других вспомогательных программ.

program development time ['prougræm dɪ'veləpmənt taɪm] полное время подготовки программы. @ Время подготовки программы, включая составление, проверку и отладку.

program editor ['prougræm 'editə] редактор текстов программ. @ Текстовый редактор, имеющий специальные команды для более эффективной работы с текстами программ: автоматическое форматирование, средства вставки и шаблонов операторов, элементы синтаксического анализа.

program element ['prougræm 'elɪmənt] элемент программы. @ Структурная единица описания программы: описание, блок, процедура, контекст, цикл, оператор и др.

program file ['prougræm faɪl] файл программ, программный файл. @ Файл, содержащий одну или несколько программ или их фрагментов на входном языке транслятора или на машинном языке.

program load(ing) ['prougræm 'ləʊd(ɪŋ)] загрузка программы. @ Считывание программы в оперативную память, инициализация и настройка адресов.

program maintenance ['prougræm 'meɪntɪnəns] сопровождение программы. @ Исправление ошибок, внесение модификаций и проведение консультаций по программе, находящейся в эксплуатации.

program scheduler ['prougræm 'ʃədju:lə] планировщик.@ Часть операционной системы, занимающаяся диспетчеризацией процессов и распределением ресурсов.

program segment ['prougræm 'segmənt] сегмент программы.@ Часть программы, отдельно обрабатываемая загрузчиком.

program segmenting ['prougræm 'segməntɪŋ] сегментация программ. @ Разделение программ на сегменты для раздельной загрузки или организации перекрытий.

program specification ['prougræm ,spesɪfɪ'keɪʃən] спецификация программы.@ Точное описание того результата, который необходимо достичь с помощью программы.

program structure ['prougræm 'strʌktʃə] структура программы.@ Общая схема программы, в которой особое внимание уделяется отдельным программным компонентам и взаимосвязями между ними.

program transformation ['prougræm ,trænsfə'meɪʃən] преобразование программ.@ Получение на основе применения систематических методов одних программ из других, так что получаемая программа обладает некоторым полезным свойством и может быть эквивалентна исходной программе.

program translation ['prougræm træns'leɪʃən] 1. конвертирование программы.@ В базах данных – модификация текста программы, работающей в одной системе управления данными, для выполнения тех же функций применительно к конвертированным данным в той же или в другой системе. 2. трансляция программы.

programmable ['prougræmeɪbl] *adj.* программируемый.@ **programmable input-output chip (PIO)** программируемый контроллер.@ **programmable interrupt controller (PIC)** программируемый контроллер прерываний.@ **programmable key storage device (PKSD)** программируемое устройство хранения ключей.@ **programmable logic array (PLA)** программируемая логическая матрица, ПЛМ.

programmable device ['prougræmeɪbl dɪ'vaɪs] программируемые устройства.@ 1. Устройства, работающие под управлением программы, которая хранится в памяти и реализуется в процессе выборки. 2. Интегральные схемы, функции которых определяются пользователем при перепрограммировании, либо один раз за весь срок службы устройства.

programmable read only memory (PROM) ['prougræm'əbl ri:d 'əʊnlɪ 'meməri] программируемое постоянное запоминающее устройство, ППЗУ.@ Постоянное запоминающее устройство (ПЗУ), в которое можно занести различную информацию; различают ППЗУ с однократной записью и стираемые ППЗУ, содержание которых может быть изменено.

progress [prə'gres] *v.* 1. прогрессировать; развиваться; продвигаться; делать успехи; 2. идти; протекать.# **in progress** проводимый в данное время.

project ['prɒdʒekt] *n.* проект.@ **project Minaret** проект "Минарет" (согласно этому проекту с 1969 по 1973 г. в USA осуществлялся комплекс мероприя-

тий, имевших целью ограничить распространение сведений о том, что NSA занимается сбором и обработкой информации конфиденциального характера).@ **project Shamrock** проект "Трилистник" (с 1952 по 1975 г. позволял NSA на добровольной основе получать доступ к телеграммам, которые пересылались по каналам связи крупнейших коммерческих телекоммуникационных компаний USA).

project ['prɒdʒekt] *v.* 1. проектировать; 2. выдаваться, выступать.@ **Project Evaluation and Review Technique (PERT)** планирование с использованием сетевого графика.

project librarian ['prɒdʒekt 'laɪbrəriən] библиотекарь проекта.@ В бригаде главного программиста – член «бригады», отвечающий за программную документацию и обеспечивающий согласованность и сохранность модулей программного продукта.

project software ['prɒdʒekt 'sɒftwɛə] программное обеспечение управляющей системы.@ Программное обеспечение, работающее в режиме реального времени в составе сложной информационной системы или системы управления реальными объектами. Например, система заказа авиабилетов, система управления спутниковой связью.

prominent ['prɒmɪnənt] *adj.* 1. выдающийся; 2. выступающий; выпуклый; заметный.# **to be prominent** выделяться.

proof [pru:f] *n.* доказательство.@ **proof listing** распечатка входной и выходной программ.@ **proof of identity** установление личности.@ **proof of ownership** доказательство права собственности.@ **proof procedure** процедура доказательств.@ **proof scheme** схема доказательства.@ **proof theory** теория доказательств.

propagating ['prɒpəgeɪtɪŋ] *n.* размножение, распространение.@ **propagating cipher block chaining (PCBC)** распространение блоков шифра с размножением.

propagation [ˌprɒpə'geɪʃən] *n.* размножение, распространение.@ **propagation criterion of degree k** критерии размножения (распространения) степени k (двоичная функция удовлетворяет критерию размножения (распространения) степени k, если ее выходное значение меняется с вероятностью 1/2 всякий раз, когда ее *i* входов, $1 < i < k$, изменяют свои значения на противоположные).@ **propagation of errors** размножение (распространение) ошибок.@ **propagation delay** задержка на распространение.@ **propagation time** время распространения, время прохождения (напр. импульса).

proper ['prɒpə] *adj.* 1. надлежащий, соответствующий; 2. правильный; истинный; 3. в собственном смысле слова, собственно, сам; *например*: **China proper** собственно Китай.@ **proper fraction** правильная дробь.@ **proper key** правильный (соответствующий) ключ.@ **proper phase** соответствующая фаза.

proper subset ['prɒpə 'sʌbset] собственное подмножество.@ Подмножество, отличное от самого множества.

properly ['prɒpəli] *adv.* надлежащим образом; правильно; соответственно

property ['prɒpəti] *n.* 1. свойство, способность.@ 1. Качество, постоянно присущее объекту. 2. Абстракция отношения данного объекта с другими, «свернутое отношение», модель отношения. 2. собственность.@ **property list** список свойств.

proprietary [prə'praɪətəri] *adj.* частновладельческий.@ **proprietary crypto-algorithm** частновладельческий криптоалгоритм (криптографический алгоритм, право собственности на который находится в частных руках).

protect [prə'tekt] *v.* 1. защищать, предохранять; 2. покровительствовать.@ **protect a private key against disclosure** защищать секретный ключ от разглашения.@ **protect against a timing attack** защищать от временной атаки.

protection [prə'tekʃən] защита.@ **protection against** защита от.@ **protection circuit** схема защиты.@ **protection lock** замок защиты.

protection domain [prə'tekʃən də'mein] защищенная область.@ Система приоритетов доступа к защищенным ресурсам.

protocol ['prəʊtəkəl] *n.* протокол.@ Совокупность правил, регламентирующих формат и процедуры обмена информацией между двумя или несколькими независимыми устройствами или процессами.@ **protocol hierarchy** иерархия протоколов.@ **protocol stack** пакет протоколов.@ **protocol statement** протокольное предложение.@ **protocol translation** преобразование протоколов.

provable ['pru:vəbl] *adj.* достоверный, доказуемый.@ **provable key** проверенный ключ.@ **provable maximum security** обеспечивать максимальную стойкость.@ **provable prime** достоверно простое число (с доказуемой принадлежностью к классу простых чисел).@ **provable public-key** доказуемо открытый ключ.@ **provable security** доказуемая стойкость.@ **provable-secure cipher** достоверно стойкий шифр.

provably ['pru:vəbli] *adv.* достоверно, доказуемо.

proved [pru:vd] *adj.* проверенный.

provide [prə'vaɪd] *v.* 1. обеспечивать; снабжать; давать; 2. предусматривать (**for**); 3. принимать меры против чего-л. (**against**).# **to provide insight into** давать представление о.

provided [prə'vaɪdɪd] *conj.* при условии (что), если только, при условии если, что

providing [prə'vaɪdɪŋ] *conj.* = **provided**

province ['prɒvɪns] *n.* 1. область, провинция; 2. область (знаний и т. п.); сфера деятельности.# **within the province of** в области; в пределах.# **to be out one's province** быть вне чьей-л. компетенции.

provision [prə'vɪʒən] *n.* 1. обеспечение; 2. мера предосторожности; 3. условие, положение.# **to make provision (for)** предусматривать; обеспечивать; принимать меры.# **with provision for** с учетом, учитывая.

proximity [prɒk'sɪmɪti] *n.* соседство, близость.# **in close proximity to** в непосредственной близости от.

pseudo- ['psj:dou] в сложных и сложносоставных словах имеет значение псевдо-.@ **Pseudo-Hadamard transform (PHT)** псевдопреобразование Адама-ра.@ **pseudokey** псевдоключ (цифровая ключевая последовательность, часть которой используется в качестве ключа).@ **pseudolanguage** псевдоязык.@ **pseudonoise (PN)** псевдошумовой.@ **pseudo-noise binary sequence** псевдошумовая двоичная последовательность (двоичная последовательность называется псевдошумовой, если она удовлетворяет трем критериям случайности, сформулированным американским криптологом С. Голомбом в 1967 г.).@ **pseudo-noise generator (PNSGN)** генератор псевдошума.@ **pseudo-noise** псевдошум.@ **pseudoprime to the base b** псевдопростой по основанию b.@ **pseudoprime** псевдопростой.@ **pseudorandom binary generator** генератор псевдослучайных двоичных последовательностей.@ **pseudorandom binary sequency (PRBS)** псевдослучайная двоичная последовательность.@ **pseudorandom distribution** псевдослучайное распределение.@ **pseudorandom key** псевдослучайный ключ.@ **pseudorandom key generator** генератор псевдослучайных ключей.@ **pseudorandom number generator** генератор псевдослучайных чисел.@ **pseudorandom number key** ключ в виде набора из псевдослучайных чисел.@ **pseudorandom numbers** псевдослучайные числа.@ **pseudorandom permutation** псевдослучайная перестановка.@ **pseudorandom sequence** 1. псевдослучайная последовательность; 2. последовательность псевдослучайных чисел.@ **pseudorandom sequence generator** генератор последовательностей псевдослучайных чисел.@ **pseudorandom sequencer** генератор псевдослучайных последовательностей.@ **pseudorandom time division encryption** мозаичное шифрование (псевдослучайная перестановка сегментов речевых сигналов во времени).@ **pseudorandom** псевдослучайный.@ **pseudorandomness** псевдослучайность.@ **pseudotext** *n.* псевдотекст (текст, полученный в результате пробного дешифрования).

pseudoinstruction (pseudooperation) ['psj:douɪn'strʌkʃən (,ɔpə'reɪʃən)] псевдокоманда.@ Управляющее предложение программы на языке ассемблера, не порождающее машинных команд, но влияющее на работу транслятора.

pseudonoise sequence ['psj:dou'nɔɪz 'si:kwəns] псевдошумовая последовательность.@ Последовательность символов с псевдослучайными свойствами, предназначенная для моделирования помех.

pseudoorder ['psj:douɔ:'də] псевдокоманда.@ Управляющее предложение программы на языке ассемблера, не порождающее машинных команд, но влияющее на работу транслятора.

pseudorandom (PR) ['psj:dou'rændəm] *adj.* псевдослучайный.@ Кажущийся случайным. Таким может быть детерминированный процесс, который в принципе не может быть случайным, но вместе с тем способен демонстрировать ряд проявлений случайности в любой требуемой степени, а поэтому может служить заменителем случайного процесса.

pseudoplaintext = pseudotext

pseudorandom bit generator = pseudorandom binary generator

public ['pʌblɪk] *n.* 1. экспортируемый; общий.@ Термин применяется в языках программирования, не имеющих специальных средств описания интерфейса; 2. общий, открытый.@ Об информации или информационной системе, доступ к которой открыт всем пользователям вычислительной системы.@ **public directory** открытый справочник (ключей или криптоалгоритмов).@ **public encryption operation** открытая операция шифрования.@ **public exponent** открытый показатель степени.

public-key (p-key) ['pʌblɪkɪ] *n.* открытый ключ.@ Системы с открытым ключом предложены У. Диффи и М. Хеллманом в работе «Новые направления в криптографии» («*New Directions in Cryptography*», 1975). Другое их название – асимметричные системы, поскольку в них ключи шифрования и расшифрования не связаны отношениями симметрии или равенства. Ключ шифрования может быть открытым, известным для всех, но расшифровать сообщение может только обладатель секретного ключа расшифрования, который обычно называют закрытым ключом.@ **public-key algorithm (PKA)** алгоритм криптосистемы с открытым ключом.@ **public-key certificate** сертификат на открытый ключ.@ **public-key certification** сертификация (заверение подлинности) открытого ключа.@ **public-key Cryptography Standard (PKCS)** Стандарт шифрования с открытым ключом.@ **public-key cryptography** криптография с открытым ключом.@ **public-key cryptosystem (PKC)** криптосистема с открытым ключом.@ **public-key distribution system** система открытого распространения ключей.@ **public-key encryption** шифрование с открытым ключом.@ **public-key management** управление открытыми ключами (в двухключевой криптосистеме).@ **public-key protocol** (криптографический) протокол с открытым ключом.@ **public-key registry** регистрация открытого ключа (специальный процесс регистрации открытого ключа, обеспечивающий достоверную информацию лицу, которое осуществляет запрос относительно этого ключа).@ **public-key-secret key pair** пара открытый-секретный ключ (в криптосистеме с открытым ключом).# **general public** широкая публика.# **public at large** широкая публика.

public-key system = **public-key cryptosystem**

publicly-revealed ['pʌblɪkɪ,rɪ'vi:lɪt] *adj.* открытый.@ **publicly-revealed an algorithm in a certified public directory** опубликован алгоритм в заверенном открытом справочнике.@ **publicly-revealed key** открытый ключ зашифрования/расшифрования (в двухключевой криптосистеме).

publish ['pʌblɪʃ] *v.* издавать, опубликовать.

published ['pʌblɪʃt] *adj.* опубликованный.@ **published cryptoalgorithm** криптоалгоритм, опубликованный в открытой печати.@ **published key** ключ на перфокарте.

punch-card ['pʌntʃka:d] *n.* перфокарта.

purchase ['pʊ:tʃəs] *v.* покупать; приобретать.

purchased ['pʊ:tʃəst] *adj.* приобретенный.@ **purchased key** приобретенный (посредством подкупа) ключ.

pure [pjʊə] *adj.* 1. чистый; 2. однородный; 3. однородный, без примесей. @ **pure cipher** однородный шифр (шифр, в котором для любых трех преобразований зашифрования, расшифрования и снова зашифрования можно найти шифрующее преобразование, идентичное произведению трех преобразований). @ **pure data** константы, неизменяемые данные. @ **pure function** функция без побочного эффекта. @ **pure gain** чистое усиление. @ **pure mathematics** чистая математика. @ **pure-Hstening attack** атака на основе одного только прослушивания (канала речевой связи). @ **pure-listening attack secure** защищенный от атаки на основе одного только прослушивания (канала речевой связи).

pure code [pjʊə koud] «чистый код». @ Программа или часть программы в машинных командах, не содержащая изменяемых ячеек. Такая программа рентабельна. а также пригодна для записи в ПЗУ.

purported ['prə:pətid] *adj.* предполагаемый. @ **purported originator** предполагаемый отправитель (сообщения). @ **purported transmitter** предполагаемый передатчик (сообщения).

purpose ['prə:pəs] *n.* цель, назначение, предназначение, намерение. @ 1. Образ желаемого будущего (субъективная цель); 2. Будущее реальное состояние (объективная цель); *v.* 1. иметь целью 2. намериваться. # **the purpose in view** поставленная цель. # **general purpose** универсальный. # **special purpose** специализированный. # **on purpose** нарочно, намеренно.

purposeful ['prə:pəsful] *n.* целенаправленный.

purposely ['prə:pəslɪ] *adv.* 1. нарочно, с целью; 2. преднамеренно.

push [puʃ] *v.* 1. толкать; 2. рекламировать. @ **push button** нажимная кнопка, клавиша. @ **push pop** помещать на стек. @ **push-down list** магазинный (стечковый) список. @ **push-down (list) stack** стек.

put [put] *n.* 1. выводить. @ 1. Помещать запись в файл или базу данных. *Ср. get, write*; 2. Выводить изображение в форме точечной матрицы на экран дисплея. 2. класть; 3. излагать; 4. предлагать, выдвигать (**forward**); 5. пропускать (**through**); 6. записывать (**down**). # **to put aside** отложить. # **to put into effect** осуществлять, приводить в исполнение. # **to put into practice** осуществлять, приводить в исполнение. # **to put into operation** вводить в действие. # **to put into play** вводить в действие. # **to put on trial** подвергать испытанию. # **to put (leave) out of account** не принимать во внимание. # **to put the other way round** другими сло-вами. # **to put restraints in** налагать ограничение на. # **to put to rights** привести в порядок.

puzzle ['plʌzl] *n.* загадка. @ "шарада" — криптограмма, полученная при помощи блочного шифра с малым ключевым пространством и содержащая ключ в заданной стандартной форме). @ **puzzle Palace** "Дворец загадок" (иносказательное название, придуманное американским журналистом Д. Бэмфордом для Агентства национальной безопасности USA).

pre- ['pri:] (в сложных и сложносоставных словах имеет значение) 1. заранее, предварительно; 2. предварительный; предшествующий. @ **pre-ciphering** предварительное шифрование. @ **pre-encrypt** шифровать предварительно. @ **pre-encryptor** устройство предварительного шифрования. @ **per-call** сеансо-

вый (предназначенный для одного сеанса связи)/@ **per-call key** сеансовый ключ.@ **per-connection** предназначенный для одного соединения.@ **per-connection key** ключ для одного соединения.

Q*

quadratic ['kwɔːdrætɪk] *adj.* квадратичный.@ **quadratic congruential generator** квадратичный конгруэнтный генератор.@ **quadratic equation** квадратичное уравнение.@ **quadratic form** квадратичная форма.@ **quadratic function** квадратичная функция.@ **quadratic mean** среднее квадратичное.@ **quadratic residue cipher (QRC)** шифр квадратичных вычетов.@ **quadratic residue modulo n** квадратичный вычет по модулю n (целое число a такое, что уравнение $x^2 = a \bmod n$ имеет целочисленное решение).@ **quadratic residuosity problem** задача о квадратичных вычетах.@ **quadratic sieve factoring** факторизация методом квадратичного решета.

quadrature ['kwɔːdrətʃə] квадратура.

quantum ['kwɒntəm] квант; *adj.* квантовый.@ **quantum cryptography (QC)** квантовая криптография. На стыке квантовой физики и математики развиваются квантовые вычисления и квантовая криптография. Хотя квантовые компьютеры лишь дело будущего, уже сейчас предложены алгоритмы для взлома существующих «надёжных» систем (например, алгоритм Шора). (в квантовой криптографии стойкость криптосистем основывается на принципе неопределенности квантовой механики) @ Промежуток времени, отведенный для отдельного процесса в системе управления с квантованием времени.@ **quantum effect** эффект квантования, влияние квантования.

quasi ['kwa:zi] *adv.* как будто; как бы, якобы.

quasi- ['kwa:zi] в сложных и сложносоставных словах имеет значение квази-.@ Приставка, иногда используемая в терминологии вычислительной техники в сложных словах вместо приставки псевдо-, как, например, в терминах, квазисинусоидальный или квазикоманда.@ **quasi-diagonal matrix** квазидиagonalная матрица.@ **quasi-random number generator** генератор квазислучайных чисел.@ **quasi-random** квазислучайный.@ **quasi-resonant** квазирезонансный.@ **quasi-steady** квазистационарный.@ **quasi-weak key** квазинестойкий ключ.@ **quasi-weak** квазинестойкий.

question ['kwesntʃən] *n.* 1. вопрос; 2. проблема; *v.* сомневаться, подвергать сомнению.# **the question is** дело в том, что.# **beyond (all) question** вне (всякого) сомнения, не-сомненно.# **past (without) question** вне (всякого) сомнения, несомненно.# **in question** рассматриваемый, обсуждаемый, о котором идет речь.# **the matter in question** обсуждаемый вопрос.# **to be open to question** об этом не может быть и речи; совершенно невозможно.# **to call in question** быть сомнительным (спорным).# **to go into (the) question** рассмотреть вопрос.# **to make no question of** не сомневаться, вполне допускать.

quinque- [kwɪŋ] в сложных и сложносоставных словах имеет значение пяти-.@ **quinteliteral** пятизначный.@ **quinteliteral cipher alphabet** пятизначный шифрalfавит (служит для замены одного знака открытого текста пятью знаками шифрованного текста).

quite [kwaɪt] *adv.* совсем, вполне, совершенно.# **quite a difference** большая разница.# **quite a few** довольно много, порядочно.# **quite as much** в такой же мере (степени).

R*

radiation ['reɪdɪeɪʃən] *n.* излучение.@ **radiation-protected** защищенный от воздействия излучений.

radio ['reɪdiəʊ] *n.* радио.@ **radio broadcast network** радиовещательная циркулярная сеть.@ **radio eavesdropping** радиоперехват.@ **radio frequencies** радиочастоты.@ **radio frequency (RF)** радиочастота.@ **radio intelligence unit** радиоразведывательное подразделение.@ **radio intelligence** радиоразведка.@ **radio intercept** радиоперехват.@ **radio noise (RN)** радиопомеха; радиочастотный шум.@ **radio reconnaissance service** радиоразведывательная служба (служба радиоразведки).

railway [reɪl'weɪ] *n.* железная дорога.@ **railway Enigma** "Железнодорожная Энигма" (модификация шифровальной машины "Энигма", которая во время второй мировой войны использовалась немцами для шифрования данных, связанных с железнодорожными перевозками).@ **railway key** ключ к "Железнодорожной Энигме".

raise [reɪz] *v.* 1. возбуждать (*особую ситуацию*); 2. поднимать; 3. повышать; увеличивать; 4. выращивать; *n.* 1. подъем; 2. повышение; увеличение.# **to raise doubts** вызывать сомнение.# **to raise to the power** возводить в степень.

random ['rændəm] *adj.* 1. случайный; беспорядочный, хаотичный; 2. произвольный; 3. статический.@ **random access machine** компьютер, оснащенный запоминающим устройством с произвольной выборкой.@ **random access memory** запоминающее устройство с произвольной выборкой.@ **random bit generator** генератор случайных битовых (двоичных) последовательностей.@ **random cipher** случайный шифр.@ **random cryptanalysis** криптоанализ методом случайного поиска.@ **random distribution** случайное распределение.@ **random initialization** случайное начальное заполнение (регистра сдвига) (случайная начальная загрузка (шифратора).@ **random key encryption** шифрование на случайном ключе.@ **random key generator** генератор случайных ключей.@ **random key** случайный ключ.@ **random mapping** случайное отображение.@ **random mixed sequences** случайные смешанные последовательности.@ **random number generator** генератор (датчик) случайных чисел.@ **random number (RN)** случайное число.@ **random padding** случайное холостое заполнение (дополнение сообщения ничего не значащей случайной информацией).@

random permutation случайная перестановка.# **at random** наугад; произвольно.

random bit pattern generator = **random bit generator**

randomization ['rændəmaɪzɪʃən] *n.* рандомизация (внесение элемента случайности в работу криптографического оборудования).

randomize ['rændəmaɪz] *v.* рандомизировать, делать случайным.

randomized ['rændəmaɪzd] *adj.* рандомизированный.@ **randomized encipherment system** рандомизированная система шифрования.@ **randomized stream cipher** рандомизированный потоковый шифр.

randomized key encryption = **random key encryption**

randomizer ['rændəmaɪzə] *n.* рандомизатор (аналоговый или цифровой источник случайных последовательностей).

randomizing ['rændəmaɪzɪŋ] *adj.* рандомизирующий.@ **randomizing sequence** рандомизирующая последовательность.

randomly ['rændəmlɪ] *adv.* случайно.@ **randomly chosen** выбранный случайно.@ **randomly-chosen key** случайно выбранный ключ.@ **randomly-generated** сгенерированный случайным образом.

randomly-selected = **randomly-chosen**

randomness ['rændəmni:s] неопределенность стохастическая.@ Неопределенность, описываемая распределением вероятностей на множестве возможных состояний рассматриваемого объекта; случайность.@ **randomness postulate** критерий случайности (критерий проверки случайности двоичной последовательности).@ **randomness walk** метод случайного блуждания.

rang *n.* = **rank**

range [reɪndʒ] *n.* 1. диапазон; отрезок, интервал, амплитуда, размах; 2. область значений функции. *Ср. domain*; 3. область; сфера; 4. пределы, диапазон; 5. пробег; *v.* 1. находиться; 2. изменяться; 3. колебаться (в известных пределах), варьировать; 4. пробегать; 5. доходить до (**up**).# **a range of** ряд, множество.# **a wide range** большое разнообразие.# **ranging from ... to** в пределах от ... до.# **over (within) the range** в пределах; в диапазоне.

rank [ræŋk] *v.* 1. классифицировать; относить; причислять; считаться; 2. занимать место (положение); 3. относиться; считаться; *n.* 1. категория, разряд, класс; 2. оценка; 3. ранг.@ 1. Номер некоторого объекта в упорядоченном по некоторому признаку ряду объектов. 2. Элемент порядковой (ранговой) шкалы.@ **rank of a language** норма языка.@ **rank of a matrix** ранг матрицы.# **rank and file** рядовой.# **to rank with** иметь то же значение, что и; занимать то же место, что и.

rate [reɪt] *n.* 1. коэффициент, степень; процент; 2. скорость, интенсивность, частота; 3. норма; производительность; 4. сорт; *v.* определять, оценивать.@ **rate of a code** скорость передачи кода.@ **rate of change** степень изменения.@ **rate of decay** скорость убывания.@ **rate of exchange** скорость обмена.@ **rate of increase** коэффициент прироста.# **at any rate** по крайней мере, во всяком случае.# **first rate** первоклассный.

rather ['rɑ:ðə] *adv.* 1. лучше, охотнее; 2. скорее, вернее; 3. довольно, несколько, до некоторой степени. # **rather than** а не; скорее, чем; вместо того, чтобы.

raw *adj.* = **undigested**

reach ['ri:tʃ] *v.* 1. достигать, доходить; 2. протягивать; *n.* досягаемость. # **beyond the reach** недостижимый. # **far reaching** многообещающий. # **of far reaching importance** имеющий большое значение. # **out of (the) reach** вне пределов досягаемости. # **within the reach** в пределах досягаемости, достижимый, доступный.

reaction [ri:ækʃən] *n.* 1. реакция; 2. обратное действие; 3. взаимодействие; 4. противодействие; *adj.* реакционный. @ **reaction attack** реакционная атака (атакующий использует реакцию жертвы на свои действия для достижения исковой цели). # **side reaction** побочная реакция.

read cryptograms читать криптограммы.

read *v.* 1. читать (дешифровывать); 2. читать, считывать (информацию).

read [ri:d] *v.* 1. читать, читать (дешифровывать); считывать. @ 1. Перемещать информацию с более низкого уровня иерархии памяти на более высокий: с внешнего устройства или внешней памяти в оперативную память, из оперативной памяти в регистр процессора. 2. Операция чтения блока из файла или внешнего устройства. @ **read after write check** контроль считывания после записи. @ **read and restore cycle** считывание с восстановлением. @ **read cycle** цикл считывания. @ **read error** ошибка считывания. @ **read only memory** постоянная односторонняя память. @ **read operation** операция считывания. @ **read out gate** 1. вентиль считывания; 2. выходной вентиль; 3. вентиль выдачи (напр. суммы). @ **read out time** время считывания. @ **read out** выходной сигнал считывания. @ **read period** период считывания. @ **read rate** скорость чтения. @ **read time** время чтения. @ **read word element** элемент считывания слов.

really *adv.* действительно. @ **really random sequence** действительно случайная последовательность (если генератор действительно случайных последовательностей запустить два раза с одинаковыми входами, полученные выходные последовательности будут разными).

real [riəl] *adj.* 1. вещественный, действительный. @ О числах, представляющих нецелые величины. 2. реальный; 3. настоящий; 4. вещественный. @ **real accumulator** накапливающий сумматор действительных частей комплексных чисел. @ **real axis** действительная (реальная) ось комплексной плоскости. @ **real constant** вещественная константа, действительная константа. @ **real part** вещественная часть (комплексного числа). @ **real root** действительный корень. @ **real storage** физическая оперативная память, основная память.

real address mode [riəl ə'dres moud] режим реальной адресации, режим абсолютной адресации. @ Режим работы процессора, при котором отключены средства преобразования виртуальных адресов в физические.

realization ['riəlaɪzeɪʃən] *n.* реализация.

realize ['riəlaɪz] *v.* 1. осуществлять; 2. основывать, понимать.

realm [reɪlm] *n.* 1. область. @ В базах данных – поименованная область базы данных. Распределение записей по областям задается независимо от их типов и связей. Понятие области в языке описания данных дает некоторые средства управления физическим размещением записей. 2. сфера, область.

real-time ['riəl'taɪm] *adj.* (производимый) в реальном масштабе времени; *n.* реальное время. @ **real-time buffer** буфер для работы в истинном масштабе времени, буферное запоминающее устройство для работы в истинном масштабе времени. @ **real-time computation** вычисление в истинном масштабе времени. @ **real-time computer** вычислительная машина, работающая в режиме реального времени. @ **real-time data processing** 1. обработка данных в реальном масштабе времени; 2. обработка данных в темпе их поступления. @ **real-time environment** режим реального времени; условия реального времени. @ **real-time mode** режим реального времени. @ **real-time operation** обработка в реальном масштабе времени. @ **real-time preview** предварительный просмотр в рабочем режиме. @ **real-time problem** задача, решаемая в реальном масштабе времени. @ **real-time processor** 1. вычислительная машина для обработки данных в реальном масштабе времени; 2. вычислительная машина для обработки данных в темпе их поступления.

real-time clock (RTC) ['riəl'taɪm klɒk] часы реального времени. @ Логическое или физическое устройство вычислительной системы, выдающее абсолютное или относительное астрономическое время.

real-time executive ['riəl'taɪm ˌeksɪ'kjutɪv] операционная система реального времени. @ Операционная система, предоставляющая программам средства для работы в режиме реального времени.

real-time language ['riəl'taɪm 'læŋɡwɪdʒ] язык реального времени. @ Язык программирования, предназначенный для систем, в которых критическим временем является время реакции вычислительной машины на сигналы, требующие от нее ответных действий.

real-time processing ['riəl'taɪm 'prəʊsesɪŋ] обработка в реальном времени; работа в режиме реального времени. @ Режим обработки данных, при котором обеспечивается взаимодействие вычислительной системы с внешними процессами в темпе, соизмеримом со скоростью протекания этих процессов. Система реального времени должна обеспечить достаточную скорость реакции на внешние прерывания и параллельную работу процессов, обслуживающих разные внешние устройства.

real-time system ['riəl'taɪm 'sɪstɪm] система реального времени. @ 1. Система, работающая в реальном времени. 2. Операционная система, позволяющая программам работать в режиме реального времени.

real-world ['riəl'wɜːld] *adj.* истинный, действительный, реальный, практический (*о решаемой задаче или применении системы*).

real-time decryption ['riəl'taɪm 'dekɪptʃən] расшифрование в реальном масштабе времени

real-world random sequence = really-random sequence

rear ['riə] *adj.* расположенный сзади; тыловой; *n.* 1. задняя сторона; 2. тыл. # **to the rear** позади; в тылу.

reason ['ri:zn] *v.* 1. рассуждать; 2. приводить доводы, убеждать; *n.* 1. причина, основание; довод; соображение; 2. разум, рассудок. # **by reason** по причине, вследствие. # **for this (that) reason** по этой причине. # **for which reason** по этой причине. # **for reasons given** на основании это-го. # **for practical reasons** из практических соображений. # **for some reason or other** по той или иной причине. # **if for no reason than** хотя бы потому, что. # **it stands to reason** ясно, очевидно. # **with reason** не без основания.

reasoning ['ri:znɪŋ] *n.* 1. рассуждения, вывод. @ В экспертных системах и искусственном интеллекте – процесс получения новых фактов (заключений) по имеющимся фактам и правилам вывода. 2. довод, аргументация; *adj.* мыслящий. # **reasoning from this fact** исходя из этого. # **by the same reasoning** на том же основании

reassigned ['ri:əsɪnt] *adj.* назначенный заново, переназначенный. @ **reassigned key** назначенный (переназначенный) заново (другому пользователю) ключ.

receive [ri'si:v] *v.* получать; принимать (сообщение и т. п.).

received [ri'si:vt] *adj.* полученный. @ **received message** полученное сообщение.

receiver (RAVR) [ri'si:və] *n.* приемное устройство, приемник; получатель, адресат (сообщения). @ **receiving register** приемный регистр.

recently [ri'sntli] *adv.* недавно, за последнее время. # **more recently** позднее. # **until recently** до недавнего времени.

recipient *n.* = **receiver**

reciprocal [ri'sɪprəkəl] *n.* обратная величина; *adj.* 1. взаимный, обоюдный; 2. соответственный; эквивалентный; 3. обратный; 4. возвратный. @ **reciprocal polynomial** возвратный полином. @ **reciprocal theorem** обратная теорема.

recirculating shift register = **feedback shift register**

reckon ['reskən] *v.* 1. считать, подсчитывать; 2. полагать, предполагать; 3. полагаться на (**upon**); 4. принимать во внимание (**with**). # **according to our reckoning** по нашему мнению, на наш взгляд. # **in the final reckoning** в конечном счете.

recognition [ri'kɒgnɪʃən] *n.* 1. узнавание; опознавание; 2. признание, одобрение. # **in recognition of the circumstance** в знак того, что

recomputation [ri,kəm'pjʊ:'teɪʃən] *n.* повторное вычисление (криптографической контрольной суммы).

recompute [ri:kəm'pjʊ:t] *v.* вычислять повторно.

reconstruct ['ri:kəns'trʌkt] *v.* восстанавливать (удаленные или испорченные данные), реконструировать. @ **reconstruct a military code** реконструировать военный код.

reconstructed ['ri:kəns'trʌktɪd] *adj.* восстановленный, реконструированный. @ **reconstructed plaintext** восстановленный (в результате расшифрования или дешифрования шифртекста) открытый текст.

reconstruction ['ri:kəns'trʌkʃən] *n.* восстановление, реконструкция. @ **reconstruction of internal settings of a cipher system** восстановление внутренних установок шифрсистемы. @ **reconstruction of the plaintext** восстановление открытого текста. @ **reconstruction of the specific keys to the cipher system** восстановление конкретных ключей шифрсистемы.

record ['rekɔ:d] *v.* записывать, регистрировать; *n.* 1. запись. @ 1. Группа взаимосвязанных элементов данных, рассматриваемая как единое целое; составной элемент данных. В реляционных базах данных соответствующее понятие называется кортеж. 2. В языках программирования – составное значение с компонентами разных типов. 2. протокол; 3. данные. # **on record** зарегистрированный. # **as a matter of record** на основании полученных данных.

recourse [ri'kɔ:s] *n.* обращение за помощью. # **to have recourse (to)** прибегать к помощи. # **without recourse (to)** не прибегая к помощи.

recover [ri'kʌvə] *v.* 1. возвращать, получать обратно; 2. выздоравливать; 3. добывать (выделять); 4. восстанавливать(ся). @ **recover a plaintext** восстанавливать открытый текст (из зашифрованного). @ **recover an encryption key from a decryption key** получать ключ зашифрования из ключа расшифрования. @ **recover session keys** восстанавливать сеансовые ключи.

recovered [ri'kʌvəd] *adj.* восстановленный. @ **recovered plaintext** восстановленный (в результате расшифрования или дешифрования шифртекста) открытый текст.

recoverable error [ri'kʌvəreɪbl 'erə] исправленная ошибка.

recovery [ri'kʌvəri] *n.* 1. восстановление. @ Средства, обеспечивающие способность системы восстанавливать целостность хранимой информации после сбоя; 2. выздоровление; 3. извлечение, добыча; 4. регенерация. @ **recovery time** время восстановления.

recovery log [ri'kʌvəri lɒg] журнал восстановления. @ Файл, обеспечивающий возможность восстановления базы данных или текущего состояния файла.

recreate ['rekri:ɛɪt] *v.* восстанавливать, воссоздавать.

recreation ['rekri:ɛɪʃən] *n.* восстановление, воссоздание.

recurrence [ri'klərəns] *n.* 1. рекуррентность. @ **recurrence relation** рекуррентное соотношение; 2. рекуррента.

recurring [ri'klərɪŋ] *adj.* рекуррентный. @ **recurring sequence** рекуррентная последовательность.

recursion [ri'kə:ʃən] *n.* рекурсия.

recursive [ri'kə:sɪv] *adj.* рекурсивный. @ **recursive computation** рекурсивное вычисление. @ **recursive descent parsing** синтаксический анализ рекурсивной функции. @ **recursive descent** рекурсивный спуск. @ **recursive procedure** рекурсивная процедура. @ **recursive process** рекурсивный процесс. @ **re-**

cursive row рекурсивное правило.@ **recursively enumerable set** рекурсивно перечисляемое множество.

recursive call [rɪ'kə:sɪv kɔ:l] рекурсивное обращение.@ Обращение к подпрограмме из нее самой или из вызванной ею подпрограммы.

recursive definition [rɪ'kə:sɪv ,defɪ'nɪʃən] рекурсивное определение. @ Определение, ссылающееся на определяемый объект. Например, «идентификатор – это буква или идентификатор, за которым следует буква или цифра».

recursive function [rɪ'kə:sɪv 'fʌŋkʃən] рекурсивная функция.@ Функция, определение которой использует саму определяемую функцию.

recursive list [rɪ'kə:sɪv lɪst] рекурсивный список.@ Список, который содержит сам себя в качестве элемента подсписка или является элементом подсписка одного из своих подподписков.

recursive relation [rɪ'kə:sɪv rɪ'leɪʃən] рекурсивное отношение.@ Отношение, характеристическая функция которого является рекурсивной.

recursive set [rɪ'kə:sɪv set] рекурсивное множество.@ Множество, принадлежность к которому определяется общей рекурсивной функцией.

recursive subroutine [rɪ'kə:sɪv səb,rʊ:'tɪn] рекурсивная подпрограмма.@ Подпрограмма, при выполнении которой прямо или косвенно вызывается эта же подпрограмма. См. *тж.* **recursive function**

recursive transition network [rɪ'kə:sɪv træn'sɪzən 'netwə:k] рекурсивная сеть переходов.@ Описание рекурсивного автомата в виде сети переходов. Вершины сети соответствуют состояниям автомата, а дуги – переходам, соответствующим входным символам. Дуги могут соответствовать либо простому переходу, либо вызову подсети.

red [red] *adj.* 1. красный; 2. открытый, незашифрованный.@ **red a key to a manageable size** уменьшить длины ключа до приемлемой величины.@ **red box** блок обработки открытой информации.@ **red data** незашифрованные данные.@ **red designation** обозначение систем, линий и аппаратуры связи для передачи и обработки незашифрованной информации.@ **red machine** "красная" машина (условное наименование, данное американскими криптоаналитиками японской шифровальной машине, находившейся в эксплуатации с 1932 по 1941 г.).@ **red side** сторона шифратора обрабатывающая открытые данные.@ **red signal** открытый сигнал (любое электромагнитное излучение, которое несет в себе информацию об используемых ключах обрабатываемых открытых текстах и алгоритмах функционирования криптографического оборудования).@ **red thread** "красная нить" (программная закладка внедряемая в шифровальную программу для понижения ее стойкости).@ **red-black concept** концепция разделения открытой и зашифрованной информации.@ **red-black isolation** разделение открытой и зашифрованной информации.

reduce [rɪ'dju:s] *v.* 1. уменьшать, понижать, ослаблять; 2. сводить, приводить; 3. восстанавливать; 4. сокращать.@ **REDUCE** программа для аналитических преобразований.

reduced [rɪ'dʒuːst] *adj.* уменьшенный, упрощенный. @ **reduced equation** приведенное уравнение. @ **reduced instruction set computer (RISC)** ЭВМ с сокращенным набором команд. @ **reduced-size sample of cryptosystem** упрощенный вариант криптосистемы с уменьшенными значениями параметров.

reduced instruction set computer architecture (RISC) [rɪ'dʒuːsd ɪn'strʌkʃən set kəm'pjuːtə 'a:kɪtektʃə] RISC – архитектура. @ Подход к организации ЭВМ на базе упрощенного набора машинных команд, обеспечивающего простоту изготовления и простоту написания трансляторов.

reducibility [rɪ'dʒuːsɪbɪlɪtɪ] *n.* сводимость. @ **reducibility axiom** аксиома сводимости. @ **reducibility problem** проблема сводимости.

reducible [rɪ'dʒuːsəblɪ] *adj.* приводимый. @ **reducible polynomial** приводимый многочлен (полином).

reduction [rɪ'dʌkʃən] *n.* 1. снижение, уменьшение, понижение, сокращение; 2. приведение к одному знаменателю; 3. сведение, редукция. @ **reduction machine** [rɪ'dʌkʃən mə'ʃiːn] редукционная машина. @ Организация ЭВМ, при которой программа представляет собой набор правил подстановки и выражения, подвыражения которого заменяются (редуцируются) в соответствии с правилами. Правила и подвыражения могут обрабатываться с произвольной степенью параллелизма. Такая организация соответствует языкам логического программирования.

redundancy [rɪ'dʌndənsɪ] *n.* избыточность. @ Свойство сигналов и систем, обеспечивающее их устойчивость против разрушительного воздействия помех, шумов, отказов элементов, непредвиденных обстоятельств и т.п. Это свойство состоит во включении в структуру системы или сигнала большего числа элементов, чем это минимально необходимо при отсутствии помех. Если критерий эффективности связан с минимизацией числа элементов, то при отсутствии помех избыточность является излишней, а при наличии помех – полезной, но возникает задача ее минимизации. @ **redundancy of message information contained in a N-sign cryptogram** избыточность текста криптограммы из N знаков.

redundancy check (RC) [rɪ'dʌndənsɪ tʃek] контроль за счет избыточности. @ Способ контроля искажений элемента данных при хранении или передаче, при котором вместе с информацией хранятся или передаются функционально зависящие от нее величины; повторное вычисление контрольных величин при считывании или приеме позволяет обнаружить ошибки.

redundant [rɪ'dʌndənt] *adj.* избыточный. @ **redundant authenticating information** избыточная аутентификационная информация. @ **redundant element removal (RER)** удаление избыточных элементов. @ **redundant information** избыточная информация.

reencipher ['riːen'saɪfə] *v.* перешифровывать. @ **reencipher with the appropriate key** перешифровывать на соответствующем ключе.

reencode ['rɪn'koud] *v.* перекодировать.

reencodement ['rɪn'koudment] *n.* перекодирование.

reencrypt *v.* = **reencipher**

refer [rɪ'fɜː] *v.* ссылаться на (**to**); 2. отсылать к (**to**); 3. упоминать; 4. относиться, иметь отношение к (**to**).# **to be referred to as** называться.

reference (**ref**) [ˈrefrəns] *n.* 1. ссылка, сноска; упоминание; 2. справка; 3. рекомендация; отзыв; 4. отношение; 5. эталон; 6. *pl.* библиография; 7. (**ref**) опорный сигнал; опорный уровень; *adj.* 1. исходный; 2. контрольный; 3. стандартный; 4. эталонный.# **to make reference to (for)** упоминать, ссылаться на.# **frame of reference** система отсчета (координат).# **of reference** исходный; эталонный; сравнительный.# **in (with) reference to** относительно, что касается; ссылаться на.# **without reference to** безотносительно к; независимо от.

reflect [rɪ'flekt] *v.* 1. отражать (*свет, звук*); 2. отражаться, давать отражение; 3. размышлять, раздумывать.

reflected [rɪ'flektɪd] рефлексный.@ **reflected binary code** рефлексный двоичный код.@ **reflected code** рефлексный (циклический) код, рефлексивный код.

reflection [rɪ'flekʃən] *n.* 1. отражение; отблеск; 2. раздумье, размышление.# **on reflection** подумав.

reflecting [rɪ'flektɪŋ] *adj.* рефлекторный.@ **reflecting rotor** рефлектор, рефлекторное колесо (ротор).

reflector *n.* = **reflecting rotor**

refuge [ˈrefjuːdʒ] *n.* убежище, прибежище.# **to take refuge in** прибегнуть к.

regard [rɪ'gɑːd] *v.* 1. считать, рассматривать; 2. касаться, иметь отношение; 3. принимать во внимание, считаться (кем-л., чем-л.); *n.* 1. внимание, забота; 2. отношение; 3. взгляд.# **as regards** что касается, в отношении.# **in (with) regard to** относительно.# **with due regard for** учитывая должным образом.# **without regard for** не учитывая.# **to have regard to** учитывать, обращать внимание.

register (**reg**) [ˈredʒɪstə] *n.* регистр, линейка слова в ассоциативном запоминающем устройстве; *v.* регистрировать.@ **register ALU (RALU)** регистровое АЛУ.@ **register length** емкость регистра, число разрядов в регистре.@ **register of length n** регистр длины (размера) *n*.@ **register operation (RO)** регистрация операции.@ **register optimization** оптимизация регистров.@ **register tap** точка съема (регистра сдвиги с обратной связью) .@ **register transfer logic (RTL)** логика (меж)регистровых передач.@ **register with carry shift register** регистр сдвига с обратной связью и переносом.@ **register** регистр сдвига с обратной связью.@ **register-direct addressing** прямая регистровая адресация.@ **registering apparatus** регистрирующее устройство.

register allocation [ˈredʒɪstə 'æləkeɪʃən] распределение регистров, назначение регистров.@ Определение соответствия регистров процессора и обрабатываемых данных; выполняется транслятором или программистом при программировании на языке ассемблера.

register capacity [ˈredʒɪstə kæ'pəsɪti] разрядность регистра.@ Число информационных битов в регистре.

register file ['redʒɪstə faɪl] массив регистров.@ Набор рабочих регистров процессора.

register transfer language ['redʒɪstə 'trænsfə 'læŋgwɪdʒ] язык межрегистровых пересылок.@ Язык высокого уровня для описания архитектуры процессора.

register variable ['redʒɪstə 'vɛəriəbl] регистровая переменная.@ Переменная, для которой транслятор выделяет регистр процессора, а не ячейку оперативной памяти.

register-to-register instruction ['redʒɪstə'tu:'redʒɪstə ɪn'strʌkʃən] команда типа «регистр-регистр».@ Команда, операнды и результат которой располагаются в регистрах процессора.

register-to-storage instruction ['redʒɪstə'tu:'stɔ:rɪdʒ ɪn'strʌkʃən] команда типа «регистр-память».@ Команда, операнды которой располагаются в регистрах, а результат записывается в оперативную память.

register-transfer-level simulator ['redʒɪstə'trænsfə'levl 'sɪmjuleɪtə] программа моделирования на уровне регистровых операций.@ Часть системы проектирования логических схем.

registry *n.* = **directory**

re-injected shift register = **feedback shift register**

reject [rɪ'dʒekt] *v.* отвергать, отбрасывать.@ **reject a message as unauthentic** отвергать сообщение как ложное.

rejection [rɪ'dʒekʃən] *n.* отбрасывание.

relapse [rɪ'læps] *n.* 1. повторение; рецидив; 2. спад; уменьшение; *v.* снова впадать (в какое-л. состояние)

rekey [rɪ'ki:] *v.* вводить ключ повторно.

rekeying [rɪ'kiŋ] *n.* повторный ввод ключа.

relate [rɪ'leɪt] *v.* 1. иметь отношение; относить(ся); 2. связывать, устанавливать отношения; 3. рассказывать.# **relating to** в отношении; касающийся.# **to be related to** иметь отношение к; быть связанным с.

related [rɪ'leɪtɪd] *adj.* 1. родственный; имеющий отношение; 2. связанный; смежный.@ **related prime to** относительно простой по отношению к.@ **related-data cryptanalysis** криптоанализ с использованием дополнительных данных.@ **related-data key** "родственный" ключ (производный от другого ключа или имеющий какое-либо еще к нему отношение).@ **related-key cryptanalysis** криптоанализ на основе "родственных" ключей (исследуется влияние различий между ключами на работу шифратора).

relation [rɪ'leɪʃən] *n.* 1. отношение.@ 1. Подмножества декартова произведения нескольких множеств. 2. В реляционных базах данных – совокупность кортежей с одинаковыми атрибутами; отношение можно представлять как прямоугольную таблицу, строки которой соответствуют экземплярам (записям), а столбцы – атрибутам. 2. (со)отношение, связь, зависимость.@ **relation matrix** матрица отношений.# **in relation to** относительно; что касается.# **to bear a relation to** иметь отношение к.

relative ['relətiv] *adj.* 1. относительный; сравнительный; 2. соответствующий. @ **relative accuracy** относительная точность, относительная погрешность. @ **relative addressing** относительная адресация. @ **relative error** относительная ошибка; относительная погрешность. @ **relative file** файл прямого доступа. @ **relative maximum** относительный максимум. @ **relative product** композиция. @ **relative programming** программирование в относительных адресах. # **relative to** относительно; в связи с.

relative address ['relətiv ə'dres] относительный адрес, смещение. @ Адрес, заданный относительно некоторой базы.

relative command ['relətiv kə'ma:nd] относительная команда. @ В машинной графике – команда отображения, параметры которой интерпретируются как координаты относительно предыдущей точки.

relative complement ['relətiv 'kɒmplɪmənt] относительные координаты. @ Координаты, задающие положение точки относительно некоторой другой точки.

relative coordinates ['relətiv kou'ɔ:dnɪts] разность множеств, дополнение. @ Множество, являющееся разностью множеств А и В, состоит из элементов принадлежащих А и не принадлежащих В.

relative frequency ['relətiv 'fri:kwənsɪ] относительная частота. @ Число повторений данного события А, поделенное на общее число наблюдаемых событий.

relative pathname ['relətiv pa:θ'neɪm] относительное составное имя, относительный путь. @ Составное имя файла или каталога, префикс которого указывает путь от текущего каталога; для файлов текущего каталога относительное составное имя имеет пустой префикс.

relative vector ['relətiv 'vektə] относительный вектор. @ Вектор, конечная точка которого задана смещением относительно начальной точки.

relatively ['relətivli] *adv.* относительно. @ **relatively prime** взаимно-простые числа.

release [rɪ'li:s] *n.* 1. версия, редакция. @ Очередной распространяемый вариант программного продукта. 2. освобождение; 3. выделение; снятие; *v.* 1. выпускать; 2. освобождать. @ Возвращать системе распределения ресурсов ранее полученный ресурс (например, блок памяти, линию связи). 3. отпускать (*нажатую клавишу*). @ **release prefix** редакционный префикс (пометка в заголовке документа с ключевой информацией, свидетельствующая о том, что ближайшие союзники USA могут получить доступ к содержимому этого документа).

reload [rɪ'loud] *v.* загружать (вводить) заново. @ **reload a key** загружать (вводить) ключ заново.

remote [rɪ'maʊt] *adj.* удаленный. @ **remote control key erasure** дистанционно управляемое стирание ключа (записанного в памяти). @ **remote key entry** удаленный ввод ключа. @ **remote key load** удаленная загрузка (удаленный ввод) ключа.

remote keying = **remote key entry**

remote rekeying = **remote key entry**

repeated [rɪ'pi:tɪd] *adj.* повторный, повторяющийся, многократный. @ **repeated encryption** повторное (повторяющееся, многократное) шифрование. @ **repeated key cipher** шифр с повторяющимся ключом (шифртекст вырабатывается при помощи повторного сложения по модулю 2 знаков открытого текста и периодической ключевой последовательности, полученной путем повторения исходного ключа). @ **repeated key load** повторная загрузка (повторный ввод) ключа. @ **repeated plaintext digraphs** повторяющиеся биграммы открытого текста.

repeatedly [rɪ'pi:tɪdli] *adv.* многократно, неоднократно

repeat [rɪ'pi:t] *v.* повторять; воспроизводить. @ **repeat-statement** оператор цикла с условием завершения.

repeat-until loop [rɪ'pi:t,ʊn'tɪl lu:p] цикл с условием завершения, цикл «пока-не». @ В языках программирования – конструкция, обеспечивающая повторение последовательности действий до тех пор, пока не станет истинно заданное условие, причем условие проверяется после каждого выполнения цикла.

repetition [rɪ'pɪtɪʃən] *n.* повторение. @ **repetitions in a ciphertext** повторения в шифртексте. @ **repetition instruction** команда повторения, повторяемая команда, команда с повторителем.

repetition codes [rɪ'pɪtɪʃən kəʊds] коды с повторением. @ Семейство циклических совершенных блочных кодов с исправлением ошибок, в которых ключевые слова формируются многократным повторением сообщения.

repeating *adj.* = **repeated**

repetitive *adj.* = **repeated**

replacement [rɪ'pleɪsmənt] *n.* замена, подстановка.

representative [reprɪzen'teɪtɪv] *adj.* характерный, показательный (**of**); *n.* 1. представитель; 2. образец. # **to be representative of** отражать, быть характерным.

repute [rɪ'pju:t] *n.* общее мнение, репутация; *v.* считать, полагать. # **of repute** известный, знаменитый. # **a scientist of world wide repute** известный всему миру ученый, ученый с мировым именем. # **to be in repute** славиться, быть известным. # **to have a repute for** славиться чем-л.

requeue [rɪ'kju:] *v.* повторно ставить в очередь, возвращать в очередь.

require [rɪ'kwaɪə] *v.* требовать.

required *adj.* требуемый. @ **required key** требуемый ключ. @ **required label** обязательная (необходимая, требуемая) метка. @ **required parameter** обязательный параметр.

required space [rɪ'kwaɪd speɪs] обязательный пробел. @ В системах подготовки текстов – символ, отображаемый как пробел, но обрабатываемый как буква или разделитель.

requirement [rɪ'kwaɪmənt] *n.* 1. требование; условие; 2. нужда, потребность. @ **requirement description** техническое задание

requirement specification 1. техническое задание; 2. описание требований к программному средству.

requirement analysis [rɪ'kwaɪment ə'næləsɪz] анализ требований. @ Анализ, выполняемый на этапе разработки технического задания.

rescrambling [rɪ'skræmblɪŋ] *n.* повторное скремблирование.

reserve [rɪ'zə:v] *v.* 1. сберегать; запасать; сохранять; откладывать; 2. резервировать; *n.* 1. запас; резерв; 2. оговорка; 3. осторожность. @ **reserve key** запасной (резервный) ключ. @ **reserve keying material** запасной ключевой материал (ключи, предназначенные для использования при возникновении непредвиденных обстоятельств). # **with reserve** осторожно. # **with some reserve (reservation)** с некоторой оговоркой, осторожно. # **without reserve** безоговорочно.

reserved [rɪ'zə:vd] *adj.* зарезервированный. @ О коде операции или поле структуры данных, которые не используются системой, но не должны использоваться и пользователем. @ **reserved code** зарезервированная команда, запрещенная команда.

reserved instruction [rɪ'zə:vd ɪn'strʌkʃən] зарезервированная команда, запрещенная команда. @ Машинная команда, код которой не входит в систему команд.

reserved word [rɪ'zə:vd wə:d] зарезервированное слово, служебное слово. @ В языках программирования – последовательность букв, которая не может использоваться в качестве идентификатора, так как имеет специальное значение в языке, например, является частью синтаксической конструкции.

residence ['rezɪdəns] *n.* резидентура.

resident ['rezɪdənt] *adj.* резидентный. @ Постоянно находящийся в оперативной памяти. *n.* резидент. @ Резидентная часть программы. @ **resident software** резидентная программа.

resident compiler ['rezɪdənt kəm'paɪlə] резидентный транслятор. @ Транслятор, постоянно находящийся в оперативной памяти.

resident executive ['rezɪdənt ˌeksɪ'kjutɪv] резидентная операционная система. @ Операционная система, постоянно располагающаяся в оперативной памяти.

resident library ['rezɪdənt 'laɪbrəri] резидентная библиотека. @ Группа загруженных в оперативную память подпрограмм, к которым могут обращаться другие программы.

residual [rɪ'zɪdʒuəl] *adj.* остаточный. @ **residual error** остаточная ошибка (погрешность).

residue ['rezɪdʒu:] *n.* 1. остаток (от деления); 2. вычет. @ **residue arithmetic** арифметика в остаточных классах. @ **residue class** класс вычетов. @ **residue number system** система счисления остаточных классов. @ **residue r-th crypto-system** криптосистема с остатком порядка *r*.

residue check ['rezɪdʒu: tʃek] контрольная сумма. @ Сумма всех слов или байтов порции данных (файла, блок, записи).

resing [rɪ'zaɪŋ] *v.* 1. отказываться от (*права и т. н.*); 2. уходить в отставку. # **to resing all hope** оставить всякую надежду.

resist [rɪ'zɪst] *v.* сопротивляться; противодействовать; противостоять. # **to offer resistance** оказывать сопротивление.

resistance to cryptanalytic attack = **resistance to cryptanalysis**

resistance [rɪ'zɪstəns] *n.* стойкость @ **resistance against ciphertext-only attack** стойкость против атаки на основе знания одного только зашифрованного текста. @ **resistance to cryptanalysis** стойкость против криптоанализа.

resistant [rɪ'zɪstənt] *adj.* стойкий; прочный; устойчивый к (to). @ **resistant against plaintext attack** стойкий против атаки со знанием открытого текста.

resistant to plaintext attack = **resistant against plaintext attack**

resolution [ˌrezə'lʊ:ʃən] *n.* 1. разрешающая способность, разрешение. @ Для растровых дисплеев определяется числом точек раstra на экране, для растровых печатающих устройств – числом точек раstra на единицу длины. 2. резолюция. @ Правило вывода в исчислении предикатов, удобное для использования при автоматическом построении доказательства. 3. решение (математической задачи). @ **resolution of decryption** решение задачи дешифрования. @ **resolution error** ошибка в результате недостаточной разрешающей способности или разрядности. @ **resolution theorem proving** доказательство теорем методом резолюции.

resource [rɪ'sɔ:s] *n.* 1. ресурс. @ Логическая или физическая часть вычислительной системы, которая может быть выделена процессу: время центрального процессора, область оперативной или внешней памяти, логическое или физическое внешнее устройство. 2. (обычно *pl.*) ресурсы, запасы, средства, возможности; 3. средство, способ. @ **resource-limited cryptanalyst** криптоаналитик с ограниченными ресурсами. # **natural resources** естественные богатства.

respect [rɪs'pekt] *n.* 1. уважение; 2. отношение; *v.* 1. уважать; 2. щадить. # **in respect of** в отношении, что касается. # **with respect to** в отношении, что касается. # **in respect that** учитывая, принимая во внимание. # **in all respects** во всех отношениях. # **in no respect** ни в каком отношении. # **without respect to** не принимая во внимание.

responsible [rɪs'pɒnsəbl] *adj.* ответственный за что-л. (for). # **to be responsible for** быть ответственным; обуславливать; составлять; являться автором чего-л.

responsive [rɪs'pɒnsɪv] *adj.* отзывчивый.

resrain [rɪs'treɪn] *n.* 1. сдерживать; удерживать (from); 2. ограничивать. # **to put resraints in** налагать ограничения на.

rest [rest] *n.* покой, отдых; *v.* 1. отдыхать; покоиться; 2. основывать(ся); 3. оставаться. # **the rest** остаток, остальное(ые). # **at rest** в покое, неподвижный. # **for the rest** в остальном; что касается остальных. # **to come to rest** остановиться.

restoration [rɪs'tɔ:reɪʃən] *n.* восстановление.

restore [rɪs'tɔ:] *v.* восстанавливать.@ Придавать переменной исходное или предыдущее значение или приводить информационный объект в исходное состояние.

restored [rɪs'tɔ:d] *adj.* восстановленный.@ **restored message** восстановленное (после зашифрования) сообщение.

restrict [rɪs'trikt] *v.* ограничивать.

restricted [rɪs'triktɪd] *adj.* суженный; узкий, ограниченный.@ **restricted predicate calculus** узкое исчисление предикатов.

restricted data [rɪs'triktɪd 'deɪtə] защищенные данные, информация с ограниченным доступом.@ Данные (файл, запись, часть базы данных), доступ к которым разрешен только части пользователей.

restricted type [rɪs'triktɪd taɪp] ограниченный тип, строгий тип.@ Приватный тип данных, для переменных которого запрещены операции присваивания и сравнения на равенство.

restriction [rɪs'triksən] ограничение, сужение.

restrictive [rɪs'triktɪv] *adj.* ограничительный, сдерживающий.

result [rɪ'zʌlt] *v.* 1. получаться; 2. происходить в результате, быть следствием (**from**); 3. давать в результате, приводит к (**in**); *n.* результат.# **with the result that** в результате чего.

result address [rɪ'zʌlt ə'dres] адрес результата.@ Адрес, по которому записывается значение результата операции.

result data item [rɪ'zʌlt 'deɪtə 'aɪtəm] элемент данных - результат.@ В базах данных - производный элемент данных, значение которого является копией значения другого элемента данных.

resultant [rɪ'zʌltənt] *n.* результирующий вектор.

resulting [rɪ'zʌltɪŋ] *adj.* результирующий, получающийся.@ **resulting cryptogram** результирующая криптограмма.@ **resulting key** результирующий ключ.@ **resulting deduction** результативный вывод.

retired [rɪ'taɪəd] *adj.* использованный.@ **retired key** использованный ключ.

retrieval [rɪ'tri:vəl] *n.* 1. поиск информации; 2. выборка.@ **retrieval system** система поиска данных.@ **retrieval time** время поиска информации.

retrieve [rɪ'tri:v] *v.* 1. найти (снова); 2. восстанавливать; исправлять

retrospect ['retroʊspekt] *n.* взгляд назад, взгляд в прошлое.# **in retrospect** ретроспективно.

retrospective equation [retroʊ'spektɪv i'kweɪʃən] ретроспективное уравнение, уравнение для распределения в прошлом.

return (ret) [rɪ'tə:n] *n.* 1. возврат.@ Выход из подпрограммы и возврат управления вызвавшей программе. 2. возвращение; 3. результат; *adj.* обратный; *v.* возвращаться.# **in return for** взамен.

reuse ['ri:ju:z] *n.* повторное использование; *v.* повторно использовать.@ **reuse of a key** повторное использование ключа.@ **reuse a pad** повторно использовать шифроблокнот.

reveal [rɪ'vi:l] *v.* 1. показывать, обнаруживать; 2. раскрывать; разоблачать. @ **reveal a secret key to an enemy** раскрывать перед противником секретный ключ.

revealed [rɪ'vi:lt] *adj.* раскрытый, разглашенный. @ **revealed key** раскрытый ключ (вскрытый противником или ставший ему известным в силу каких-либо других обстоятельств).

reverse [rɪ'və:s] *adj.* обратный; противоположный; *v.* менять. @ **reverse assembler** дисассемблер. @ **reverse bias** обратное смещение. @ **reverse consequence** обратная последовательность. @ **reverse index** 1. обратный индекс; 2. перемещение текущей позиции вверх (*в обработке текста*). @ **reverse Polish notation (RPN)** постфиксная запись, польская инверсная (обратная) запись, полиз. @ **reverse standard cipher alphabet** обратный стандартный шифрalfавит. @ **reverse-engineer a cryptographic algorithm from executable code** восстановить криптографический алгоритм средствами обратного проектирования по исполняемому коду (программы). @ **reverse-engineer a smart card** восстанавливать алгоритм функционирования интеллектуальной карты средствами обратного проектирования. @ **reverse-engineer** *v.* восстанавливать средствами обратного проектирования.

reverse execution [rɪ'və:s ,eksɪ'kju:ʃən] обратное выполнение. @ Имитация выполнения программы от точки останова или конца программы к началу. Для обеспечения обратного выполнения при каждом присваивании значения переменной сохраняется ее старое значение. При обратном выполнении переменные восстанавливают сохраненные значения.

reversed [rɪ'və:st] *adj.* обращенный, расположенный в обратном порядке. @ **reversed alphabet** обращенный (расположенный в обратном порядке) алфавит.

reverse-encode *v.* = **decode reverse-encrypt** = **decrypt**

reversible [rɪ'və:sɪbl] *adj.* обратимый. @ **reversible encryption** обратимое шифрование. @ **reversible process** обратимый процесс. @ **reversible relation** обратимое соотношение. @ **reversible transformation** обратимое преобразование.

review [rɪ'vju:] *v.* 1. делать обзор; 2. пересматривать; 3. рецензировать; *n.* 1. обзор; 2. рецензия. # **under review** рассматриваемый.

revoke [rɪ'vouk] *v.* аннулировать, объявлять недействительным. @ **revoke a key** аннулировать, (объявлять недействительным) ключ.

revoked [rɪ'voukt] *v.* аннулированный, объявленный недействительным. @ **revoked a key** аннулированный, (объявленный недействительным) ключ.

rig [rɪg] *v.* искусственно занижать стойкость. @ **rig a cipher machine** искусственно занижать стойкость шифратора.

rigged [rɪgət] *adj.* характеризующийся искусственно заниженной стойкостью. @ **rigged Crypto AG cipher machine** шифратор фирмы "Крипто AG" с искусственно заниженной стойкостью.

right [raɪt] *adj.* 1. прямой; 2. правый; правильный, верный; 3. правый (в противоположность левому); *adv.* 1. прямо; 2. как раз; *n.* право.# **right away** немедленно, сразу.# **right down to** вплоть до.# **in one's own (right)** в своем праве; по праву.# **in the right way** правильно, надлежащим образом.# **on one's own (right)** самостоятельно; сам по себе.# **to put rights** привести в порядок

ring [rɪŋ] *n.* кольцо.@ Множество S , на котором определены две операции (сложение и умножение), причем S является группой по отношению к сложению и моноидом по отношению к умножению, сложение коммутативно, а умножение дистрибутивно по отношению к сложению. Например, множество целых чисел.@ **ring accumulator** кольцевой накапливающий сумматор.@ **ring counter** кольцевой счетчик.@ **ring shift** циклический сдвиг.

ring network [rɪŋ 'netwɜ:k] кольцевая сеть, сеть типа «кольцо».@ Топология сети ЭВМ, при которой каждый узел связан с двумя другими; все узлы вместе образуют кольцо. Узел получает сообщение от одного из соседей и либо обрабатывает его сам, либо ретранслирует его другому соседу.

ring structure [rɪŋ 'strʌktʃə] кольцевая структура.@ Список, последний элемент которого указывает на первый.

Rip van Winkle cipher шифр Рипа ван Винкля

rise [raɪz] *v.* (**rose, risen**) 1. подниматься; 2. возрасть. *n.* 1. возрастание; 2. возникновение.# **to give rise to** вызывать, приводить к.

Rivest's Cipher = Rivest's Code

Rivest's Code (RC) Код Ривеста (общее название серии алгоритмов шифрования, разработанных Ривестом).

Rocket = Railway Enigma

roll [roul] *v.* прокручивать; просматривать.@ **roll-call polling** круговой опрос абонентов.

rollback ['roulbæk] возврат.@ Перезапуск обработки с контрольной точки.

roll-in [roul'in] 1. загрузка, подкачка. 2. загрузка, считывание.@ Считывание группы данных из внешней памяти в оперативную память.

roll-out [roul'aut] 1. выгрузка, откачка. 2. выгрузка, сохранение.@ Запись группы данных из оперативной памяти во внешнюю память.

rolling [roulɪŋ] *adj.* чередующийся, изменяющийся.@ **rolling bandscrambler** спектрально-полосный скремблер с чередующимся кодом перестановки полос.@ **rolling mode** режим работы с изменяющимся ключом.

rolling key = running key

"Room 40" *n.* "Комната 40" (подразделение английского адмиралтейства, в годы первой мировой войны занимавшееся криптоанализом перехваченных шифросообщений противника).

"Room Forty" = "Room 40"

root [ru:t] *n.* 1. корень.@ Исходный узел древовидной структуры, от которого доступны все остальные узлы. 2. причина, источник, корень; *adj.* коренной, основной.# **root mean square (r.m.s.)** средне-квадратичное (значение).# **the root of the matter** сущность вопроса.

rotary ['routəri] *adj.* 1. поворотный; 2. вращательный; 3. ротационный; роторный 4. вращающийся. @ **rotate alphabet 13 places (rot13)** вращать алфавит на 13 позиций (простейший шифр, который заменяет каждую букву английского алфавита на другую, расположенную в нем через 13 позиций). @ **rotary wheel** роторное колесо.

rotate initial settings = starting positions

rotate [rou'teɪt] *v.* 1. вращать; 2. циклически сдвигать. @ **rotate machine** роторная (колесная) шифровальная машина. @ **rotate movement** движение роторов. @ **rotate order** порядок следования роторов. @ **rotate starting positions** начальные положения роторов.

Rotation Cipher = rotate alphabet 13 places

rotor ['routə] *n.* ротор, колесо.

rough [ɹʌf] *adj.* 1. грубый, шероховатый; необработанный; 2. приблизительный; маловероятный. @ **rough approximation** грубая аппроксимация. @ **rough frequency count** маркировка (текста), показывающая значительные отличия от равновероятного распределения. # **rough and ready** поспешный.

roughness ['ɹʌfnɪs] *n.* маловероятность.

round ['raʊnd] *n.* цикл, раунд (один из последовательных шагов обработки в алгоритме блочного шифрования). @ **round function** функция цикла (раунда). @ **round key** ключ цикла (раунда).

route [raʊt] *n.* 1. путь, маршрут. @ Последовательность узлов сети передачи данных, по которой данные передаются от источника к приемнику. 2. траектория. @ **route transposition sequences** путевые перестановочные последовательности. @ **route transposition** шифр путевой перестановки.

routine [ru:'ti:n] *n.* 1. подпрограмма; 2. стандартная программа, стандартная подпрограмма, алгоритм; 3. шаблон; *adj.* 1. обычный, установившийся; 2. серийный. @ **routine library** библиотека программ. @ **routine maintenance** сопровождение, обслуживание; профилактика. @ **routine of work** режим работы.

routing ['raʊtɪŋ] *n.* маршрутизация. @ Выбор последовательности узлов сети передачи данных, по которой данные передаются от источника к приемнику. @ **routing information** сведения маршрутизации.

routing table (directory) ['raʊtɪŋ 'teɪbl (dɪ'rektəri)] таблица маршрутизации. @ Таблица, связанная с узлом сети коммутации пакетов или сообщений и указывающая для каждого адресата оптимальный выходной канал может быть указано несколько каналов в порядке их предпочтительности.

R. Rivest, A. Shamir and L. Adelman (RSA). @ **RSA algorithm** алгоритм RSA. @ **RSA Data Security Incorporated (RSADSI)** (название американской компании, производящей средства шифрования данных) . @ **RSA implementation** реализация алгоритма RSA. @ **RSA key pair** пара открытый-секретный ключ в криптосистеме RSA. @ **RSA Laboratories (RSALABS)** подразделения американской компании RSA Data Security Incorporated. @ **RSA protocol for mental poker** протокол RSA для игры в покер "вслепую" (криптографический протокол, дающий возможность честно играть в покер, не прибегая к картам). @ **RSAREF** библиотека криптографических процедур на языке програм

мирования "Си", разработанная американской фирмой RSA Laboratories. @ **RSA scheme** схема RSA. @ **RSA system** криптосистема RSA. Криптосистема построена на основе степенной функции с секретом $f(x) = x^e \bmod n$, где определение открытого текста по шифрованному сводится к задаче извлечения корня степени e из числа y по модулю n , либо к задаче разложения числа n на простые множители. @ **RSA trapdoor one-way function** односторонняя функция RSA с потайным ходом. @ **RSA-encrypted message** сообщение, зашифрованное по алгоритму RSA. @ **RSA-signed message** сообщение, заверенное (цифровой) подписью по алгоритму RSA.

rule [ru:l] *n.* 1. правило; 2. масштабная линейка, масштаб; 3. власть, правление; *v.* 1. управлять; 2. исключать (**out**). @ **rule-based cryptanalysis** криптоанализ на основе принятых правил. # **rule and thumb** чисто практический метод (правило). # **hard and fast rule** жесткое правило.

rule D = deciphering rule

rule of cipherment = enciphering rule

rule E = enciphering rule

run [rʌn] *n.* 1. выполнение; запуск; счет, работа ЭВМ; 2. отрезок. @ В растровой графике – группа точек растра, цвет которых задается для всей группы одновременно. 3. бег, однократный проход, прогон (*напр. программы*), работа, ход, эксплуатация; 4. ход, пробег; работа; 5. опыт; *v.* (**ran, rub**) 1. бежать; 2. вращаться, работать (о машине); 3. управлять; 4. гласить; 5. проводить (*опыт, испытание*). @ **"run"** "полоска" (набор одинаковых, подряд идущих компонентов битовой последовательности, которому предшествует и за которым следует компонент отличный от повторяющегося в наборе компонента). @ **"runs" test** "полосковый" тест (используется для проверки случайности двоичной последовательности). @ **run about one thousandth as fast as DES** работать примерно в тысячу раз медленнее, чем DES-алгоритм. # **blank run** холостой ход. # **in the long run** в конце концов. # **in the short run** вскоре, в ближайшем будущем. # **to run counter** идти против, противоречивость. # **to run low** иссякать, истощаться. # **to run short** иссякать, истощаться.

running [ˈrʌnɪŋ] *adv.* подряд; *adj.* переменный, пробегающий ряд значений; выполняемый, активный. @ Выполняемый в данное время, обычно в центральном процессоре. *n.* прогон. @ **running check** текущий контроль. @ **running key cipher** 1. шифр с динамическим (бегущим) ключом; 2. шифр с одинаковой длиной ключа и сообщения. @ **running key generator (RKG)** генератор ключевого потока (ключевой последовательности). @ **running key** ключевой поток; динамический (бегущий) ключ; ключевая последовательность. @ **running speed** 1. быстродействие; 2. рабочая скорость. @ **running task** текущая задача.

Russian [ˈrʌʃən] *adj.* российский. @ **Russian encryption algorithm** "российский алгоритм шифрования" (ГОСТ 28147-89). @ Итеративный 32-цикловой обратимый блочный шифр Фейстеля. Размер входного блока – 64 бита. Размер ключа шифра – 256 бит.

S*

sacrifice ['sækrɪfaɪs] *n.* жертва; потеря; *v.* жертвовать.# **sacrifice of accuracy** потеря в точности.# **sacrificing** за счет.# **without sacrificing** не за счет.# **to make a sacrifice of** жертвовать чем-л.

safe [seɪf] *adj.* 1. безопасный; допустимый; 2. надежный.@ **safe cryptoalgorithm** безопасный криптоалгоритм (затраты на вскрытие этого криптоалгоритма значительно превышают ценность шифруемых с его помощью данных).# **it is safe to say** можно с уверенностью сказать.# **it may safely be said** можно с уверенностью сказать.# **to be on the safe side** на всякий случай, для большей верности.

safeguard ['seɪfɡɑ:d] *v.* защищать.@ **safeguard communications** защищать каналы связи.

safety ['seɪftɪ] *n.* безопасность; сохранность.# **with safety** безопасно, без риска.# **to play for safety** избегать риска, соблюдать осторожность.

sake [seɪk] *n.* употребляется в выражениях.# **for the sake** ради, для.# **for one's sake** ради кого-л.

same [seɪm] *adj.* тот же самый; одинаковый; один и тот же.# **the same as** так же, как.# **the same that** тождественный.# **all the same** все равно; тем не менее; все-таки.# **just the same** точно такой же; все равно.# **much (about) the same** почти такой же.# **this same** этот же.

sample ['sɑ:mpl] *n.* 1. выборка.@ Совокупность элементов из некоторого множества, выбранная для его статистического исследования. 2. замер; 3. пример, образец; 4. шаблон, модель; *v.* 1. замерять; производить выборку; 2. опрашивать; *adj.* 1. пробный; 2. выборочный.@ **sample estimation** оценка по выборке, выборочная оценка.@ **sample key** пробный ключ (предназначен для целей наладки криптографического оборудования).@ **sample mean** выборочное среднее.@ **sample program** 1. типовая программа; 2. пример программы.@ **sample space** выборочное пространство, пространство выборок.@ **sample unit** элемент выборки.@ **sample-and-hold (S/H)** дискретизация с запоминанием отсчетов.

sample input mode ['sɑ:mpl 'ɪnpʊt moʊd] способ организации взаимодействия с вводным устройством.@ В машинной графике – способ организации взаимодействия с вводным устройством, при котором программе доступно последнее выданное устройством значение.

sampled ['sɑ:mpld] *adj.* дискретный.@ **sampled data** дискретные (цифровые) данные.@ **sampled data system** система дискретных данных.@ **sampled information** выборочная (квантовая) информация.

sampling ['sɑ:mplɪŋ] *n.* 1. дискретизация.@ Измерение значения непрерывной величины через определенные (дискретные) промежутки времени. 2. опрос; 3. выборка, взятие образцов.@ **sampling distribution** выборочное распределение.@ **sampling frequency** частота стробирования.@ **sampling moment** выборочный момент.@ **sampling ratio** выборочное отношение, выборочная

доля. @ **sampling theorem** теорема о дискретном преобразовании (теорема Маркова). @ **sampling with replacement** выбор с возвращением.

satellite ['sætəlaɪt] *n.* спутник. @ **satellite interception system** система спутникового перехвата. @ **satellite personal communications system (SPCS)** система персональной спутниковой связи. @ **satellite scrambler** скремблер для спутниковой связи.

save [seɪv] *v.* 1. сохранять, записывать; 2. спасать; 3. экономить; *prp.* кроме; за исключением того, что. # **save and except** за исключением, не считая. # **save for** за исключением, не считая.

say [seɪ] *v.* (**said**) говорить, сказать. # (**let us**) **say** скажем; например. # **it goes without saying** само собой разумеется. # **it is safe to say** можно с уверенностью сказать. # **that is to say** то есть, другими словами. # **which is to say** то есть, другими словами. # **this is not to say** это не означает. # **to say nothing of** не говоря уже о. # **to say the least of it** без преувеличения.

scalable ['skeɪləbl] *adj.* масштабируемый. @ **scalable cipher** масштабируемый шифр (позволяет изменять свои параметры -длину ключа, размер блока и т.д.).

scalar ['skeɪlə] *n.* скаляр; *adj.* скалярный. @ **scalar function** скалярная функция. @ **scalar product** скалярное произведение.

scalar type ['skeɪlə taɪp] скалярный тип. @ Тип данных, значения которого не имеют компонент.

scalar variable ['skeɪlə 'vɛəriəbl] 1. простая переменная, скалярная переменная. @ Переменная скалярного типа. 2. скалярная переменная (*в математике*).

scale [skeɪl] *n.* 1. масштаб; 2. шкала; 3. весы; *v.* масштабировать. @ **scale factor** масштабный коэффициент; коэффициент масштабирования. @ **scale factor method** метод масштабных коэффициентов (множителей). @ **scale of notation** 1. система счисления; 2. система обозначений. # **on a large scale** в большом масштабе. # **to scale down** сводить к определенному масштабу; определять масштаб.

scheme [ski:m] *n.* схема, система.

scientific [saɪən'tɪfɪk] *adj.* научный. @ **scientific secret-key cryptology** научная криптология с секретным ключом.

score [skɔ:] *n.* 1. счет; 2. *pl.* множество; 3. два десятка. # **on the score (of)** вследствие. # **on this score** на том основании.

scramble ['skræmbəl] *v.* 1. шифровать; засекречивать; 2. скремблировать. @ Шифровать путем перестановки и инвертирования участков спектра сигнала или групп сигналов (засекречивать речевое сообщение).

scrambled ['skræmbld] *n.* зашифрованный, скремблированный. @ **scrambled message** сообщение, защищенное с помощью скремблирования.

scrambler (SCR) ['skræmblə] *n.* скремблер (устройство засекречивания речевых сообщений).

scrambling ['skræmblɪŋ] *n.* скремблирование (преобразование речевых данных по определенному закону с целью исключения подслушивания).@ **scrambling equipment** аппаратура скремблирования.@ **scrambling generator** генератор кода скремблирования.@ **scrambling key** ключ скремблирования.@ **scrambling matrix** матрица скремблирования.

scratch [skrætʃ] *adj.* рабочий.@ **scratch pad store (SPS)** временная ключевая память (используется для временного хранения ключевой информации в криптографическом оборудовании).@ **scratch file** рабочий файл.@ **scratch-pad memory (SPM)** сверхоперативная память.

scratch temporary [skrætʃ 'tempərəri] 1. рабочий, временный.@ О структуре данных, используемой только в течении выполнения некоторой операции. 2. затирать (*информацию на магнитном носителе*).

seal [si:l] *v.* 1. запечатывать; 2. закрывать, изолировать; запаивать; 3. скреплять; *n.* затвор (*жидкостной и т. п.*).

sealed [si:lt] *adj.* запечатанный.@ **sealed-authenticator authentication scheme** схема аутентификации с запечатанным аутентификатором.

sealing ['si:lɪŋ] *adj.* запечатывающий.@ **sealing encryption algorithm** запечатывающий алгоритм шифрования.

search [sə:tʃ] *n.* 1. поиск; перебор; 2. поиски; 3. исследование, изыскание; *v.* 1. искать (*иногда с out, for*); 2. исследовать.@ **search and insertion algorithm** алгоритм поиска и вставки.@ **search attribute** поисковый атрибут, атрибут поиска.@ **search cycle** цикл поиска.@ **search image** поисковый образ, образец.@ **search instruction** команда поиска.@ **search memory** ассоциативная память.@ **search register** регистр признака в ассоциативном запоминающем устройстве.@ **search time** время поиска (*напр. информации в памяти ЭВМ*).

search area [sə:tʃ 'ɛəriə] область поиска.@ Обычно подразумевается область памяти, в пределах которой производится поиск.

search domain [sə:tʃ də'mein] область поиска.@ Множество, среди элементов которого производится поиск.

search key [sə:tʃ ki:] ключ поиска.@ Имя элемента данных, значения которого рассматриваются при поиске.

search space [sə:tʃ speɪs] область поиска.@ В системах логического вывода – множество всех возможных решений.

search tree [sə:tʃ tri:] дерево поиска.@ Древоподобная структура данных, используемая для организации ключевого доступа. Внутренние вершины дерева поиска содержат ключи, указывающие, какие ключи содержатся в соответствующих под-деревах.

search word [sə:tʃ wə:d] признак.@ Значение, задаваемое при выборке слова из ассоциативной памяти.

searched [sə:tʃt] *adj.* искомый.@ **searched key** искомый ключ (при криптоанализе).

searching ['sə:tʃɪŋ] *n.* поиск.@ Процесс поиска информации в таблице или в файле путем просмотра специального поля в каждой записи, называемого

ключем. Целью поиска является отыскание записи (если она есть) с данным значением ключа.

second *adj.* = **secondary**

secondary (**sec**) ['sekəndəri] *adj.* 1. вторичный.@ 1. Вспомогательный, дополнительный; подчиненный. 2. Относящийся ко второму уровню иерархии. 2. второстепенный; побочный; 3. вторичная обмотка.@ **secondary entry point** дополнительная точка входа.@ **secondary memory (SM)** внешняя память.

secondary access method ['sekəndəri 'ækses 'meθəd] вторичный метод доступа.@ В базах данных – совокупность средств для обеспечения эффективного доступа по вторичным ключам.

secondary attribute ['sekəndəri 'ætribju:t] вторичный атрибут (*отношения реляционной базы данных*).@ Атрибут, не входящий ни в один ключ отношения.

secondary index ['sekəndəri 'indeks] 1. вторичный индекс.@ Индекс, содержащий вторичные ключи. 2. детальный индекс, вторичный индекс.

secondary key ['sekəndəri ki:] вторичный ключ (доступ к которому открывает другой ключ).@ 1. В базах данных – ключ, не являющийся первичным ключом. 2. В методах доступа – поле записи, различающее записи с одинаковыми первичными ключами.

secondary storage ['sekəndəri 'stɔ:rɪdʒ] внешняя память.@ Как правило, подразумевается внешнее запоминающее устройства в иерархической памяти или в системе с виртуальной памятью, к которым не происходит явных обращений из прикладных программ.

secondary word ['sekəndəri wə:d] вторичная команда.@ Невстроенная операция; аналог имени подпрограммы в других языках.

secrecy ['si:krisi] *n.* секретность.@ **secrecy channel** канал обеспечения секретности.

secret ['si:krit] *adj.* секретный, тайный.@ **secret exponent** секретный показатель степени.@ **secret key distribution** 1. секретное распределение ключей; 2. распределение секретных ключей.@ **secret key** секретный ключ.@ **secret writing** тайнопись.@ **secret-key agreement** соглашение (договоренность) о секретном ключе (между участниками обмена сообщениями).@ **secret-key cipher** шифр с секретным ключом.@ **secret-key cryptography** криптография с секретным ключом (одноключевая криптография).@ **secret-key cryptosystem** криптосистема с секретным ключом (одноключевая криптосистема).

secure [si'kjuə] *v.* 1. обеспечивать; 2. доставлять, получать, достигать; *adj.* прочный, надежный.@ **secure access unit (SAU)** устройство защиты от несакционированного доступа.@ **secure against substitution and modification** защищать от подмены и модификации.@ **secure against** обеспечивающий защиту от (защищенный от).@ **Secure And Fast Encryption Routine (SAFER)** Стойкий и быстрый алгоритм шифрования (алгоритм блочного шифрования, изобретенный американским криптологом Дж. Месси).@ **secure channel** защищенный канал.@ **secure cryptosystem** безусловно стойкая криптосистема (ее стойкость не зависит ни от вычислительной мощности, ни от времени, ко-

торыми может располагать противник).@ **secure electronic exchange of keys (SEEK)** секретный электронный (безопасный) обмен ключами.@ **Secure Hash Algorithm (SHA)** Стойкий алгоритм хэширования.@ **Secure Hash Standard (SHS)** Стандарт (USA) на стойкое хэширование принят в 1993 г. В нем принята односторонняя функция хеширования без ключа, отображающая любое двоичное сообщение длины не более 2^{64} в 160 битовую строку.@ **Secure Hypertext Transfer Protocol (SHTTP)** Защищенный протокол для передачи гипертекста (криптографический протокол для передачи мультимедийных документов в компьютерной сети "Интернет").@ **secure integrity of information** обеспечивать целостность информации.@ **secure key generator** генератор стойких ключей.@ **Secure Key Management Protocol (SKMP)** Защищенный протокол управления ключами (разработанная корпорацией "Ай-Би-Эм" система депонирования ключей).@ **secure key passing channel** защищенный канал для передачи ключей.@ **secure message** защищенное (засекреченное) сообщение.@ **Secure Multipurpose Internet Mail Extensions (SMIME)** Дополнительные средства защиты электронной почты в "Интернет" (криптографический протокол для шифрования сообщений, передаваемых через компьютерную сеть "Интернет", а также для работы с цифровыми подписями).@ **Secure Sockets Layer (SSL)** Защищенный гнездовой уровень (криптографический протокол американской фирмы "Нетскейп Коммьюникейшнс", предназначенный для защиты информации при ее передаче по глобальной компьютерной сети "Интернет").@ **Secure Wide Area Network (SWAN)** Защищенная глобальная компьютерная сеть (набор аппаратных и программных средств для обеспечения конфиденциальности при работе с протоколами TCP/IP).

secure key exchange = secure exchange of keys

security [sɪ'kjʊərɪti] *n.* 1. защита (*информации от несанкционированного доступа*); 2. безопасность; надежность.@ **security attribute** атрибут секретности.@ **security auditing** проверка на стойкость.@ **security certification** аттестация защиты.@ **security classification** гриф секретности; категория защиты.@ **security estimate** оценка стойкости (криптосистемы).@ **security label** гриф секретности (пометка на документе, обозначающая степень секретности содержащейся в нем информации).@ **security of a key** стойкость ключа.@ **security period** период сохранения (информации) в секрете.@ **security period** период сохранения стойкости (криптосистемы).

security accreditation [sɪ'kjʊərɪti ə'krɪdɪteɪʃən] гарантия защиты.@ Формальное разрешение на использование для работы данной конкретной машины на месте ее установки только после обеспечения защиты от несанкционированного доступа.

security clearance [sɪ'kjʊərɪti 'kliərəns] категория допуска; уровень защиты.@ Категоризация информации, связанная с субъектом и проводимая для выполнения категории защиты той информации, к которой этому пользователю предоставлено право доступа.

security evaluation [sɪ'kjuəri'ti i'vælju'eɪʃən] оценка защиты.@ Проверка системы с целью определения степени ее соответствия установленным моделям механизма защиты.

security kernel [sɪ'kjuəri'ti 'kə:nl] ядро безопасности.@ Аттестованный процесс, который увязывает всю информацию внутри системы в соответствии с определенной моделью механизма защиты.

security label [sɪ'kjuəri'ti 'leɪbl] метка грифа.@ Указатель грифа секретности, непосредственно связанный с той информацией, к которой он относится, например, как часть протокола передачи информации.

security model [sɪ'kjuəri'ti 'mɒdl] модель механизма защиты.@ Формальное определение обеспечиваемых системой внутренних характеристик безопасности.

security policy [sɪ'kjuəri'ti 'pɒləsi] стратегия защиты.@ Формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении системы защиты от известных угроз.

security processing mode [sɪ'kjuəri'ti 'prəʊsesɪŋ moʊd] режим обеспечения безопасности.@ Описание всех категорий допусков всех пользователей в привязке ко всем категориям защиты информации, которая должна храниться и обрабатываться в системе.

security standard [sɪ'kjuəri'ti 'stændəd] стандарт обеспечения защиты.@ 1. Описание последовательности оценок, которые необходимо выполнить, чтобы считать данную характеристику безопасности подтвержденной с точки зрения аттестации секретности. 2. Множество характеристик безопасности, которые должна обеспечить система, чтобы ее можно было бы использовать в данном конкретном режиме обеспечения безопасности или же в соответствии с общей стратегией защиты.

seed [si:d] *n.* начальное заполнение; величина рассеивания (рандомизации) (данные, используемые для инициализации генератора псевдослучайной последовательности, напр., линейного регистра сдвига).@ **seed key** исходный (первичный) ключ.@ **seed number** порождающее число.

seed value = seed

seem [si:m] *v.* казаться.# **seem** + *inf.* по-видимому.# **it seems** кажется, по-видимому

select [sɪ'lekt] *v.* 1. выбирать; 2. выделять.@ В экранных редакторах и машинной графике – операция, указывающая фрагмент текста или элемент изображения, над которым выполняется следующая операция. 3. устанавливать связь (*с внешним устройством*); 4. подбирать.@ **select error** ошибка «отсутствие связи» (*с внешним устройством*).@ **select pattern** кодовая комбинация.@ **select(ion) circuit** схема выборки.

selected [sɪ'lektɪd] *adj.* 1. отображенный; 2. избранный; 3. отдельный; 4. выбранный.@ **selected key** выбранный ключ.

selection [sɪ'lekʃən] *n.* 1. выбор. @ Операция реляционной алгебры, выбирающая из отношения подмножество кортежей, удовлетворяющих заданному

условию. 2. селекция; отбор; 3. выделение; выделенный фрагмент (*текста или изображения*); выделенный текст. @ **selection check** 1. выборочная (частичная) проверка; 2. контроль выборки. @ **selection ratio** 1. допустимое число обращений; 2. отношение выборки. @ **selection system** система выборки.

selective [sɪ'lektɪv] *adj.* избирательный, селективный. @ **selective calling** (*secal, selcal*) избирательный вызов. @ **selective encryption** избирательное шифрование (отдельных отрезков открытого текста сообщения). @ **selective key distribution** избирательное распределение ключей. @ **selective listing** 1. выборочная распечатка; 2. выборочная группировка данных для печати. @ **selective packet encryption** избирательное шифрование пакетов (сообщения). @ **selective trace** условная трассировка, выборочная трассировка. @ **selectivity factor** коэффициент избирательности.

selective dump [sɪ'lektɪv dʌmp] выборочный дамп. @ Дамп, при котором распечатываются только заданные фрагменты памяти.

self [self] *n.* (*pl. selves*) сам; *pref.* в сложных и сложносоставных словах имеет значение само-. @ **self-dual key** самодвойственный (самосдвоенный) ключ (в DES-алгоритме). @ **self-dual** самодвойственный, самосдвоенный. @ **self-shrinking generator** самосверточный генератор. @ **self-shrinking key generator** самосинхронизирующий генератор ключей. @ **self-shrinking stream cipher** самосинхронизирующий поточный шифр. @ **self-shrinking** самосверточный. @ **self-synchronous** самосинхронизирующий.

self-synchronizing = **self-synchronous**

semantic [sɪ'mæntɪk] *adj.* семантический. @ **semantic security** семантическая стойкость. @ **semantic method** семантический метод. @ **semantic paradox** семантический парадокс. @ **semantic technique** семантический метод анализа текста. @ **semantic unit** семантическая единица.

semantic error [sɪ'mæntɪk 'erə] семантическая ошибка. @ Ошибка в программе, не нарушающая правила синтаксиса языка программирования.

semantic grammar [sɪ'mæntɪk 'græmə] семантическая грамматика. @ Описание синтаксиса естественного языка, основывающееся на семантических признаках слов.

semantic network [sɪ'mæntɪk 'netwɜ:k] семантическая сеть. @ В искусственном интеллекте – способ представления знаний или смысла текста в виде ориентированного графа, в котором вершины соответствуют понятиям, объектам, действиям или сложным отношениям, а дуги – свойствам и элементарным отношениям.

semantics [sɪ'mæntɪks] *n.* 1. семантика. @ 1. Изучение связи знака и значения, т. е. раздел семиотики, изучающий отношения между знаками и тем, что они обозначают. 2. Часть определения языка программирования, приписывающая смысл его конструкциям. 2. семантика, смысл (*конструкции языка программирования*).

semi- [semi-] *pref.* в сложных и сложносоставных словах имеет значение полу-. @ **semi-infinite** полубесконечный. @ **semi-infinite sequence** полубесконечная последовательность (генерируется конечная случайная последователь-

ность длины n и затем повторяется нужное число раз для получения периодической последовательности с периодом n).

semiweak [ˌsemiˈwi:k] *adj.* полустойкий, полувыврожденный. @ **semiweak key** полустойкий (полувыврожденный) ключ.

send [send] *v.* посылать, передавать (сообщение). @ **send a message over a link** посылать сообщение по каналу (связи). @ **send a message under an existing protocol** посылать сообщение в соответствии с существующим протоколом.

sender [ˈsendə] *n.* отправитель (сообщения).

sense [sens] *n.* 1. чувство, ощущение; 2. смысл, значение; 3. направление; 4. *pl.* сознание, разум; *v.* 1. ощущать, воспринимать; считывать (*информацию*). # **in a sense** в некотором смысле. # **in the sense of** в смысле; в том смысле, что. # **to make sense** иметь смысл.

sensitive [ˈsensitiv] *adj.* 1. секретный, конфиденциальный (об информации); 2. уязвимый.

sensitivity [ˈsensitiviti] *n.* 1. чувствительность; 2. секретность, конфиденциальность; 3. уязвимость. @ **sensitivity analysis** [ˈsensitiviti əˈnæləsɪz] анализ чувствительности. @ Исследование влияния на поведение системы изменения значения некоторого (явного или неявного) параметра или переменной или же сочетания нескольких таких изменений.

separation [ˈsepəreɪʃən] *n.* 1. разделение; 2. перегородка; 3. интервал. @ **separation axiom** аксиома отделимости. @ **separation of capacities for encryption and decryption in public-key crypto-systems** разделение возможностей (пользователей) по зашифрованию и расшифрованию в криптосистемах с открытым ключом (многие могут зашифровать сообщение, которое в состоянии расшифровать только один человек, или наоборот, один человек может зашифровать сообщение, которое в состоянии прочесть многие).

separative control [ˈsepəreitiv kənˈtrɒl] раздельное управление.

separator [ˈsepəreɪtə] *n.* разделитель. @ 1. Символ, разделяющий лексемы или предложения языка программирования (например, пробел, точка с запятой, знак операции). 2. Управляющий символ, разделяющий порции данных при передаче. @ **separator symbol** символ разделения, разделительный символ.

sequel [ˈsi:kwəl] *n.* продолжение. # **in the sequel** в дальнейшем.

sequence [ˈsi:kwəns] *n.* 1. последовательность; 2. порядок следования; 3. натуральный ряд чисел; 4. маршрут в графе; 5. последствие, следствие, результат. @ **sequence generation** генерация (порождение) последовательности. # **sequence of events** ход событий. # **in sequence** один за другим.

sequencer [ˈsi:kwənsə] *n.* генератор последовательностей.

serial [ˈsiəriəl] *adj.* последовательный. @ Как правило, подразумевает временную или физическую упорядоченность и относится к устройствам. @ **serial access memory** последовательная память. @ **serial accumulator** накапливающий сумматор последовательного действия, последовательный накапливающий сумматор. @ **serial adder** последовательный сумматор. @ **serial binary multiplication** последовательное двоичное умножение. @ **serial by bit** пораз-

рядный. @ **serial by byte** посимвольный, побайтовый. @ **serial by character** посимвольный, побайтовый. @ **serial by word** пословный. @ **serial data controller (SDC)** последовательный контроллер данных. @ **serial event timer and recorder (SETAR)** устройство хронирования и записи последовательных событий. @ **serial in serial out (SISO)** последовательный ввод и последовательный вывод. @ **serial number** 1. порядковый номер; 2. серийный номер. @ **serial operation** последовательная операция. @ **serial printer** посимвольное печатающее устройство. @ **serial programming** последовательное программирование. @ **serial shift arrangement (SSA)** устройство последовательного сдвига. @ **serial test** последовательный тест (служит для проверки случайности двоичной последовательности путем сравнения вероятностей совпадения и различия ее двух подряд идущих элементов). @ **serial transfer** последовательная пересылка (*данных*); последовательная передача (*данных*).

serial access ['siəriəl 'ækses] последовательный доступ. @ Способ доступа, при котором данные считываются в оперативную память в порядке физического размещения на носителе внешнего запоминающего устройства.

serial arithmetics ['siəriəl ə'riθmətiks] последовательная арифметика. @ Способ вычислений, при котором в каждый момент времени обрабатывается только один двоичный разряд или одна цифра числа.

serial interface ['siəriəl ,intə'feis] последовательный интерфейс. @ Средства подключения и передачи данных по последовательному каналу.

serial process ['siəriəl 'prouses] последовательный процесс. @ Процесс, этапы которого выполняются последовательно: в каждый конкретный момент времени выполняется только один этап, и каждый последующий этап начинает выполняться только после завершения предыдущего.

serial processing ['siəriəl 'prousesɪŋ] последовательная обработка. @ Обработка данных в порядке их физического расположения или поступления.

serial search ['siəriəl sə:tʃ] последовательный поиск. @ Поиск, при котором элементы области поиска анализируются по одному, но не обязательно в соответствии с их естественной упорядоченностью.

service ['sə:vɪs] *n.* 1. служба; 2. обслуживание; *v.* обслуживать. @ **service Enigma** военная "Энигма" (одна из модификации шифровальной машины "Энигма", которые использовались в вооруженных силах Германии во время второй мировой войны). @ **service engineering** техническое обслуживание. @ **service routine** сервисная программа; служебная программа. # **to be of service** быть полезным.

service bit ['sə:vɪs bɪt] служебный разряд; служебный бит. @ Бит в пакете протокола, указывающий, несет ли пакет информацию или управляющие сигналы.

servicing time ['sə:vɪsɪŋ taɪm] время обслуживания.

session ['seʃən] *n.* сеанс. @ Цикл работы пользователя с диалоговой системой от входа в систему (вызова системы) до выхода из системы. @ **session cryptography** криптография со сменой сеансового ключа. @ **session key (SK,**

s-key) сеансовый ключ (действующий только в течение ограниченного промежутка времени, напр, в одном сеансе передачи сообщений).

session (layer) protocol ['seʃən ('leiə) 'proutəkəl] сеансовый протокол, протокол сеансового уровня.@ Уровень протокола сети передачи данных, регламентирующий взаимодействие между определенными типами задач, выполняющихся на узлах сети.

session layer ['seʃən 'leiə] сеансовый уровень.@ Уровень взаимодействия в сети передачи данных, поддерживающий взаимодействие между задачами, выполняющимися на узлах сети.@ **session layer of network protocol** сеансовый уровень функций сетевого протокола.

set [set] *n.* 1. набор.@ В сетевых базах данных – структура данных, используемая для представления связи типа «один-ко-многим». Набор состоит из одной записи – владельца набора и произвольного числа записей – членов набора. 2. множество.@ Неупорядоченная совокупность различных объектов или структура данных, используемая для представления множества. 3. набор; комплект; *v.* 1. устанавливать, присваивать разряду значение 1; 2. помещать, ставить; 3. учреждать (**up**); 4. не учитывать (**aside**); 5. излагать (**forth**); 6. выставлять (**forth, out**); 7. выдвигать (**forth, forward**); 8. отправляться (**forth, forward**); 9. приступать (**to**).@ **set algebra** алгебра множеств.@ **set key** команда "ввести ключ".@ **set of keys** комплект ключей@ **set theory** теория множеств.@ **set of keys** комплект ключей.@ **set up** сделать начальные установки.@ **set up a cipher machine** сделать начальные установки в шифровальной машине.@ **set value** заданное значение, заданная величина, установленное значение, установленная величина.@ **set-key operation** операция установки (правила) ключа.

set difference [set 'dɪfrəns] разность множеств, дополнение.@ Множество, являющееся разностью множеств А и В, состоит из элементов принадлежащих А и не принадлежащих В.

set type [set taɪp] 1. тип набора.@ В сетевых базах данных – описание набора, задающее тип владельца набора, тип или типы членов набора, процедуры базы данных, связанных с набором, и другие его атрибуты. 2. множество, тип множества.@ Составной тип данных, значения которого представляют множества элементов некоторого типа.

settings ['setɪŋs] *n.* установки (параметры шифрсистемы, определяющие состояние, в котором она находится).@ **settings of a cipher system** установки шифрсистемы.

shadow ['ʃædou] *n.* тень.# **beyond all shadow of doubt** нет ни малейшего сомнения.# **there is a shadow of doubt** нет ни малейшего сомнения.

Shamir's three-pass protocol трехэтапный протокол Шампра (криптографический протокол, не требующий предварительного распределение! ключей перед обменом сообщениями).

Shannon's bound for perfect secrecy граница Шеннона для совершенно стойких систем.

Shannon's five criteria пять критериев Шеннона (критерии оценки шифросистем, предложенные Шенноном в 1940 г.).

Shannon's theory approach подход на основе теории Шеннона.

share [ʃeə] *v.* 1. совместно использовать; 2. разделять; 3. участвовать; *n.* 1. доля; 2. участие; совместное владение. @ **share a key** пользоваться ключом совместно. @ **share keys with a key distribution center** получать ключи из центра распределения ключей.

shareable [ˈʃeəeɪbl] *adj.* общий. @ Допускающий совместное использование. @ **shareable resource** общий ресурс, разделяемый ресурс.

shareable area [ˈʃeəeɪbl ˈeəriə] общая область. @ 1. Область памяти, к которой могут иметь доступ несколько задач одновременно. 2. Область памяти, динамически распределенная между задачами.

shareable data [ˈʃeəeɪbl ˈdeɪtə] общие данные, разделяемые данные. @ Данные, которые могут обрабатываться несколькими процессами одновременно.

shareable data base [ˈʃeəeɪbl ˈdeɪtə beɪs] 1. общая база данных. @ База данных, с которой могут работать несколько прикладных программ или пользователей одновременно. 2. база данных коллективного пользования.

shareable file [ˈʃeəeɪbl faɪl] файл совместного доступа, общий файл. @ Файл, который может быть использован (открыт) несколькими задачами одновременно.

shareable image file [ˈʃeəeɪbl ˈɪmɪdʒ faɪl] многопользовательский загрузочный модуль. @ Файл, содержащий загрузочный модуль задачи, один экземпляр которого может использоваться несколькими процессами.

shared [ʃeəd] *adj.* общий. @ Совместно используемый в данный момент. @ **shared key** ключ, находящийся в совместном владении нескольких лиц.

shared file [ʃeəd faɪl] общий файл. @ Файл, открытый и обрабатываемый несколькими задачами одновременно.

shared logic system [ʃeəd ˈlɒdʒɪk ˈsɪstɪm] система с совместно используемой логикой. @ Термин, иногда используемый для описания системы, в которой несколько терминалов одновременно совместно используют один и тот же центральный процессор.

shared memory [ʃeəd ˈmeməri] совместно используемая память. @ Область памяти, используемая разными процессами.

shared common key = shared key

shielded [ˈʃiːldɪd] *adj.* экранированный, экранирующий. @ **shielded enclosure** экранированным (экранирующий) корпус (кожух). @ **shielded room** экранированная комната (помещение, защищенное от электромагнитных излучений).

shift *n.* сдвиг; *v.* сдвигать. @ **shift a register one position to the left** сдвигать содержимое регистра на одну позицию влево. @ **shift register cascade** каскад регистров сдвига (множество регистров сдвига, соединенных между собой таким образом, что работа одного отдельно взятого регистра зависит от функционирования предыдущего регистра каскада). @ **shift register with linear**

feedback регистр сдвига с линейной обратной связью. @ **shift register with non-linear feedback** регистр сдвига с нелинейной обратной связью. @ **shift register** регистр сдвига. @ **shift transformation** сдвиговое преобразование.

shift register with non-linear logic = **shift register with non-linear feedback**

shift-by-thirteen cipher = **rot 13**

shift-by-three cipher = **Caesar cipher**

short [ʃɔ:t] *v.* закорачивать; *adj.* 1. короткий; 2. недостаточный. # **short of** почти до; за исключением. @ **short key** короткий ключ. @ **short shift register** короткий регистр сдвига. @ **short signal cipher** краткий сигнальный шифр (во время второй мировой войны применялся для засекречивания эфирных позывных немецких военных кораблей и подводных лодок). @ **short weather cipher** краткий погодный шифр (во время второй мировой войны применялся немецкими военными кораблями и подводными лодками для засекречивания прогнозов и сводок погоды). @ **short-cut cryptanalysis** упрощенный криптоанализ. @ **short-cut short-term** упрощенный. @ **short-term** краткосрочный. @ **short-term key** краткосрочный ключ. # **short-term** кратковременный; краткосрочный. # **in short** короче говоря. # **in the short run** вскоре, в ближайшем будущем. # **to be short of** ощущать недостаток в чем-л.

short signal codebook = **short signal cipher**

short weather codebook = **short weather cipher**

shorthand [ʃɔ:t'hænd] *n.* стенография. # **shorthand notation** сокращенное обозначение.

shortly [ʃɔ:tlɪ] *adv.* 1. вскоре; 2. коротко, сжато. # **shortly after** вскоре после. # **shortly before** незадолго до.

shrinking [ˈʃrɪŋkɪŋ] *adj.* сверточный. @ **shrinking generator** сверточный генератор.

shuffle [ˈʃʌfl] *n.* тасование (разновидность перестановки).

side [saɪd] *n.* сторона; *adj.* боковой; побочный. @ **side-channel attack** атака через побочный канал (вместо криптоалгоритма анализу подвергается его аппаратная или программная реализация — каким образом изменяется энергопотребление шифратора в различных режимах его работы, как он функционирует, если температура окружающей среды значительно превышает установленную норму, сколько времени занимает выполнение той или иной криптооперации и т.д.) # **side by side with** рядом, бок о бок, наряду с. # **on the theoretical side** с теоретической точки зрения. # **sideliness of science** смежные области науки.

side-channel cryptanalysis = **side-channel attack**

sight [saɪt] *n.* 1. зрение; 2. поле зрения; 3. вид. # **at first sight** с первого взгляда. # **to lose sight of** потерять из виду; упустить из виду.

signals intelligence (SIGINT) ['sɪgnəls ɪn'telɪdʒəns] служба радиоэлектронной разведки, радиотехническая разведка. @ **SIGINT performance** эффективность радиоэлектронной разведки. @ **SIGINT satellite** спутник радиоэлектронной разведки. @ **SIGINT service** служба радиоэлектронной разведки. @ **SIGINT summary (SIGSUM)** суммарная сводка радиоэлектронной разведки.

sigmage ['sɪgmɪdʒ] *n.* определение величины стандартного отклонения (уклонения).

sign [saɪn] *n.* подписывать, заверять. @ **sign a digital message** подписать цифровое сообщение.

signal ['sɪɡnəl] *n.* сигнал. @ **signal related information (SRI)** информация о сигнале. @ **signals analyst** специалист в области радиотехнической разведки.

signature (SIG) ['sɪɡnətʃə] *n.* сигнатура, подпись. @ **signature authentication key** ключ аутентификации (цифровой) подписи. @ **signature block** блок подписи (присоединяемый к сообщению). @ **signature channel** канал обмена сообщениями с подписью. @ **signature generation key** ключ генерации (цифровой) подписи. @ **signature key** ключ (цифровой) подписи.

significance [sɪɡ'nɪfɪkəns] *n.* 1. значение, важность; 2. значение, смысл. @ **significance level of a test** уровень значимости теста.

significance set [sɪɡ'nɪfɪkəns set] проверка по критерию значимости. @ Статистическая процедура, посредством которой числовая характеристика, определенная по данным выборки, сравнивается с теоретическими значениями стандартных распределений вероятностей.

significant [sɪɡ'nɪfɪkənt] *adj.* 1. многозначительный, выразительный; 2. существенный, значительный, важный; знаменательный; 3. значимый. @ **significant digit** значащий разряд, значащая цифра.

significant event [sɪɡ'nɪfɪkənt 'i:vent] существенное событие. @ Событие, реакция на которое предусмотрена операционной системой.

simple ['sɪmpl] *adj.* простой, несложный. @ **simple algebra** простая алгебра. @ **simple columnar transposition** шифр простой колонной перестановки. @ **simple equation** линейное уравнение. @ **simple harmonic motion** гармоническое колебание. @ **simple key for IP** простой ключ для IP-протокола (упрощенная система управления ключами при работе с IP-протоколом, созданная корпорацией "Сип Майкросистемс"). @ **simple parity check code** код с простым контролем по четности. @ **simple substitution** простая замена.

simple name ['sɪmpl neɪm] простое имя. @ Последняя часть составного имени.

Simple Public-Key Mechanism (SPKM) простой механизм с открытым ключом @ в криптологии – сетевой протокол, обладающий инфраструктурой с открытым, а не симметричным ключом. Протокол применяется для аутентификации, формирования ключей, сохранения целостности и конфиденциальности данных.

simple statement ['sɪmpl 'steɪtmənt] простой оператор. @ Оператор, в состав которого не входят другие операторы. В большинстве языков это оператор присваивания и оператор вызова процедуры.

simple variable ['sɪmpl 'vɛəriəbl] простая переменная. @ Переменная, не имеющая компонент.

simplex (SPX, sx) ['sɪmplɛks] *n.* 1. симплексное соединение; 2. симплекс. @ 1. Физическое или логическое соединение двух точек, между которыми дан-

ные могут перемещаться в результате только в одном направлении и невозможно движение потока данных в противоположном направлении. **2.** Конечный граф, имеющий k вершин, или геометрическая фигура, в которых каждая вершина соединена с каждой другой вершиной. @ **simplex method** симплексный метод; симплекс-метод.

simplex circuit ['simpləks 'sə:kɪt] симплексный канал. @ Канал, позволяющий передавать данные только в одном направлении.

simplex codes ['simpləks kəʊdɪz] симплексные коды. @ Семейство линейных блочных блочных кодов с исправлением или обнаружением ошибок, реализуемых в виде полиномиальных кодов посредством сдвиговых регистров.

simplicity ['sɪmplɪsɪti] *n.* простота.

simplification ['sɪmplɪfəi'keɪʃən] *n.* упрощение.

simplified ['sɪmplɪfaɪd] *adj.* упрощенный; упрощенная. @ **simplified fraction** несократимая дробь. @ **simplified model** упрощенная модель.

simplify ['sɪmplɪfaɪ] *v.* упрощать.

simply connected region ['sɪmplaɪ kə'nektɪd 'ri:ʒən] односвязная область.

simulate ['sɪmjuleɪt] *v.* воспроизводить; моделировать.

simulation [sɪmju'leɪʃən] *n.* моделирование. @ **simulation technique** техника моделирования.

simulation language [sɪmju'leɪʃən 'læŋgwɪdʒ] язык моделирования. @ Язык программирования, ориентированный на задачи исследовательского моделирования.

simulator ['sɪmjuleɪtə] *n.* модель; имитатор. @ Программа или устройство, моделирующее функционирование некоторого объекта. Обычно «модель» подразумевает моделирование устройства объекта и используется для его исследования, «имитатор» относится к моделированию внешних проявлений для применения вместо моделирующего объекта.

simulator routine ['sɪmjuleɪtə ru:'ti:n] программа интерпретации. @ Программа интерпретации на одной машине программ, составленных для другой машины.

simultaneous ['sɪməl'teɪnjəs] *adj.* одновременный; совместный. @ **simultaneous access** одновременная выборка, параллельный доступ. @ **simultaneous carry** одновременный (параллельный) перенос. @ **simultaneous computer** вычислительная машина с совмещением операций. @ **simultaneous diophantine approximation** совместные диофантовы приближения. @ **simultaneous equations** система уравнений. @ **simultaneous iterative reconstruction technique (SIRT)** одновременный итерационный метод восстановления. @ **simultaneous linear equations** система линейных уравнений. @ **simultaneous multiplier** комбинационное множительное устройство.

simultaneously [sɪməl'teɪnjəsli] *adv.* одновременно.

simplified ['sɪmplɪfaɪd] *adj.* упрощенный. @ **simplified DES** упрощенный DES-алгоритм. @ **simplified fraction** несократимая дробь. @ **simplified model** упрощенная модель.

simplify ['sɪmplɪfaɪ] *v.* упрощать.

simply connected region ['sɪmplaɪ kə'nektɪd 'rɪ:ʒən] односвязанная область.

single ['sɪŋɡl] *adj.* один; единственный; единичный; отдельный; однократный, одинарный; единый; *v.* выбирать, отбирать; выделять (**out**).@ **single carry** одиночный перенос.@ **single encryption** однократное шифрование.@ **single ended pair logic circuit** спаренная логическая схема с однополюсным выходом.@ **single error correcting and double error detecting code** код с исправлением одиночных ошибок и обнаружением двойных ошибок.@ **single error correcting code** код с исправлением одиночных ошибок.@ **single length key** ключ единой установленной длины.@ **single processing element (SPE)** элемент обработки сигналов.@ **single program initiator (SPI)** инициатор одиночных программ.@ **single space** одиночный пробел (интервал) .@ **single threading** последовательная обработка вызовов.@ **single transposition** шифр одинарной перестановки.

single-['sɪŋɡl] в сложных и сложносоставных словах имеет значение одно-.@ **single-action printer** печатающее устройство одноразового действия.@ **single-address code** одноадресный код.@ **single-address instruction** одноадресная команда.@ **single-bit cipher feedback** однобитовая обратная связь по шифртексту.@ **single-bit** однобитовый.@ **single-channel** одноканальный.@ **single-chip controller (SCC)** однокристальный контроллер.@ **single-density disk (SD)** диск для записи с одинарной плотностью.@ **single-digit adder** одноразрядный сумматор.@ **single-digit** одноразрядный.@ **single-directional** однонаправленный.@ **single-directory device** устройство с одним каталогом.@ **Single-Instruction Multiple Data stream (SIMD) architecture** архитектура (параллельной) ЭВМ с одним потоком команд и несколькими потоками данных.@ **Single-Instruction Single Data (SISD) architecture** архитектура ЭВМ с одним потоком команд и одним потоком данных.@ **single-iterated** одноитерационный (с использованием единственной итерации).@ **single-key cryptography** одноключевая криптография (криптография с секретным ключом).@ **single-key network** сеть (засекреченной связи) с использованием одного ключа.@ **single-key** одноключевой.@ **single-letter frequency cryptanalysis** криптоанализ, основанный на частотах встречаемости (появления) отдельных букв (в тексте).@ **single-letter** однобуквенный.@ **single-level address** прямой адрес.@ **single-order device** одноразрядное устройство.@ **single-pass assembler** однопроходной ассемблер.@ **single-phase** однофазный.@ **single-place shift** сдвиг на один разряд.@ **single-pulse device** генератор одиночных импульсов.@ **single-sideband frequency modulation (SID)** частотная модуляция с одной боковой полосой.@ **single-step** пошаговый.@ **single-use pad encryption** шифрование при помощи одноразового шифрблокнота.@ **single-use pad** одноразовый шифрблокнот.@ **single-use** одноразовый.@ **single-valued encryption** однозначное шифрование.@ **single-valued function** однозначная функция.@ **single-valued** однозначный.@ **single-way (connection)** нулевая (схема).

single-assignment language ['sɪŋɡl,ə'saɪnmənt 'læŋɡwɪdʒ] язык с однократным присваиванием.@ Язык программирования, в котором значения динамиче-

чески присваиваются именам, но после присваивания значение имени не может быть изменено. Такие языки близки к языкам функционального программирования и связаны с потоковой архитектурой ЭВМ.

single-keystroke command одноклавишная команда.@ В интерактивных системах – команда, задаваемая нажатием одной клавиши.

single-precision ['sɪŋɡl.pri'sɪʒən] с одинарной точностью.@ О числах и переменных, представляемых одним машинным словом и об операциях над такими числами.

single-step operation ['sɪŋɡl'stɛp ,ɔpə'reɪʃən] пошаговая работа.@ Выполнение программы либо с отановкой после каждой команды, либо по одному шагу (такту) в рамках команды.

single-stepping ['sɪŋɡl'stɛpɪŋ] выполнение в пошаговом режиме.@ Способ отладки, при котором программа выполняется под управлением отладчика и останавливается после выполнения каждой машинной команды или оператора исходного языка, позволяя проконтролировать результаты и состояние памяти.

single-task system ['sɪŋɡl'ta:sk 'sɪstɪm] однозадачная система.@ Операционная система, позволяющая выполнять только одну задачу в каждый момент.

single-user ['sɪŋɡl'ju:zə] однопользовательский.@ О вычислительной или операционной системах, обслуживающих или имеющих только один терминал и обеспечивающих работу только одного пользователя.

size [saɪz] *n.* размер, длина (ключа).@ **size of a key** размер (длина) ключа (количество бит в ключе).@ **size-limited key** ограниченный по размерам (длине) ключ

skip [skɪp] *n.* прыжок, скачок.@ **skip code** "прыжковый" код (зашифрование осуществляется вставкой букв открытого текста сообщения в другой текст невинного содержания).

skipjack "Скипджек" (букв "Попрыгунчик") (название алгоритма шифрования, аппаратно реализованного в виде чипа "Клиппер").

slide [slaid] *v.* (**slid**) скользить; *n* движок.# **sliding rule** логарифмическая линейка.

small [smɔ:l] *adj.* короткий.@ **small key** короткий ключ.

smooth ['smu:ð] *v.* сглаживать; *adj.* гладкий, плавный.@ **smooth integer** "гладкое" целое число (обладает только малыми по величине простыми делителями).

sneaker ['sni:kə] *n.* взломщик средств защиты компьютерных систем.

so [sou] *adv.* 1. так; настолько; таким образом; потому; 2. и так; *adj.* такой; *ср.* следовательно, поэтому; *употребляется для замены какого-л. глагола (вместо повторения).*# **so as +inf.** с тем, чтобы (так, чтобы) + *инф.*# **so that +inf.** с тем, чтобы (так, чтобы) + *инф.*# **so far** до сих пор, пока.# **(in)so far as** посколькy.# **(in)so far as ... is concerned** что касается; поскольку речь идет о; когда дело касается.# **so long as** пока; поскольку.# **so much as** нечто, вроде; даже.# **so much for** это все, что касается.# **so much so** до такой степени; так (что).# **so much the more** тем более, что.# **(all) the more so** тем более, что.# **and so forth (on)** и так далее.# **or so** или около этого.

software ['sɒftweə] *n.* 1. программное обеспечение, программные средства. @ Программы, процедуры, правила и документация, входящие в состав вычислительной системы. Часть вычислительной системы, не являющаяся аппаратными средствами. 2. программа, программное средство; 3. программный. @ **software compatibility** программная совместимость. @ **software compatible** программно-совместимый. @ **software cracker** программа вскрытия (ключа, шифра). @ **software development environment** среда программирования. @ **software development** разработка программного обеспечения, программирование. @ **software encryption** программные средства шифрования. @ **software error** программная ошибка, ошибка в программном обеспечении. @ **software failure** программная ошибка, ошибка в (используемом) программном обеспечении. @ **software house** фирма по разработке программного обеспечения. @ **software implementation of DES** программная реализация DES-алгоритма. @ **software life-cycle** жизненный цикл программы. @ **software prototyping** 1. программное моделирование (*разрабатываемого объекта*); 2. моделирование разрабатываемых программ (*исследуемого объекта*). @ **software quality assurance (SQA)** обеспечение качества программного обеспечения. @ **software reliability** надежность программного обеспечения. @ **software simulation** программное моделирование. @ **software support** программная поддержка; программная реализация. @ **software tools** 1. вспомогательные программы; 2. инструментальные программные средства; сервисные программы. @ **software-implemented encryption algorithm** программная реализация алгоритма шифрования. @ **Software-optimized Encryption Algorithm (SEAL)** Оптимизированный для программной реализации алгоритм шифрования.

software-based encryption = software encryption

software engineering ['sɒftweə ,en'dʒɪnɪərɪŋ] разработка программного обеспечения, программирование. @ Техническая дисциплина, изучающая методы программирования и производства программного продукта.

software engineering environment ['sɒftweə ,en'dʒɪnɪərɪŋ in'vaɪərmənt] средства поддержки программирования. @ Вычислительная система, которая обеспечивает возможность разработки, корректировки и модернизации программ, а также координацию и управление этими действиями.

software environment ['sɒftweə in'vaɪərmənt] программная среда. @ Программные средства, с которыми взаимодействует программа.

software interrupt ['sɒftweə ,ɪntə'rʌpt] программное прерывание. @ Прерывание, вызванное машинной командой (обычно для передачи управления операционной или исполняющей системе).

software package ['sɒftweə 'pækɪdʒ] пакет программ. @ Совокупность программ, объединенных общим приложением.

software piracy ['sɒftweə 'paɪərəsɪ]. @ Незаконная деятельность, заключающаяся в копировании и распространении программного обеспечения без соответствующей лицензии.

software specification ['sɒftweə ,spesɪfɪ'keɪʃən] технические условия на средства программного обеспечения.@ Точное описание действий, которые должна выполнять программная часть всей вычислительной системы.

solution [sə'lu:ʃən] *n.* 1. решение (математической задачи) ; 2. вскрытие.@ **solution by analogy** вскрытие по аналогии.@ **solution by frequency matching** вскрытие методом согласования частот.@ **solution by probable word method** вскрытие методом вероятного слова.@ **solution efforts on a machine** усилия по вскрытию шифровальной машины.@ **solution of a cipher** вскрытие шифра.@ **solution space** пространство решений.@ **solution to a knapsack problem** решение задачи об укладке ранца.

solvable ['sɒlveɪbl] *adj.* разрешимый; вскрываемый.@ **solvable cipher** вскрываемый.

solve [sɒlv] *v.* 1. решать (математическую задачу); 2. вскрывать, подвергать криптоанализу (напр, шифратор).@ **solve a cipher** вскрывать шифр.@ **solve a key** вскрывать ключ.@ **solve a system of linear equations** решать систему линейных уравнений.@ **solve by cryptanalysis** вскрыть с помощью криптоанализа.@ **solve the Enigma** вскрывать "Энигму".

solved [sɒlvt] *adj.* вскрытый.@ **solved cipher** вскрытый шифр.

solving ['sɒlvɪŋ] *n.* вскрытие.

somehow ['sʌmhau] *adv.* как-то; как-нибудь.# **somehow in association** в какой-то степени.# **somehow or other** так или иначе.

something ['sʌmθɪŋ] *n.* что-то, нечто; что-нибудь.# **something like** около, приблизительно.

somewhat ['sʌmwɒt] *adv.* несколько, отчасти, до некоторой степени; довольно, сравнительно, относительно.

son file [sʌn faɪl] новая версия (основного) файла.

soon [su:n] *adv.* вскоре; скоро.# **as soon as** как только.# **no sooner ... than** как только.# **sooner or later** рано или поздно.

sort [sɔ:t] *n.* 1. сортировка.@ Упорядочивать совокупность объектов в соотношении с заданным отношением порядка. 2. вид, род, класс; сорт; 3. качество, характер; *v.* 1. сортировать; классифицировать.@ **sort cryptograms by frequency (by length)** сортировать (упорядочивать) криптограммы по частоте (длине).# **in sort** в известной мере.# **some sort of** какой-либо.# **a sort of** что-то вроде; своего рода.

source [sɔ:s] *n.* источник, отправитель (сообщения).@ **source alphabet** исходный (входной) алфавит.@ **source coding** первоначальное кодирование (уменьшение избыточности открытого текста сообщения перед его зашифрованием).@ **source cryptor** шифратор источника (отправителя) (сообщения).@ **source key** ключ источника (отправителя) (сообщения).@ **source address bus (SAB)** шина адреса источника.@ **source coding theorem** теорема о кодировании источника.@ **source computer** инструментальная ЭВМ.@ **source editor** редактор текстов программ.@ **source field** исходное поле, исходный элемент данных.@ **source file** 1. исходный файл; 2. текст программы; файл, содержа-

щий текст программы. @ **source image** 1. источник изображения; 2. вводимое изображение в машину. @ **source information** первичная информация. @ **source language debugger** отладчик, работающий в терминах языка программирования. @ **source language program** 1. входная программа; 2. программа на входном языке. @ **source library** библиотека исходных модулей, библиотека текстов программ. @ **source program** исходная программа. @ **source statement** оператор исходной программы.

source-to-destination encryption = end-to-end encryption

source (compression) coding [sɔ:s (kəm'prefən) koudɪŋ] кодирование источника; сжатое кодирование. @ Использование в рамках заданного алфавита кодов переменной длины с целью уменьшения числа символов в сообщении до минимума без потери информации.

source address [sɔ:s ə'dres] 1. адрес источника данных. @ Адрес устройства, откуда поступают пересылаемые данные. 2. адрес операнда. @ Адрес ячейки памяти или области памяти, откуда извлекаются обрабатываемые данные.

source alphabet [sɔ:s 'ælfəbɪt] входной алфавит. @ Алфавит, из символов которого состоит входная последовательность.

source code [sɔ:s koud] исходный текст, исходная программа. @ Программа на языке программирования.

source data item [sɔ:s 'deɪtə 'aɪtəm] элемент данных – копия источника. @ В сетевых базах данных – производный элемент данных, значения которого является копией значения другого элемента данных.

source debugger [sɔ:s dɪ'blʌgə] отладчик, работающий в терминах языка программирования. @ Отладчик, позволяющий анализировать и отлаживать программу в терминах языка, на котором она написана: просматривать исходный текст, задавать трассировку и точки останова в указанных операторах, просматривать переменные программы в формате, соответствующем их типам.

source language [sɔ:s 'læŋgwɪʒ] 1. исходный язык. @ Язык, с которого производится трансляция. 2. входной язык. @ Язык, на котором записывается входная программа для компилятора или транслятора.

source listing [sɔ:s 'lɪstɪŋ] распечатка программы. @ Выдаваемая транслятором распечатка исходного текста программы.

Soviet ['souviət] *adj.* советский. @ **Soviet encryption algorithm** "советский алгоритм шифрования" (ГОСТ 28147-89 – итеративный 32-цикловый обратимый блочный шифр Фейстеля. Размер входного блока – 64 бита. Размер ключа k шифра – 256 бит.).

space [speɪs] *n.* 1. пространство, место; 2. пробел; 3. интервал, промежуток; 4. пространство. @ Множество, на котором определено некоторое отношение; *v.* располагать с интервалами, оставлять промежутки, расставлять с промежутками, оставлять пробел; *adj.* космический. @ **space complexity** пространственная сложность. @ **space list** 1. список свободного листа; 2. список свободных ячеек в памяти. @ **space quantization** квантование пространства. @

space vector 1. обобщенный вектор; 2. пространственный вектор. # **outer space** космос. # **space technology** космонавтика.

space character (SP) [speɪs 'kærɪktə] пробел. @ Текстовый символ, отображаемый пустой позицией при выводе на экран или печать. В коде ASCII представляется числом 32.

space division switch [speɪs dɪ'vɪʒən swɪtʃ] пространственный коммутатор. @ Механизм переключения, основанный на перекрестном выборочном соединении множества входных линий со множеством выходных линий.

space domain [speɪs də'meɪn] пространственная область сигнала. @ Термин, используемый для обозначения развертки амплитуды сигнала в пространстве, а не во времени.

space suppression [speɪs sə'preʃən] удаление пробелов. @ Удаление ненужных пробелов (например, в конце строки) при хранении или передачи данных.

spare [speə] *adj.* запасной. @ **spare key** запасной ключ.

special ['speʃəl] *adj.* специальный; специализированный. @ **Special Collection Element** Специальное подразделение по сбору информации (станция перехвата NSA USA расположенная в американском посольстве или консульстве). @ **Special Collection Service (SCS)** Специальная служба сбора информации (занимается разработкой и изготовлением оборудования для тайных технических операций по сбору информации для NSA и CIA USA, а также готовит квалифицированный перечень: для обслуживания этого оборудования). @ **Special Committee on Compromising Emanation (SCORE)** Специальный комитет (NSA USA) по компрометирующему излучению. @ **Special Compartmented Information** Специально скомпонованная информация (обозначение, применяемое в NSA USA для особо секретных разведывательных данных, которые, как правило, добываются путем перехвата и дешифрования сообщений). @ **special purpose machine** специализированная вычислительная машина. @ **Special Signals Division (SSD)** Специальное британское военное радио-разведывательное подразделение. @ **special signature scheme** специальная схема цифровой подписи.

Special Section = Spets-Otdel

specific [spi'sɪfɪk] *adj.* специальный. @ **specific key** специальный ключ (выбранный из некоторого множества ключей для конкретного применения).

speculation [spekju'leɪʃən] *n.* 1. размышление; 2. предположение, гипотеза, теория. # **to be open to speculation** вызывать сомнения; быть спорным, быть сомнительным.

speech *n.* речь. @ **speech encryption** шифрование речи. @ **speech scrambler device** речевой скремблер. @ **speech security device** прибор засекречивания речи.

speed [spi:d] *n.* 1. скорость, быстродействие; 2. передача; 3. быстродействие; 3. быстрота; *v.* ускорять; *adj.* скоростной, быстродействующий. @ **speed up** ускорять. @ **speed up an attack** ускорять атаку.

spiral ['spaɪəɹəl] *adj.* спиральный, винтовой, винтообразный. @ **spiral cipher clock** спиральный шифровальный циферблат (графическое представление шифра многоалфавитной замены в виде спирали, во внутренней стороны которой выписываются буквы алфавита открытого текста, а с внешней – алфавитов шифрованного).

spite [spaɪt] *n.* употребляется в выражении. # **in spite of** несмотря на.

split [splɪt] *adj.* разделенный; *v.* делить на части. @ **split a key** делить ключ на части (ключ делится на составные части, которые распределяются между несколькими лицами так, что ключ может быть восстановлен в полном объеме только в том случае, если каждый из них предоставит для этого свою часть ключа). @ **split key cryptosystem** система с разделенным ключом. @ **split key** разделенный (на несколько частей) ключ. @ **split-key entry** ввод ключа по частям. @ **split-key technique** метод распределения (секретного) ключа по частям между отдельными лицами.

splitting ['splɪtɪŋ] *adj.* ветвящийся; *n.* ветвление. @ **splitting does not occur in any encoding rule** ветвления не происходит ни в одном правиле кодирования. @ **splitting strategy** ветвящаяся стратегия.

spread [spred] *v.* (**spread**) распространять(ся), простираться; *n.* 1. распространение; 2. разброс. @ **spread of cryptography** распространение криптографии.

spy [sprai] *v.* следить, шпионить. @ **spy on a communication channel** следить за тем, что передается по каналу связи.

square [skwɛə] *n.* 1. квадрат (матрица размера $n \times n$, элементами которой являются символы n -буквенного алфавита); 2. площадь; 3. прямоугольник; *adj.* прямоугольный, квадратный; *v.* возводить в квадрат. @ **square-and-multiply trick** метод возведения в произвольную степень путем многократного возведения в квадрат и умножения. # **root mean square (r.m.s)** среднеквадратичное (значение).

stage [steɪdʒ] *n.* 1. стадия, фаза; 2. разряд; каскад; 3. ячейка, ступень; 4. сцена. @ **stage shift register** разрядный регистр сдвига. # **setting stage** начальная стадия, начальный этап.

stake [steɪk] *n.* ставка. # **to be at stake** быть поставленным на карту, под угрозой.

stale [steɪl] *adj.* устаревший, потерявший значение. @ **stale message** устаревшее (потерявшее значение) сообщение.

stand [stænd] *v.* (**stood**) 1. стоять; 2. выдерживать; 3. обозначать (**for**); *n.* 1. позиция, место; 2. стенд; 3. остановка; 4. сопротивление; 5. взгляд, точка зрения. # **as it stands** при создавшемся положении вещей. # **it stands on its own** это говорит само за себя. # **it stands to reason** ясно, очевидно.

stand-alone ['stændə'loun] *adj.* автономный. @ **stand-alone encryption device** автономное устройство шифрования.

standard (STD) ['stændəd] *adj.* 1. стандартный, типовой, нормальный; 2. образцовый; *n.* стандарт. @ **standard cipher alphabet** стандартный шифр алфавит. @ **standard cryptanalysis** стандартный криптоанализ. @ **standard encryp-**

tion algorithm стандартный алгоритм шифрования. @ **standard form** стандартная форма (представления данных). @ **standard function** стандартная функция. @ **standard key** стандартный ключ (напр, имеющий стандартную длину). @ **standard mode of operation** стандартный режим работы (шифратора). @ **standard product of sums** нормальная конъюнктивная форма. @ **standard product term (miniterm)** элементарная конъюнктивная форма; минитерм. @ **standard remote terminal (SRT)** стандартный удаленный терминал. @ **standard software** стандартное программное обеспечение. @ **standard sum of products** нормальная дизъюнктивная форма. @ **standard sum term (maxterm)** элементарная дизъюнктивная форма; макситерм.

standard deviation ['stændəd ,di:vɪ'eɪʃən] среднеквадратичное отклонение. @ Характеристика разброса случайной величины, равная квадратному корню из дисперсии.

standard input ['stændəd 'ɪnpʊt] стандартный ввод. @ Логический файл для ввода данных, связанный с физическим файлом или стандартным выводом другой программы при запуске; по умолчанию стандартный ввод в пакетном режиме связывается с входным потоком, а в диалоговом режиме с терминалом.

standard output ['stændəd 'aʊtpʊt] стандартный вывод. @ Логический файл для вывода данных, связанный с физическим файлом или стандартным вводом другой программы при запуске; по умолчанию стандартный вывод в пакетном режиме связывается с выходным потоком, а в диалоговом режиме с терминалом.

standard subroutine ['stændəd səb.ru:'tɪn] стандартная подпрограмма. @ 1. Библиотечная подпрограмма; 2. Предопределенная подпрограмма.

standing ['stændɪŋ] *n.* 1. положение; 2. длительность; продолжительность. # **of long standing** длительный; застарелый. # **to have no standing** не иметь веса, быть неубедительным.

start-up ['sta:tʌp] *n.* пуск, запуск. @ **start-up key encryption key** пусковой ключ шифрования ключей (распространяется среди потенциальных, абонентов сети связи).

state [steɪt] *n.* 1. состояние, положение; 2. структура, форма; 3. режим работы; 4. государство; 5. штат; *v.* 1. формулировать; 2. выражать знаками; 3. устанавливать; излагать; 2. заявлять. @ **state of a cryptosystem** состояние крипто-системы. @ **state of a shift register** состояние регистра сдвига. # **state of (the) art** уровень развития науки (техники и т. п.) на данном этапе. # **as stated above** как сказано выше. # **unless otherwise stated** если не указано особо.

static ['stætɪk] *adj.* статический. @ **static key** статический (не изменяющийся во времени) ключ.

station ['steɪʃən] *n.* 1. станция (перехвата).

station-to-station protocol = authenticated key agreement protocol

statistical ['stætɪkəl] *adj.* статистический. @ **statistical analysis** статистический анализ. @ **statistical approach** статистический подход. @ **statistical approximation** статистическая аппроксимация. @ **statistical attack** статистическая атака. @ **statistical cryptanalysis** статистический криптоанализ. @ **statistical**

data recorder (SDR) регистратор статистических данных.@ **statistical even** статистически равновероятный.@ **statistical independent keys** статистически независимые ключи.@ **statistical inference** статистический вывод.@ **statistical methods** статистические методы.@ **statistical prediction** статистическое прогнозирование.@ **statistical properties of a sequence** статистические свойства последовательности.@ **statistical quality control (SQC)** статистический контроль качества.@ **statistical test of a sequence** статистический тест последовательности.

statistical flat = statistical even

statistical multiplexing ['stætɪkəl 'mʌltɪpleksɪŋ] статистическое мультиплексирование.@ Метод временного мультиплексирования некоторого числа подканалов в один широкополосный канал, при котором общая ширина полосы пропускания, требуемая под отдельные подканалы, превышает ширину пропускания мультиплексного канала.

statistically ['stætɪkəlɪ] *adv.* статистически.

statistics ['stætɪks] *n.* статистика, статистические свойства.@ **statistics of a ciphertext** статистические свойства шифртекста.@ **statistics of a plaintext** статистические свойства открытого текста.

steckerboard *n.* = **plug-board**

steganogram [ste'nɒgræm] *n.* стеганограмма.

steganographic [stenɒ'græfɪks] *adj.* стеганографический.@ **steganographic methods** методы стеганографии.@ **steganographic program** стеганографическая (компьютерная) программа.

steganography [stenɒ'græfɪ] *n.* стеганография.

step [step] *n.* 1. шаг; 2. ступень, стадия.@ **step encryption** пошаговое шифрование.# **step by step** постепенно.# **step by step method** метод последовательных приближений.# **in step** синхронно.# **to take steps** принимать меры.

stereotype ['stiəriətaɪp] *adj.* стереотип, шаблон.

stereotyped ['stiəriətaɪpt] *adj.* стереотипный, шаблонный.@ **stereotyped command** стандартная программа.@ **stereotyped message** стереотипное (шаблонное) сообщение.

still-sensitive *adj.* по-прежнему конфиденциальный.@ **still-sensitive ciphertext** недостаточно стойкий шифртекст (требуется повторного зашифрования).

stochastic ['stə'kæstɪk] *n.* случайный.@ **stochastic approximation** вероятностная (стохастическая) аппроксимация.@ **stochastic balance** стохастическое (вероятностное) равновесие.@ **stochastic convergence** сходимости по вероятности.@ **stochastic distribution** случайное распределение.@ **stochastic disturbance** случайное (стохастическое) возмущение.@ **stochastic matrix** вероятностная (стохастическая) матрица.@ **stochastic process** случайный (стохастический) процесс.@ **stochastic variable** случайная переменная.

stone [stoun] *n.* камень; *adj.* каменный. # **corner stone** краеугольный камень.

storage medium ['stɔ:riɔz 'mi:djəm] носитель данных.

storage protection ['stɔ:riɔz prə'tekʃən] защита памяти.

storage (STOR) ['stɔ:riɔz] *n.* 1. память. @ Функциональная часть вычислительной системы, предназначенная для приема, хранения и выдачи данных. «storage» и «memory» являются синонимами, однако «storage» употребляется чаще по отношению к запоминающим устройствам, а «memory» – по отношению к способу использования памяти программой; «memory» также используется применительно к новым видам запоминающих устройств и запоминающим устройствам микроЭВМ. 2. хранение (*информации*); 3. хранение; накопление; 4. склад; 5. запоминающее устройство. @ **storage access** выборка из запоминающего устройства, обращение к запоминающему устройству. @ **storage address** адрес запоминающего устройства. @ **storage allocation** распределение памяти. @ **storage area** область памяти. @ **storage block** 1. блок запоминающего устройства; 2. блок чисел в запоминающем устройстве. @ **storage circuit** запоминающая ячейка, запоминающая схема, накопительная схема. @ **storage class** класс памяти. @ **storage cycle period** время цикла запоминающего устройства. @ **storage cycle** цикл работы запоминающего устройства. @ **storage data register (SDR)** регистр данных ЗУ. @ **storage decoder** дешифратор с памятью. @ **storage density** плотность расположения ячеек запоминающего устройства. @ **storage device** запоминающее устройство. @ **storage disk** запоминающий диск. @ **storage dump** дампы памяти. @ **storage fragmentation** фрагментация памяти. @ **storage function** функция запоминания (хранения). @ **storage hierarchy** иерархия памяти. @ **storage key** ключ памяти. @ **storage limits register** регистр границ области памяти. @ **storage location** 1. ячейка памяти; 2. адрес ячейки памяти. @ **storage logic array (SLA)** матрица запоминающих логических элементов. @ **storage map** карта (распределение) памяти. @ **storage of keys** хранение ключей. @ **storage operation** операция в памяти машины или накопителя. @ **storage pool** динамическая область памяти, динамически распределяемая область памяти. @ **storage position** адрес ячейки запоминающего устройства. @ **storage problem** задача (проблема) о хранении. @ **storage register** регистр запоминающего устройства. @ **storage selection circuit** 1. схема выборки ячейки запоминающего устройства; 2. схема выборки запоминающего устройства. @ **storage speed** быстродействие запоминающего устройства. @ **storage structure** структура представления (*данных в памяти*), структура хранения. @ **storage system** система памяти. @ **storage tube** запоминающая трубка. @ **storage unit** запоминающее устройство. @ **storage zone** зона запоминающего устройства.

storage element ['stɔ:riɔz 'elimənt] запоминающий элемент. @ Часть запоминающего устройства, хранящая наименьшую единицу данных.

storage cell ['stɔ:riɔz si:l] ячейка запоминающего устройства. @ Совокупность запоминающих элементов, реализующих ячейку памяти.

storage-to-register instruction ['stɔːrɪdʒ,tuː'redʒɪstə ɪn'strʌkʃən] команда типа «память – регистр». @ Команда, при выполнении которой данные из оперативной памяти перемещаются в регистр(ы) процессора.

storage-to-storage instruction ['stɔːrɪdʒ,tuː'stɔːrɪdʒ ɪn'strʌkʃən] команда типа «память – память». @ Команда, операнды и результат которой располагаются в оперативной памяти.

store [stɔː] *v.* 1. хранить (*информацию*); записывать в память. 2. снабжать; 3. запасать; 4. хранить; 5. помещать; вмещать; *n.* 1. память. 2. запас; 3. склад. # **to be (have, hold) in store** ожидать в будущем.

strange ['streɪndʒ] *adj.* 1. странный; необыкновенный; 2. чужой, чуждый; 3. незнакомый, неизвестный; 4. непривычный. # **strangely enough** как это ни странно.

strategic ['strætɪdʒɪk] *adj.* стратегический. @ **strategic communication interception** перехват стратегических сообщений. @ **strategic cryptography** криптография стратегического уровня.

stream [striːm] *n.* поток. @ **stream cipher** асинхронный потоковый шифр. @ **stream encryption** поточное шифрование.

strength [streŋθ] *n.* 1. сила; 2. прочность; 3. криптостойкость. @ **strength of encryption** криптостойкость шифрования. @ **strength of cryptographic algorithm** стойкость криптографического алгоритма. # **on the strength of** в силу, на основании.

strengthen ['streŋθən] *v.* повышать криптостойкость. @ **strengthen a cipher** повышать криптостойкость шифра.

strict [strikt] *adj.* строгий. @ **strict avalanche criterion (SAC)** строгий критерий лавинообразных изменений (двоичная функция удовлетворяет этому критерию, если ее выходное значение меняется на противоположное с вероятностью 1/2 при изменении ровно одного из ее входов).

strictly ['striktli] *adv.* строго. @ **strictly periodic** строго периодический.

strip [stri:p] *v.* 1. отделять; 2. снимать перешифровку. @ **strip an authenticates off one message to authenticate another** отделять аутентификатор от одного сообщения, чтобы аутентифицировать другое.

strong ['strɒŋ] *adj.* 1. сильный; 2. крепкий; 3. решительный, энергичный. @ **strong cryptoalgorithm** стойкий криптоалгоритм. @ **strong definition of security** строгое определение стойкости (криптосистема является стойкой, если любой алгоритм атаки этой криптосистемы, обладающий не пренебрежимо малой вероятностью ее успешного вскрытия, связан с неприемлемо большим объемом вычислений). @ **strong encryption** стойкое шифрование. @ **strong intersymbol dependence** сильная межсимвольная зависимость. @ **strong key** стойкий ключ. @ **strong law of large numbers** усиленный закон больших чисел. @ **strong prime** строгое простое число. @ **strong primes** стойкие простые числа (два простых числа p и q называются стойкими, если их произведение n таково, что, если p и q неизвестны, разложение n на множители является очень трудоемкой задачей). @ **strong pseudoprime to the base b** строгое псевдопростое число по основанию b . @ **strongest encryption level allowed by the USA**

government самый высокий уровень стойкости, разрешенный правительством USA.

strongly ['strɒŋli] *adv.* сильно.@ **strongly-randomized cipher** шифр с высокой степенью случайности.

structure ['strʌktʃə] *n.* 1. структура.@ Совокупность связей между частями системы. 2. устройство, строение.@ **structure of a cryptosystem** структура криптосистемы.

structured ['strʌktʃəd] *adj.* структурный.@ **structured analysis** структурный анализ.@ **structured coding** структурное программирование.

structured English ['strʌktʃəd 'ɪŋɡlɪʃ 'ɪŋɡlɪʃ] структурированный английский язык.@ Форма представления логики процесса, аналогичная псевдоязыку, используемая в структурном системном анализе.

structured programming ['strʌktʃəd 'prɒɡræmɪŋ] структурное программирование.@ Методология программирования, основанная на предположении, что логичность и понятность программы обеспечивает надежность, облегчает модификацию и ускоряет разработку; характерными чертами структурного программирования являются отказ от неструктурных передач управления, ограниченное использование глобальных переменных, модульность.

structured systems analysis ['strʌktʃəd 'sɪstɪms ə'neɪləsɪz] структурный системный анализ.@ Особая технология системного анализа, охватывающая все его этапы, начиная от первоначального представления проблемы и кончая ее спецификацией и построением верхнего уровня системы программного обеспечения.

structured variable (record) ['strʌktʃəd 'vɛəriəbl ('rekɔ:d)] переменная типа «структура».@ Переменная в языке программирования, которая является сложным информационным объектом, составленным из компонент, которые сами являются либо простыми элементами данных, либо структурированными объектами. Эти компоненты обозначаются именами.

study ['stʌdi] *n.* изучение, исследование.# **under study** изучаемый.

subject ['sʌbdʒɪkt] *adj. predic.* 1. подверженный (**to**); 2. подлежащий (**to**); *adv.* при условии; *n.* 1. тема, сюжет; 2. предмет, дисциплина; 3. подданный; 4. субъект, человек; *v.* подвергать, испытывать.@ **subject a cryptosystem to cryptanalytic attack by experts** испытывать криптосистему методом экспертного криптоанализа.# **human subjects** люди.# **subject-matter** основная тема; сущность, содержание; предмет (обсуждения и т. п.).# **subject to** в соответствии с, в зависимости от; при условии, допуская, если; подверженный, подлежащий.# **to be subject to** подвергаться, подчиняться; зависеть от; быть подверженным чему-л.

subkey ['sʌbki:] *n.* подключ (ключ более низкого иерархического уровня).

subscriber [səb'skraɪbə] *n.* абонент (сети).@ **subscriber's public-key** открытый ключ абонента.

subsequence ['sʌbsɪkwəns] *n.* подпоследовательность.

subsequent ['sʌbsɪkwənt] *adj.* последующий; являющийся результатом (upon).# **subsequent to** вслед за.

subsequently ['sʌbsɪkwəntli] *adv.* впоследствии, в дальнейшем.

subset ['sʌbset] *n.* подмножество.@ Множество А является подмножеством В тогда и только тогда, когда все элементы А принадлежат В.@ **subset sum problem** задача о сумме подмножеств (задача о рюкзаке).

subset language ['sʌbset 'læŋgwɪdʒ] подмножество языка.@ Язык программирования, односторонне совместимый с основным языком.

subsidiary [səb'sɪdjəri] *adj.* вспомогательный, дополнительный.

subsidiary deduction [səb'sɪdjəri dɪ'dʌktʃən] вспомогательный вывод.

subset problem = subset sum problem

subspace ['sʌbspeɪs] *n.* подпространство.

substance ['sʌbstəns] *n.* 1. вещество; 2. сущность.# **in substance** по существу, по сути.

substitute (SUB) ['sʌbstɪtju:t] *n.* 1. замена; 2. заместитель; 3. заменитель; *v.* заменять; замещать, подставлять вместо чего-л. (**for**).@ **substitute fraudulent messages for legitimate ones** заменять истинные сообщения на ложные.

substitution [sʌbstɪ'tju:ʃən] *n.* 1. замена, подстановка (криптографическая операция, связанная с заменой каждого символа открытого текста на другой символ из того же алфавита, при этом конкретный вид перестановки определяет секретный ключ); 2. подмена.@ **substitution attack** попытка подмены (атака с подменой).@ **substitution box (S-box)** блок замены.@ **substitution cipher module** модуль (блок) шифрования заменой.@ **substitution cipher** шифр замены.@ **substitution key** ключ шифра замены.@ **substitution row** замена строки.@ **substitution table** таблица замен (одномерный массив без повторов).@ **substitution-permutation network (SPN)** заменно-перестановочная сеть.@ **substitution-transposition cipher** шифр замены-перестановки (замена предшествует перестановке).

substitutional [sʌbstɪ'tju:ʃənəl] *adj.* подстановочный.

subtractive [sʌb'træktɪv] *n.* разностный.@ **subtractive cryptosystem** разностная криптосистема (шифрование выполняется вычитанием ключа из открытого текста, а расшифрование - сложением шифртекста с ключом).

success [sək'ses] *n.* успех.# **to be a success** иметь успех.# **to score a success** иметь успех.# **to meet with success** оказаться успешным.

successful [sək'sesful] *adj.* 1. успешный, удачный; 2. счастливый, удачный.@ **successful attack** успешная (криптоаналитическая) атака.# **to be successful** иметь успех.

succumb [sə'klʌm] *v.* быть уязвимым.@ **succumb to a chosen-ciphertext attack** быть уязвимым по отношению к атаке на основе выбранного шифртекста.

such [sʌtʃ] *adj.* такой.# **such as** такой как; как например.# **such that** так что.# **and such things** и тому подобное.# **as such** как таковой, сам по себе; по существу.

suggest [sə'dʒest] *v.* 1. предлагать; 2. предполагать, высказывать предположение; 3. наводить на мысль. # **to suggest itself** казаться заманчивым, напрашиваться.

suggestive [sə'dʒestiv] *adj.* 1. многообещающий; 2. наводящий (на мысль), напоминающий. # **to be suggestive** напоминать; указывать.

suit [sju:t] *v.* годиться, соответствовать, подходить. # **to be suited for** годиться. # **to follow suit** следовать примеру.

suitable ['sju:təbl] *adj.* подходящий, соответствующий, пригодный.

suite [swi:t] *n.* комплект программ. @ Набор программ или программных модулей, которые в целом отвечают некоторым определенным общим требованиям, причем каждая программа или модуль отвечают некоторой части требований.

summation [sʌ'meɪʃən] *n.* суммирование. @ **summation cipher** суммарный шифр. @ **summation generator** суммирующий генератор (объединяет выходные последовательности, полученные с использованием нескольких регистров сдвига, путем выполнения операции сложения). @ **summation check** проверка суммированием.

sun [sʌn] *n.* солнце. # **against the sun** против часовой стрелки. # **with the sun** по часовой стрелке. # **in the sun** на солнце.

superenciphering ['sju:pə, en'saɪfəɪŋ] *n.* наложение шифров, перешифрование, избыточное шифрование (шифрование уже зашифрованного текста).

superencipherment *n.* = **superenciphering**

superencrypting *n.* = **superenciphering**

superencryption *n.* = **superenciphering**

superimpose (super) [sju:pəɪm'pɒnz] *v.* налагать; накладывать; придавать; *n.* наложение изображений. @ **superimpose cryptograms** накладывать одну криптограмму на другую.

superincreasing [sju:pəɪn'kri:sɪŋ] *adj.* сверхвозрастающий. @ **superincreasing key** сверхвозрастающий (в процессе шифрования) ключ. @ **superincreasing sequence** сверхвозрастающая последовательность.

superpolynomial [sju:pəpɒlɪ'nɒumjəl] *adj.* сверхполиномиальный. @ **superpolynomial cryptanalytic algorithm** сверхполиномиальный криптоаналитический алгоритм, который имеет криптоаналитическую вычислительную сложность дешифрования.

supply [sə'plai] *v.* снабжать; давать; подавать; *n.* 1. снабжение; подача; питание; 2. запас; 3. *pl.* поставки. # **in good supply** в большом количестве; с большим выходом

support [sə'pɔ:t] *n.* 1. поддержка, обеспечение; 2. подтверждение; 3. опора; *v.* 1. поддерживать, обеспечивать. @ Предоставлять необходимые средства. 2. поддерживать, сопровождать. @ Продолжать работу над программным изделием, сданным в эксплуатацию: исправлять ошибки, реагировать на замечание пользователей, давать консультации, распространять новые версии. # **to give (lend) support** оказывать поддержку; подтверждать.

sure [ʃuə] *adj.* уверенный; определенный.# **sure ground** твердая почва.# **to be sure (of)** быть уверенным (в чем-л.).# **to be sure** конечно; несомненно.# **to make sure** удостовериться.

susceptible [sə'septəbl] *adj.* восприимчивый, чувствительный.@ **susceptible to a dictionary attack** уязвимый по отношению к словарной атаке.

suspect [səs'pekt] *v.* подозревать; 2. предполагать.# **to be suspect** быть сомнительным.

sustain [səs'tein] *v.* 1. одерживать; 2. выдерживать; поддерживать.# **self-sustaining** автоматический.

syllabary ['silbəri] *adj.* слоговый.@ **syllabary cipher** слоговый шифр.@ **syllabary code** слоговый кол (содержит отдельные буквы и слоги вместе с соответствующими кодовыми группами, которые используются для кодирования слов и имен собственных отсутствующих в основном коде).@ **syllabary square** шифр типа "слоговой квадрат" (при зашифровании в качестве единиц открытого текста используются как отдельные буквы, так и слоги).

syllabary *n.* 1. = **syllabary code**; 2. = **syllabary cipher**

syllable ['silbəl] *adj.* слоговый.@ **syllable code** слоговый код, силлабический код.@ **syllable frequency** частота встречаемости (появления) слогов (в тексте).

symbol ['simbəl] *n.* 1. символ, обозначение; 2. символ, идентификатор; 3. символ, знак, литера.@ **symbol code** код символа.@ **symbol frequency** частота встречаемости (появления) символов (в тексте).@ **symbol identifier** идентификатор символов.

symbol manipulation ['simbəl mə'nɪpju'leɪʃən] символические операции.@ Манипулирование символами, а не числами, которое имеет место в символьной математике, при подготовки текстов и при моделировании конечных автоматов.

symbol table ['simbəl 'teɪbl] таблица символов; таблица идентификаторов; таблица символических имен.@ Список идентификаторов в исходной программе и их свойств, выдаваемый транслятором.

symbolic [sim'bɒlɪk] *adj.* символический.@ **symbolic address** символический адрес.@ **symbolic assembly-language listing** распечатка программы на входном и выходном языках ассемблера.@ **symbolic code** символический код.@ **symbolic coding** программирование в условных обозначениях (на языке ассемблера).@ **symbolic instruction** символическая команда, команда в символической записи, команда на символическом языке.@ **symbolic interactive design system (SIDS)** система символического интерактивного проектирования.@ **symbolic language** символический язык, язык с символическими обозначениями, язык символов.@ **symbolic layout description language (SLDL)** язык описания символической топологии.@ **symbolic logic** символическая логика.@ **symbolic mathematics** символическая математика.@ **symbolic name** символическое имя (название, наименование).@ **symbolic-coding format** 1.

формат символьных данных; 2. формат слова при символическом кодировании.

symbolic addressing [sim'bolik ə'dresɪŋ] символическая адресация. @ Схема адресации, посредством которой обращение к какому-либо адресу осуществляется через некоторый условный символ.

symbolic debugger [sim'bolik dɪ'bləʒə] символьный отладчик. @ Отладчик, обеспечивающий просмотр и модификацию программы в символических обозначениях, а не в машинном коде.

symmetric ['simetrik] *adj.* симметричный. @ **symmetric cryptosystem** симметричная криптосистема (Общепризнанное преимущество симметричных криптосистем – более высокая скорость шифрования, меньшие размеры используемого ключа и более высокая гарантия криптографической стойкости). @ **symmetric difference** строгая дизъюнкция; исключающее ИЛИ. @ **symmetric encryption** симметричное шифрование. @ **symmetric group** симметричная группа. @ **symmetric key** симметричный ключ (используется как для зашифрования, так и для расшифрования). @ **symmetric relation** симметричное отношение. @ **symmetric(al) distribution** симметричное распределение.

symmetric function ['simetrik 'fʌŋkʃən] 1. симметричная функция. @ Функция, значение которой не меняется при любой перестановке ее аргументов.

symmetric traversal ['simetrik 'trævə:sl] симметричный обход. @ Симметричный маршрут прохождения вершин в двоичном дереве с использованием рекурсивного алгоритма.

symmetric(al) ['simetrik(əl)] *adj.* симметричный. @ **symmetric(al) components** симметричные составляющие. @ **symmetric(al) matrix** симметричная матрица.

symmetrically ['simetrikəli] *adv.* симметрично. @ **symmetrically encrypted** зашифрованный по одноключевому алгоритму.

synchronous ['sɪŋkrənəs] *adj.* 1. синхронный, с ожиданием. @ Об обмене, при котором программа не выполняется во время операции ввода-вывода. 2. синхронный. @ **synchronous circuit** синхронная схема. @ **synchronous command generator (SCG)** генератор синхронных команд. @ **synchronous computer** синхронная машина с постоянным циклом выполнения операций. @ **synchronous cryptooperation** синхронная криптооперации (выполняется в реальном масштабе времени и требует синхронной работы криптографического оборудования). @ **synchronous device** синхронное устройство. @ **synchronous network** синхронная сеть. @ **synchronous stream cipher** синхронный поточный шифр. @ **synchronous system trap routine (SSTR)** ['sɪŋkrənəs 'sɪstɪm træp ru:'ti:n] программа реакции на синхронное (внутреннее) прерывание. @ **synchronous system** синхронная система. @ **synchronous time division multiplexing (STDM)** синхронное временное мультиплексирование. @ **synchronous transmission** синхронная передача (данных). @ **synchronous transmitter-receiver (STR)** синхронный приемопередатчик.

synchronous data link control (SDLC) ['sɪŋkrənəs 'deɪtə lɪŋk kən'troul] синхронная система управления линиями передачи данных.@ Протокол управления передачи данных фирмы IBM.

synchronous system trap (SST) ['sɪŋkrənəs 'sɪstɪm træp] синхронное прерывание.@ Прерывание возникающее в определенной точке программы; как правило внутреннее прерывание, вызванное самой программой.

synthesis ['sɪnθɪsɪs] синтез.@ 1. Мысленное или реальное соединение частей в единое целое. 2. Метод познания, основанный на мысленном или реальном соединении частей в единое целое. Познание является единением, сочетанием анализа и синтеза.@ **synthesis of pseudorandom number generators** синтез генераторов псевдослучайных чисел.

system ['sɪstɪm] *n.* 1. система.@ Средство достижения цели; основные особенности систем: целостность, относительная обособленность от окружающей среды, наличие связей со средой, наличие частей и связей между ними (структурированность), подчиненность всей организации системы некоторой цели. 2. вычислительная система, ЭВМ. 3. системный.@ Относящийся к операционной системе или к системному программированию.@ **system interrupt** обращение к операционной системе.@ **system manager** 1. системный программист. 2. администратор системы.@ **system accounting** учет системных ресурсов.@ **system activity** действия операционной системы.@ **system call** обращение к операционной системе, операция операционной системы.@ **system check** контроль системы.@ **system component** элемент системы.@ **system desing** проектирование системы.@ **system dictionary** системный словарь, словарь системы.@ **system documentation** документация по системе; системная документация.@ **system flowchart** блок-схема работы системы.@ **system for interactive design (SID)** система интерактивного проектирования.@ **system hacker** системный хакер, системщик-виртуоз.@ **system hole** существенная ошибка в системе.@ **system key** системный ключ (используется для шифрования других ключей).@ **system librarian** библиотечарь системы.@ **system loader** программа-загрузчик вычислительной системы.@ **system master key** главный ключ (мастер-ключ) системы.@ **system message block (SMB)** блок системных сообщений.@ **system name** системное имя, системный идентификатор.@ **system of cryptography** криптографическая система.@ **system of equations** система уравнений.@ **system of linear equations in n unknowns** система линейных уравнений с *n* неизвестными.@ **system of logic** система логики, система логических схем.@ **system processing unit (SPU)** системный процессор.@ **system session key** системный сеансовый ключ.@ **system test mode (STM)** режим испытаний на уровне системы.@ **system testing** системные испытания.@ **system variable** системная переменная, системный параметр.@ **system(s) definition** описание вычислительной системы.@ **system-generated key** ключ, генерируемый системой.

system administrator ['sɪstɪm əd'mɪnɪstreɪtə] администратор системы.@ Лицо или группа лиц, контролирующие применение системы пользователями

и определяющие ее конфигурацию, режим работы и используемые программные средства.

system constant ['sɪstɪm 'kɒnstənt] константа операционной системы.@ Параметр операционной системы, доступный пользовательским задачам по фиксированному адресу или посредством системной операции.

system generation ['sɪstɪm 'dʒenəreɪʃən] генерация (операционной) системы.@ Настройка операционной системы на конкретную конфигурацию вычислительной системы и режим ее использования.

system generation option ['sɪstɪm 'dʒenəreɪʃən 'ɒpʃən] параметр генерации.@ Характеристика или средство, выбираемые при генерации системы.

system high ['sɪstɪm haɪ] наивысший уровень полномочий.@ Режим защиты данных, при котором все пользователи системы снабжаются допуском, позволяющим получать доступ ко всей информации в системе, несмотря на то, что различные части базы данных могут иметь разную степень защиты.

system image ['sɪstɪm 'ɪmɪdʒ] образ системы.@ Состояние оперативной памяти ЭВМ с загруженной операционной системой и, возможно, другими задачами, сохраненное на внешнем носителе для последующей загрузки и запуска.

system life cycle ['sɪstɪm laɪf 'saɪkl] жизненный цикл системы.@ Совокупность фаз развития системы, в которой используются средства вычислительной техники. Известны такие фазы системы: концептуальное (эскизное) проектирование, техническое задание, технический проект, рабочий проект, программирование, тестирование, внедрение, эксплуатация и модификация. Некоторые фазы системы могут отсутствовать в ее жизненном цикле.

system log ['sɪstɪm lɒɡ] системный журнал.@ Файл, в котором регистрируются события операционной системы: начало и окончание выполнения задач, смена носителей на внешних запоминающих устройствах, особые действия операторов.

system management ['sɪstɪm 'mænɪdʒmənt] сопровождение системы, координация работы системы.@ Административное управление системой: распределение ресурсов, определение оптимального режима использования системы.

system network architecture (SNA) ['sɪstɪm 'netwɜ:k 'ɑ:kɪtektʃə] сетевая архитектура систем, протокол SNA.@ Разработанная фирмой IBM организация сети ЭВМ. В SNA определено три уровня взаимодействия элементов сети — уровень управления передачей, уровень функционального управления и прикладной уровень.

system process ['sɪstɪm 'prəʊses] системный процесс.@ Часть операционной системы, выполняемая как отдельный процесс.

system programmer ['sɪstɪm 'prəʊgræmə] системный программист.@ Программист, разрабатывающий системное программное обеспечение.

system programming ['sɪstɪm 'prəʊgræmɪŋ] системное программирование.@ Разработка системного или высококачественного программного обеспечения.

system security ['sɪstɪm sɪ'kjʊərɪti] защита системы.@ Обеспечение соответствующих условий для управления доступом к системным ресурсам с учетом требований по защите данных и для контроля за доступом к тем частям системы, которые охвачены средствами защиты.

system specification системная спецификация.@ Четкое определение действий, которые должна выполнять система. Системная спецификация дает законченное описание того, что должна делать система, без каких-либо замечаний по поводу того, как она должна это делать. В рамках системной спецификации система трактуется как «черный ящик»; системная спецификация задает только поведение системы с точки зрения внешнего наблюдателя и не затрагивает ее внутреннюю реализацию.

system tables ['sɪstɪm 'teɪbls] системные таблицы.@ Данные, которые в совокупности определяют состояние всех ресурсов и всех процессов в системе.

systematically [ˌsɪstɪ'mætɪkəli] *adv.* систематически.@ **systematically mixed sequences** методично смешанные последовательности.

systematicity [ˌsɪstɪ'mætɪsɪti] *n.* системность.@ 1. Обладание всеми признаками системы. 2. Всеобщее свойство материи, форма ее существования, а следовательно, неотъемлемое свойство человеческой практики, включая мышление

syndromesystem-call interrupt ['sɪndrəʊm'sɪstɪm'kɔ:l ɪntə'rʌpt] 1. обращение к операционной системе. 2. системное прерывание; 3. прерывание от управляющей программы системы.

systems architect ['sɪstɪms 'a:kɪtekt] разработчик архитектуры вычислительной системы или программы, архитектор вычислительной системы.

systems analysis ['sɪstɪms ə'næləsɪz] системный анализ.@ 1. С практической стороны системный анализ есть система методов или проектирования сложных систем, поиска, планирования и реализации изменений, предназначенных для ликвидации проблем. 2. С методологической стороны системный анализ является прикладной диалектикой, так как реализует идеи материалистической диалектики применительно к конкретным практическим задачам, особенность которых состоит в необходимости выяснения причин их сложности и устранения этих причин. 3. С методической стороны системный анализ отличается междисциплинарным и наддисциплинарным характером и вовлечением в работу как неформальных, эвристических, экспертных методов, так и эмпирических, экспериментальных методов, а также при возможности и необходимости – строгих формальных математических методов.

systems approach ['sɪstɪms ə'prəʊtʃ] системный подход.@ Рассматривается либо как одна из ранних форм системного анализа, либо как начальная фаза современного системного анализа, этап первоначального, качественного анализа проблемы и постановки задач.

systems programmer ['sɪstɪms 'prəʊgræmə] системный программист.@ Специалист, который специализируется по системному программированию и

программному обеспечению нижнего уровня, т. е. операционным системам, компиляторам, системам связи и системами управления базами данных.

systems programming ['sɪstɪms 'prɒɡræmɪŋ] системное программирование. @ Создание системного программного обеспечения. Граница между системным программированием и прикладным программированием нечеткая. Например, с точки зрения программиста, который занимается ядром операционной системы, человек, создающий компиляторы, является пользователем системы (т. е. прикладным программистом), хотя этот же человек будет, вероятно, рассматриваться как системный программист тем лицом, которое занимается написанием подпрограмм для отыскания минимума функции. Однако, человек, который будет использовать программу минимизации, может считать всех трех вышеупомянутых программистов системными программистами.

systems software ['sɪstɪms 'sɒftwɛə] системное программное обеспечение. @ Программное обеспечение, используемое для разработки и выполнения прикладных программ. Понятие «системный» и «прикладной» относительно: транслятор является прикладной программой по отношению к операционной системе и системной – по отношению к транслируемой программе.

systems theory ['sɪstɪms 'θiəri] теория систем. @ Область науки, связанная с изучением систем как таковых с целью выявления их общих характеристик или классификации.

T*

table ['teɪbl] *n.* 1. таблица, стенд, планшетный стол; 2. стол. # **table of contents** оглавление. # **time-table** расписание.

tactical ['tæktɪkəl] *adj.* тактический. @ **tactical encryption device** шифратор тактического назначения.

take [teɪk] *v.* (**took, taken**) 1. брать; 2. принимать, считать; 3. браться за что-л. (**up**); 4. требовать; 5. взлетать (**off**); 6. поглощать (**up**); присоединять (**up**). # **to take account of** учитывать. # **to take advantage** использовать; воспользоваться. # **to take care of** заботиться; следить; принимать меры. # **to take as (for) granted** считать доказанным; принимать без доказательства. # **to take effect** возыметь действие; вступать в силу. # **to take hold of** воспользоваться; ухватиться. # **to take measures** принимать меры. # **to take note of** обращать внимание на что-л. # **to take notice of** обращать внимание на что-л. # **to take recourse to** прибегать к помощи. # **to take a picture (a photograph)** снимать, фотографировать. # **to take place** иметь место, происходить. # **to take steps** принимать меры. # **to take stock (of)** подвести итоги; проводить инвентаризацию, переучет. # **to take to pieces** разобрать на части.

tamper ['tæmpə] *v.* подделывать. @ **tamper proof** защищенный от воровства или от неумелого обращения. @ **tamper resistant** имитостойкий. @ **tamper with information** подделывать информацию. @ **tamper-free channel** физически защищенный канал.

tap [tæp] *n.* отвод, ответвление (от линии связи); *v.* делать отвод (от линии связи), подключаться (к линии связи).

tapped *adj.* = **wiretapped**

target (ТА, tgt) ['tɑ:gɪt] *n.* 1. адресат. @ Элемент данных или область памяти, куда пересылается результат или где производится поиск. 2. выходной; объектный; целевой; 3. мишень; 4. цель. @ **target assignment problem** задача (проблема) целераспределения. @ **target conversion** адаптация программы к особенностям целевой ЭВМ. @ **Target Exploitation (TAREX)** разработка цели (поиск несекретной информации, касающейся страны, которая является объектом радиоразведывательной деятельности, а также периодическое посещение этой страны специально обученным персоналом с целью сбора открытых данных о ее коммуникациях). @ **target language** объектный язык, выходной язык. @ **target method** метод проб, метод «пристрелки». @ **target phase** фаза первого прогона программы после составления.

target alphabet ['tɑ:gɪt 'ælfəbɪt] выходной алфавит. @ Алфавит, из символов которого строится выходная последовательность.

target processor ['tɑ:gɪt 'proʊsesə] целевой процессор, объектный процессор. @ При кросс-разработке – процессор, на котором будет работать разрабатываемая система.

target record ['tɑ:gɪt 'rekɔ:d] целевая запись. @ Запись, удовлетворяющая условиям поиска запроса.

target system ['tɑ:gɪt 'sɪstɪm] целевая система. @ Система, для которой предназначена разрабатываемая программа.

target-computer ['tɑ:gɪt kəm'pjʊ:tə] целевая ЭВМ, объектная ЭВМ. @ При кросс-разработке – ЭВМ, программа для которой разрабатывается с использованием системы разработки программ на другой ЭВМ.

taxonomy ['tæksənəmi] *n.* классификация. @ **taxonomy for authentication schemes** классификация схем аутентификации.

technical ['tekni:kəl] *adj.* технический. @ **technical extracts of traffic (TEXTA)** технические отрывки из переписки (сгенерированный компьютером NSA USA отчет, содержащий характеристику всех коммуникационных сетей в мире кому, каким образом и что именно они передают). @ **technical instructions (TECHINS)** технические инструкции.

technique [tek'ni:k] *n.* 1. метод, методика; 2. техника, технические приемы; 3. технология; техническое оснащение, аппаратура. @ **technique of substitution** метод подстановки.

technocratic [tek'nə'krəti:k] *adj.* технократический.

technological [tek'nə'lɒdʒɪkəl] *adj.* технологический, технический.

technology [tek'nɒ'lɒdʒɪ] *n.* 1. технология; 2. техника.

telecommunication ['telɪkə'mju:ni'keɪʃən] связь. @ **telecommunication access method (TCAM)** общий телекоммуникационный метод доступа. @ **telecommunication network** сеть связи; сеть передачи данных. @ **telecommunications** телекоммуникации, средства телекоммуникационной связи. @ **telecommunica-**

tions systems accessible to wiretaps телекоммуникационные системы, доступные для перехвата путем подключения к проводным линиям связи.

telegram ['teligræm] *n.* телеграмма. @ **telegram in cipher** шифрованная телеграмма (шифровка). @ **telegram in clear** открытый текст телеграммы (незашифрованная телеграмма). @ **telegram in code** кодированная телеграмма.

telegraph ['teligra:f] *n.* телеграф; *v.* телеграфировать, передавать по телеграфу.

telegraphic [ˌtelɪ'græfɪk] *adj.* телеграфный. @ **telegraphic code** телеграфный код. @ **telegraphic communication** телеграфная связь.

telemetry [ti'lemɪtri] *n.* телеметрия. @ **telemetry automatic reduction equipment (TARE)** аппаратура автоматической обработки телеметрических данных. @ **telemetry information system (TIS)** телеметрическая информационная система.

telemetric equipment (TE, TME) [ti'lemɪtrɪk ɪ'kwɪpmənt] телеметрическое оборудование.

telex (TEX, TLX) ['telɪks] *n.* телекс. @ **telex tape encryptor** шифратор телексных сообщений с записью на ленту.

telex server ['telɪks 'sɜ:və] станция телексной связи. @ Узел локальной сети, обеспечивающий связь других узлов сети с телексной сетью.

telltale ['telteɪl] *adj.* сигнальный, контрольный. @ **telltale emanation** сигнальное излучение (работающей радиоэлектронной аппаратуры, несущее конфиденциальную информацию).

temporary ['tempərəri] *n.* временный, рабочий. @ О структуре данных (во внешней памяти), время существования которой ограничено временем работы использующей ее задачи. @ **temporary disk** рабочий диск. @ **temporary error** неповторяющаяся ошибка, нерегулярная ошибка. @ **temporary key** временный (временно действующий) ключ. @ **temporary storage** 1. рабочая память; буфер; 2. временное хранение (данных). @ **temporary storage register** регистр временного запоминания данных.

temporary file ['tempərəri faɪl] рабочий файл, временный файл. @ Файл, который удаляется или может быть удален после завершения создавшей его задачи или последовательности задач.

temporary realm ['tempərəri relm] временная область. @ В базах данных — область (множество записей), которая существует только в течение выполнения создавшего ее процесса.

term [tɜ:m] *n.* 1. термин; 2. терм. @ Элементарный член арифметического или логического выражения, именующий элемент данных или являющийся значением функции или константой. 3. условие; 4. выражение; значение; 5. член (*mat.*); 6. срок; *v.* называть, выражать. # **in terms of** в понятиях; на языке; в единицах; в выражениях; на примере; через; в виде; на основе; в функции; в значениях; в зависимости от; с точки зрения; по. # **in general terms** в общих чертах. # **to make terms with** прийти к соглашению с кем-л.

terminal *adj.* терминальный; *n.* терминал (оконечное абонентское устройство).@ **terminal cryptographic unit (TCU)** криптографический терминал.@ **terminal key** терминальный ключ.

test (TST) [test] *n.* 1. тестирование, проверка; 2. тест.@ Данные и программы, используемые для тестирования. 3. проверка (*условия*); 4. испытание; *v.* 1. тестировать, проверять.@ Запускать программу по специально подобранным данным, чтобы обнаружить имеющиеся в ней ошибки или убедиться в отсутствии некоторой определенной ошибки. 2. проверять; 3. испытывать.@ **test key** проверочный ключ.@ **test on a "bombe"** проверять (ключ немецкой шифровальной машины "Энигма") с помощью "бомбы".# **under test** испытываемый.# **end-use test (ing)** эксплуатационное испытание.

tetragram [te'trægrəm] *n.* тетраграмма (четыре символа текста).@ **tetragram count** маркировка тетраграмм.@ **tetragram frequency** частота встречаемости (появления) тетраграмм (в тексте).

tetragram counting = tetragram count

tetragraph *n.* = **tetragram**

text (TXT) [tekst] *n.* текст.@ 1. Напечатанная, написанная или отображенная на экране дисплея последовательность литер. 2. Данные, последовательные байты которых интерпретируются как коды литер. 3. Информационная часть сообщения. 4. Части объектного модуля, содержащие команды программы.@ **text-dependent encryption** шифрование, зависящее от текста (шифрование на ключе, зависящем от текста).@ **text origination** ввод текста с клавиатуры.@ **text processing** 1. обработка текста; 2. подготовка текстов.@ **text revision** редактирование текста.@ **text routine** тестовая программа.@ **text string** текстовая строка.

text editor [tekst 'editə] текстовый редактор, редактор текстов.@ Программа, обеспечивающая редактирование текстов программ и документов в соответствии с задаваемыми пользователем командами.

text file [tekst fail] текстовый файл.@ Файл, содержащий информацию в виде последовательности текстовых символов, разделенных символами новой строки, и не содержащий управляющих символов. Такой файл можно распечатать командой TYPE.

text formatting [tekst 'fɔ:mætɪŋ] форматирование текста.@ В системах подготовки текстов – преобразование текста в вид, в котором он должен печататься: форматирование абзацев, центрирование заголовков, выравнивание полей, с разбивкой на страницы.

text-retrieval system [tekst,ri'tri:vəl 'sistɪm] документальная информационная система.@ База данных или информационная система, элементы которой являются текстовыми фрагментами произвольной длины (документами) и доступ к которым производится по дескрипторам или ключевым словам.

than [ðæn] *conj.* чем.# **rather than** а не; скорее ... чем; вместо того, чтобы.

thank [θæŋk] *v.* благодарить.# **thanks to** благодаря, вследствие.

that [ðæt] *pron. (pl.. those)* 1. тот, та, то; 2. который; 3. заменяет предыдущее существительное (*of*); *conj.* что, чтобы; так что; то, что (обычно в начале

предложения); *adv.* так, до такой степени. # **that is (to say)** то есть. # **that is why** вот почему. # **by that** тем самым, этим. # **in that** в том (смысле) что; тем, что. # **now that** теперь, когда.

the [ði:] *определенный артикль* этот, эта, эти. # **the ... the** чем ... тем (*употребляется в сочетании с прилагательным или наречием в сравнит. степени, например: the sooner the better* чем скорее, тем лучше).

then [ðen] *adv.* 1. тогда; 2. потом, затем; 3. в таком случае. # **every now and then** время от времени. # **since then** с того времени, после этого, с тех пор.

theoretical [θiə'retikəl] *adj.* теоретический. @ **theoretical attack** теоретическая атака (крипто-аналитическая атака на шифр, которая хотя и приносит желаемый успех при наличии определенных условий, но тем не менее не реализуема на практике, поскольку в реальной жизни эти условия невозможно соблюсти). @ **theoretical cryptanalysis** теоретический криптоанализ. @ **theoretical security** теоретическая стойкость.

theoretically [θiə'retikəli] *adv.* теоретически. @ **theoretically unbreakable** теоретически невскрываемый.

thing [θɪŋ] *n.* 1. вещь; предмет; 2. дело; 3. случай. # **and such things** и тому подобное. # **(all) other things (conditions) being equal** при прочих равных условиях. # **among other things** между прочим. # **for one thing** во-первых; прежде всего. # **the thing is** дело в том, что. # **the same kind of thing** то же самое.

third-party [θə:d'pa:ti] *adj.* третья сторона (в дополнение к отправителю и получателю сообщений). @ **third-party key** ключ, полученный от третьей стороны (напр, из центра распределения ключей).

though [ðəu] *conj.* хотя. # **as though** как будто, как если бы. # **even though** даже если.

thought [θɔ:t] *n.* мысль; мышление. # **at first thought** на первый взгляд. # **on (upon) second thoughts** поразмыслив, основательно подумав. # **upon further thought** поразмыслив, основательно подумав.

threat [θret] *n.* угроза. @ **threat analysis** анализ (возможных) угроз.

three- [θri:] в сложных и сложносоставных словах имеет значение трех-, @ **three(-)key method** трех-ключевой метод; метод трех ключей (передача секретного ключа шифрования с использованием криптосистемы с открытым ключом). @ **three-wheel Enigma** трехроторная (трехдисковая) "Энигма".

threshold ['θreʃəʊld] *n.* порог, пороговая величина. @ **threshold cryptosystem** пороговая криптосистема. @ **threshold RSA signature scheme** пороговая RSA-схема цифровой подписи.

through ['θru:] *prep.* 1. через, сквозь, по; 2. посредством; при помощи; 3. на протяжении; 4. включительно, по; *adv.* сплошь, насквозь; *adj.* 1. прямой, беспересадочный; сквозной; 2. свободный (о проходе и т. п.). # **all through** на сем протяжении. # **through (by) the agency** посредством. # **to be through with** покончить с чем-л. # **to carry through** довести до конца; закончить что-л. # **to look through** просмотреть (статью и т. п.)

throughout ['θru:aut] *adv.* 1. во всех отношениях; 2. повсюду; на всем протяжении.

throughput ['θru:put] *n.* 1. производительность (вычислительной системы); пропускная способность (канала связи); 2. выход.

thus [ðʌs] *adv.* таким образом. # **thus far** до сих пор, пока.

tight ['taɪt] *adj.* 1. плотный; 2. непроницаемый, устойчивый; 3. сжатый. # **water-tight** водонепроницаемый.

time [taɪm] *n.* 1. время, момент времени; 2. период; 3. раз; 4. умноженный на; *v.* 1. отмечать время; хронировать; рассчитывать по времени; согласовать во времени, синхронизовать. @ **time and frequency sequential permutation** последовательная частотно-временная перестановка. @ **time attack** временная атака (позволяет вскрывать ключи путем замера времени, которое требуется для выполнения криптографических операций). @ **time complexity** временная сложность (алгоритма). @ **time division multiplexing (TDM)** мультиплексирование с временным делением. @ **time segment permutation** перестановка сегментов сигнала во времени. @ **time-dated message** сообщение с отметкой времени. @ **time-expired key** ключ с ограничением срока действия. @ **time-lock puzzle** "шарада" с временным замком. @ **timestamp** отметка времени. @ **time-varying cipher** шифр с изменяющимся во времени ключом (меняющийся во времени шифр). # **theree (four etc.) times** умноженный на три (четыре и т. д.); в три (четыре и т. д.) раза больше. # **time and again** неоднократно. # **at a time** за (один) раз. # **at the time** в это (то) время. # **at times** иногда. # **at no time** никогда. # **at one time** в одно время. # **by that time** к тому времени. # **for a time** в течение некоторого времени. # **for the first time** в первый раз, впервые. # **for the time being** пока; на некоторое время. # **from time to time** время от времени. # **in due time (course)** в свое время. # **in no time** очень быстро. # **in time** вовремя; со временем. # **some time or other** когда-нибудь. # **this time** на этот раз.

time cryptanalysis = time attack

timing ['taɪmɪŋ] *n.* хронометраж, замер времени.

tiny ['taɪnɪ] *adj.* очень маленький, крошечный. @ **Tiny Encryption Algorithm (TEA)** Крошечный алгоритм шифрования.

tissue ['tɪʃu:] *n.* ткань. # **conjunctive (connective) tissue** соединительная ткань.

top [tɒp] *n.* вершина, верхняя часть. # **on top** поверх.

top-secret [tɒp'sekret] *adj.* совершенно секретный.

total ['təʊtl] *adj.* тотальный. @ **total encryption** тотальное шифрование (всего потока информации).

totally ['təʊtlɪ] *adv.* абсолютно. @ **totally-random key** абсолютно случайный ключ.

tractable ['træktəbl] *adj.* легко поддающийся обработке. @ Разрешимый с полиномиальной сложностью (о математической задаче, для которой существует алгоритм решения с полиномиальной сложностью).

trade [traɪd] *adj.* торговый. @ **trade cipher system** "торговый" шифр (шифр, применявшийся для засекречивания переписки между Москвой и советским торговым представительством в USA).

traffic ['træfɪk] *n.* 1. трафик. @ Поток сообщения в сети передачи данных. 2. рабочая нагрузка линии. @ Мера объемов данных или сообщений, проходящих между пунктами в сети связи. @ **traffic analysis** анализ переписки. @ **traffic key** ключ обмена сообщениями. @ **traffic problem** транспортная задача. @ **traffic padding** холостое заполнение трафика (генерация ничего не значащих (фальшивых блоков данных) и/или отдельных ничего не значащих (фальшивых элементов данных) внутри подлинных блоков данных).

traffic encryption key (TEK) = traffic key

traffic control ['træfɪk kən'troul] управление трафиком. @ Термин, используемый в некоторых случаях применительно к управлению вводом и выводом.

traffic requirement matrix ['træfɪk rɪ'kwaɪment 'meɪtrɪks] матрица трафика. @ Матрица M , в которой m_{ij} обозначает интенсивность пересылки сообщений из узла i в узел j .

training ['treɪnɪŋ] *adj.* учебный, тренировочный. @ **training key** учебный (тренировочный) ключ (используется для целей обучения обслуживающего персонала).

transaction [træn'zækʃən] *n.* 1. транзакция, обработка запроса. @ 1. В диалоговых системах – прием порции данных (сообщения, запроса) от пользователя, ее обработка и выдача ответного сообщения. 2. В базах данных и файловых системах – выполнение элементарной целостной операции над данными (например, постановка, удаление или модификация записи), в течение которой база данных или файловая система находится в неустойчивом состоянии. 2. запрос, запись файла изменений. @ **transaction key** ключ (одной) транзакции. @ **transaction processing monitor (TP monitor)** монитор обработки транзакций. @ **transaction record** управляющая запись, запись транзакции. @ **transaction-oriented system** диалоговая система обработки запросов. @ **transaction-routing (TR)** маршрутизация сообщений. @ **transactions log** журнал транзакций.

transaction data [træn'zækʃən 'deɪtə] параметры транзакции. @ Данные подлежащие внесению в основной массив для его обновления.

transaction file [træn'zækʃən faɪl] файл изменений, файл транзакций; файл входных сообщений. @ Файл, содержащий записи входных сообщений и сформированный до момента изменения эталонного файла.

transaction processing [træn'zækʃən 'prəʊsesɪŋ] диалоговая обработка запросов. @ Режим работы многопользовательской системы, при котором каждый запрос пользователя обрабатывается как независимая задача, взаимодействующая с пользователем.

transfer (xfer) ['trænsfə:] *n.* 1. пересылка (данных); передача (данных). @ Перемещение данных из одной области памяти в другую или с одного устройства на другое. 2. переход, передача управления; *adj.* передаточный; *v.* 1. выполнять команду перехода; 2. передавать, переносить; пересылать; переставлять. @ **transfer authentication code (TRAC)** код передачи с паролем. @ **transfer characteristic** передаточная характеристика. @ **transfer constant** 1. коэффициент передачи; 2. постоянная передачи. @ **transfer control** переходить, пере-

давать управление. @ **transfer efficiency** коэффициент переноса. @ **transfer instruction** команда перехода. @ **transfer of a secret key** передача секретного ключа. @ **transfer of control instruction** команда перехода, команда передачи управления. @ **transfer of control** передача управления, команда перехода, команда передачи управления. @ **transfer operation** операция передачи управления, операция перехода. @ **transfer rate** скорость передачи (*данных*). @ **transfer scheme** схема чтения и записи. @ **transfer time** время пересылки (*данных*).

transfer function ['trænsfə: 'fʌŋkʃən] функция преобразования типа. @ В языках программирования со строгим контролем типов – функция, преобразующая значение одного типа в соответствующее значение другого типа с изменением или без изменения внутреннего представления этого значения.

transfer table ['trænsfə: 'teɪbl] таблица переходов, переключатель. @ Обычно подразумевается реализация переключателя в виде массива команд перехода.

transfer unit ['trænsfə: 'ju:nɪt] блок; слово; порция обмена. @ Порция данных, пересылаемое как единое целое. Размер порции зависит от обменивающихся устройств: при пересылке внутри процессора или между регистрами и памятью – слово, при обмене с внешней памятью – блок, сегмент или страница.

transform [træns'fɔ:m] *n.* преобразование; *v.* 1. преобразовывать; 2. превращать; *n.* трансформация

transformation [trænsfə'meɪʃən] *n.* трансформация; преобразование (функция, отображающая пространство сообщений в пространство криптограмм). @ **transformation row** правило преобразования. @ **transformation semantics** трансформационная семантика.

transformation matrix (TM) [trænsfə'meɪʃən 'meɪtrɪks] матрица преобразований. @ Числовая матрица размерности $m \times n$, используемая для отображения векторов с n компонентами на векторы с m компонентами.

transformed [træns'fɔ:md] *adj.* преобразованный. @ **transformed ciphertext** преобразованный шифртекст.

transient ['trænzɪənt] *n.* 1. нерезидентный. @ 1. О программе или сегменте программы, которые загружаются в оперативную память по мере необходимости и освобождают ее после завершения. 2. Об областях оперативной памяти, выделенных для нерезидентных программ. *adj.* 1. преходящий, кратковременный; 2. неустановившийся; переходный; промежуточный. @ **transient error** неповторяющаяся ошибка, нерегулярная ошибка. @ **transient key** промежуточный ключ. @ **transient period** длительность переходного процесса. @ **transient state** 1. промежуточное состояние, неустойчивое состояние; 2. переходное во времени состояние. @ **transient-key cryptography** криптография с переменным ключом.

transient area ['trænzɪənt 'ɛəriə] нерезидентная область. @ Область оперативной памяти, в которую загружаются нерезидентные программы.

transient command ['trænzjənt kə'ma:nd] *нerezидентная команда.*@ Команда диалогового монитора, выполняемая *нerezидентной программой* или *нerezидентной частью операционной системы*.

transient routine ['trænzjənt ru:'ti:n] *нerezидентная программа.*@ Программа, загружаемая в оперативную память при каждом вызове.

transition from clear to cipher = transition from clear to cipher

transition [træn'sɪzən] *n.* 1. переход (*из одного состояния в другое*); 2. перемещение, переход; 3. изменение.@ **transition from clear to cipher** переход (переключение) с открытой на шифрованную связь.@ **transition operator** 1. оператор перехода; 2. операция перехода.@ **transition point** точка ветвления.@ **transition probability** вероятность перехода.

translate [træns'leɪt] *v.* 1. сдвигать, перемещать; 2. переводить; транслировать; 3. преобразовывать (*из одного кода в другой*).@ **translate into cipher** зашифровывать.@ **translate out of cipher** расшифровывать.

translation [træns'leɪʃən] *n.* 1. сдвиг.@ В машинной графике – прибавление постоянного вектора (*вектора сдвига*) к координатам одного или нескольких элементов изображения, вызывающее их перемещение. 2. перевод; трансляция; конвертирование.@ Применительно к программам может обозначать как перевод (трансляцию) на машинный язык, так и немедленную интерпретацию или перевод на другой язык программирования.@ **translation algorithm** алгоритм преобразования, алгоритм автоматического перевода.@ **translation circuit** 1. схема перевода; 2. схема преобразования одного кода в другой.@ **translation from one key to another** переход от одного ключа к другому.@ **translation vector** вектор сдвига.

translation table [træns'leɪʃən 'teɪbl] 1. адресная таблица, таблица страниц.@ Программная или аппаратная структура данных, используемая для преобразования виртуальных адресов в физические. 2. таблица перевода.@ Информационная таблица, хранящаяся в процессоре или периферийном устройстве, которая используется для преобразования закодированной информации в другую форму кода с сохранением тех же значений.

transmission [trænz'mɪʃən] *n.* 1. передача (*данных по линии связи*); 2. пропускание; 3. прохождение.@ **transmission and distribution (TD)** передача и распределение.@ **transmission channel** канал передачи.@ **transmission control character** знак управления передачей.@ **transmission control protocol (TCP)** протокол управления передачей.@ **transmission control unit (TCU)** блок управления передачей.@ **transmission delay** задержка в цепи передачи сигнала.@ **transmission distortion measuring set (TDMS)** устройство для измерения искажений при передаче.@ **transmission factor** коэффициент пропускания.@ **transmission line** линия связи.

transmit [trænz'mɪt] *v.* передавать; пересылать.@ **transmit a coded message** передавать кодированное сообщение.@ **transmit in encrypted form** передавать в зашифрованном виде..

transmitted [trænz'mɪtɪd] *adj.* переданный.@ **transmitted key** переданный ключ.@ **transmitted message** переданное сообщение.

transmitter [trænz'mitə] *v.* 1. отправитель (сообщения) ; 2. передатчик. @ **transmitter's** ключ отправителя (сообщения).

transparency [træns'pɛərənsi] *n.* прозрачность (инвариантность по отношению к характеристикам различных систем и устройств, а также к типу шифруемых данных).

transparent [træns'pɛənt] *adj.* прозрачный, скрытый. @ О промежуточных средствах взаимодействия, применение которых незаметно пользователю (человеку или программе), так как они сохраняют интерфейс, используемый при их отсутствии. @ **"transparent" cryptography** "прозрачная" криптография (не требует от пользователя знания ее принципов, не зависит от типа шифруемых данных, характеристик системы и входящих в нее устройств, не влияет на их нормальную работу). @ **transparent language** язык с очевидной семантикой. @ **transparent transmission** кодонезависимая передача (данных).

"transparent data" [træns'pɛənt 'deitə] «прозрачные данные», абстрактные данные. @ Данные, физическая организация которых скрыта от программы; программа работает только с существующими для нее элементами данных и не обрабатывает служебных подструктур.

transparent interface [træns'pɛənt ,intə'feis] прозрачный интерфейс. @ Организация интерфейса, при которой интерфейсные средства не преобразуют передаваемые данные и логически незаметны для пользователя.

transport ['trænsɜ:t] *adj.* транспортный; *n.* 1. перенос; 2. перемещение; 3. транспорт; *v.* переносить. @ **transport encryption** транспортное шифрование (транзитное шифрование информации, поступающей по внешним каналам, на транспортном уровне). @ **transport factor** коэффициент переноса. @ **transport key** транспортный ключ (используется для шифрования другого ключа при его передаче). @ **transport problem** транспортная задача.

transport (layer) protocol ['trænsɜ:t ('leiə) 'proutəkɒl] транспортный протокол, протокол транспортного уровня. @ Основной уровень протокола сети передачи данных, регламентирующий пересылку сообщений (пакетов) между процессами, выполняемыми на ЭВМ сети.

transposition = transposition cipher

transposition [trænsɜ:'ziʃən] *n.* перестановка (специальная криптографическая операция, при которой символы открытого текста перемешиваются, причем конкретный вид перемешивания определяет секретный ключ). @ **transposition cipher** перестановочный шифр. @ **transposition mixed sequences** перестановочные смешанные последовательности. @ **transposition-substitution cipher** шифр перестановки - замены (перестановка предшествует замене).

trapdoor ['træp'dɔ:] *n.* лазейка, потайной ход (слабое место в шифрсистеме). @ **trapdoor cipher** шифр с потайным ходом. @ **trapdoor knapsack** ранец с лазейкой. @ **trapdoor one-way function** односторонняя функция с лазейкой.

trapping ['træpiŋ] *n.* организация лазеек (потайных ходов) (в шифрсистеме).

treatise *n.* трактат. @ **treatise on cryptography** трактат по криптографии, @ **Treatise on the "Enigma"** Трактат об "Энигме" (работа А. Тьюринга, в которой на примере немецкой шифровальной машины "Энигма" поясняются различные методы, используемые в криптоанализе).

treble *adj.* = **triple**

trial decipherment = **trial decryption**

trial [triəl] *n.* проба. @ **trial decryption** пробное дешифрование. @ **trial encryption** пробное шифрование. @ **trial key** пробный ключ (при криптоаналитическом исследовании криптосистемы методом проб и ошибок). @ **trial-and-error cryptanalysis** криптоанализ методом проб и ошибок.

trick [trɪk] *v.* добиваться обманным путем. @ **trick subscribers into encrypting their messages with phony keys** обманным путем добиваться, чтобы абоненты шифровали свои сообщения на ложных ключах.

trigram counting = **trigram count**

trigram ['trɪgræm] *n.* триграмма (три символа текста). @ **trigram count** маркировка триграмм. @ **trigram frequency** частота встречаемости (появления) триграмм (в тексте).

trigraph *n.* = **trigram**

trilateral ['trɪlætərə] *adj.* 1. трехбуквенный; трехсторонний; 2. трехбуквенная шифрсистема. @ **trilateral frequency count** трехсторонняя маркировка (для каждой буквы текста подсчитываются три частоты встречаемости - ее самой, а также двух букв, расположенных от нее слева и справа).

trinome ['trɪnoum] *n.* три цифры, тройка цифр.

trinomic ['trɪnoumɪk] *adj.* 1. трехцифровой; 2. трехцифровая шифрсистема. @ **trinomic cipher system** трехцифровая шифрсистема (при зашифровании каждый символ открытого текста заменяется на три цифры).

triple ['trɪpl] *adj.* строенный; тройной; трехкратный; утроенный; *v.* утраивать. @ **triple access** тройная выборка, тройное одновременное обращение. @ **triple encryption** трехкратное шифрование. @ **triple error correcting code** код с исправлением тройных ошибок. @ **triple integral** тройной интеграл.

triple precision ['trɪpl prɪ'sɪʒən] утроенная точность (тройная тоность). @ Использование для представления числа втрое большего, чем обычно, числа битов. @ **triple DES** "тройной" DES (утроенное шифрование по DES-алгоритму с разными ключами).

triplet ['trɪplet] *n.* триплет (три одинаковых, идущих подряд знака текста).

Trojan horse ['trɔɪdʒən 'hɔ:s] троянский конь. @ Любая функциональная возможность в программе, специально встроенная для того, чтобы обойти системный контроль секретности. @ **Trojan horse software** компьютерные программы типа "троянский конь" (резидентные программы, предназначенные для перехвата ключей и открытых текстов, принадлежащих пользователям компьютерных систем).

true [tru:] *adj.* 1. истинный. @ 1. Имеющий значение «истина». 2. Физический (в отличии от условного, логического, виртуального). 2. «истина» (логи-

ческое значение); 3. справедливый, подлинный. @ **true complement** точное дополнение. @ **true key** подлинный ключ. @ **true mean** истинное среднее значение. @ **true message** настоящее сообщение. @ **true rate of a language** истинная норма языка. @ **true representation** прямой код, представление в обычном виде. @ **true statement** истинное утверждение. @ **true-time operation** операция в истинном масштабе времени. # **true to life (nature)** реалистический, правдивый. # **to hold true** быть справедливым; быть действительным.

truly ['tru:li] *adv.* действительно. @ **truly unbreakable cipher** действительно невскрываемый шифр.

truly random sequence = **really random sequence**

truncate ['trʌŋkeit] *v.* 1. усекать, округлять (*отбрасыванием младших разрядов*); 2. обрезать, укорачивать. @ Отбрасывать конечные, реже начальные, элементы строки. 3. прерывать (*вычисление ряда или выполнение итерационного процесса*). @ **truncate list** список остатков.

truncated ['trʌŋkeitɪd] *adj.* усеченный. @ **truncated congruential generator** усеченный конгруэнтный генератор. @ **truncate(d) distribution** усеченное распределение.

trunk ['trʌŋk] *n.* линия магистральной связи. @ **trunk encryption device** устройство шифрования для линий магистральной связи.

trusted ['trʌstɪd] *adj.* надежный, проверенный; доверенный, трастовый. @ **Trusted Computing System Evaluation Criteria (TCSEC)** Критерий оценки защищенности вычислительной системы (американский стандарт, установленный директивой MO USA № 520028-STD и определяющий 4 иерархических класса защищенности вычислительных систем, разрабатываемых и используемых в правительственных интересах). @ **trusted key distribution center (TKDC)** доверенный (трастовый) центр распределения ключей. @ **Trusted Third Party (TTP)** доверенная третья сторона.

truth [tru:θ] *n.* истинность. @ **truth value** истинное значение.

truth table [tru:θ 'teɪbl] истинностная таблица. @ Способ задания логической функции в виде таблицы, каждый элемент которой соответствует комбинации аргументов.

try [traɪ] *v.* 1. пробовать, испытывать; 2. пытаться, стараться. @ **try-all-possible-keys cryptanalysis** криптоанализ методом перебора всех возможных вариантов ключа. # **cut and try method** экспериментальный метод; метод последовательных приближений

tuple [tʌpl] *n.* кортеж (набор взаимосвязанных величин); **k-tuple** кортеж из k элементов.

Turing machine ['tju:ɾɪŋ mə'ʃi:n] машина Тьюринга.

turn(-)off ['tə:n ɔ:f] *adj.* двухключевой; *n.* запирающее, выключение; *v.* запирать, выключать. @ **turn off cryptography** двухключевая криптография. @ **turn off encryption** отключать шифрование.

turn(-)on ['tə:n 'ɒn] *n.* отпирание, включение; *v.* отпирать, включать.

twice [twais] *adv.* 1. дважды; 2. вдвое. # **twice as good** вдвое лучше. # **twice as little** вдвое меньше. # **twice as much** вдвое больше.

two- [tu:] в сложных и сложносоставных словах имеет значение двух-.@ **two-address instruction** двухадресная команда.@ **two-dimensional array** матрица, двумерный массив.@ **two-dimensional graph** двумерный граф.@ **two-dimensional picture** двумерное плоское изображение.@ **two-dimensional word selection memory** память с двумерной выборкой слова.@ **two-letter** двухбуквенный.@ **two-level address** косвенный адрес.@ **two-level grammars** двухуровневые грамматики.@ **two-norm (Euclidean norm)** норма по скалярному квадрату; Евклидова норма.@ **two-part code** двухчастевой код (состоит из двух частей, одна из которых используется для кодирования исходящих сообщений, а другая — для декодирования входящих).@ **two-part key** ключ из двух частей (постоянной и сменяемой).@ **two-part** состоящий из двух частей, двухчастевой.@ **two-party key distribution protocol** протокол распределения ключей между двумя участниками обмена сообщениями.@ **two-party** состоящий из двух участников.@ **two-pass assembler** двухпроходной ассемблер.@ **two-plus-one address** (2 + 1)-адресный.@ **two-quadranted** двухквадрантный.@ **two's complement** (точное) дополнение в двоичной системе счисления.@ **two-stage sampling** двухступенчатая выборка.@ **two-valued logic** двоичная (двухзначная) логика.@ **two-valued variable** двоичная переменная.@ **two-way circuit** дуплексный канал.@ **two-way communication** двухсторонняя связь.@ **two-way key** двухсторонний ключ (используется и для зашифрования, и для расшифрования).@ **two-way** двухсторонний.

two-level memory [tu:'levl 'meməri] двухуровневая память.@ Система памяти с двумя запоминающими устройствами различной емкости и разного быстродействия.

two-way linked list [tu:'wei lɪŋkt list] двунаправленный список. @ Связной список, каждый элемент которого связан с предшествующим и споследующим элементами.

two-way merge [tu:'wei mə:dʒ] двойное слияние.@ Алгоритм слияния двух упорядоченных файлов в один сортировочный файл.

type [taɪp] *n.* 1. тип (данных); 2. образец; *v.* 1. печатать (*на пишущей машинке*); 2. вводить, набирать; 3. выводить, печатать.@ **type 1 cryptographic product** криптографический продукт Типа 1 (по классификации NSA USA).@ **type 2 cryptographic product** криптографический продукт Типа 2 (по классификации NSA USA).@ **type box** шрифтовая коробка.@ **type check** проверять соответствие типов.@ **type declaration** описание типа.@ **type drum** цифровой барабан печатающего устройства.@ **type list** список типов, список типа.@ **type printer** буквопечатающее устройство.@ **type specification** описание типа.@ **typed language** язык с контролем типов.@ **type-in** вводить, набирать.

type checking [taɪp 'tʃekɪŋ] контроль (соответствия) типов, проверка (соответствия) типов.@ Проверка соответствия между операциями и комбинациями типов операндов, между формальными и фактическими параметрами, между левой и правой частями присваивания. Контроль типов может выполняться статически — во время трансляции, и динамически — во время выполнения программы.

type coercion [taɪp kou'ə:ʃən] приведение (типов).@ В языках с развитой системой типов данных – выполняемое транслятором преобразование типа выражения к типу, требуемому контекстом, или явно указанному типу. Приведение может включать или не включать преобразование представления значения.

type conversion [taɪp kən'veɪ:ʃən] преобразование типов.@ Операция программы, преобразующая значение одного типа в соответствующее значение другого типа.

type face [taɪp feɪs] 1. начертание шрифта.@ Вариант изображения литер одной клавиатуры, например, полужирный, курсивный. 2. шрифт.

type mismatch [taɪp mis'mætʃ] несоответствие типов.@ Ошибка в программе, вызванная нарушением правил соответствия типов.

type of data object [taɪp ɔv 'deɪtə 'ɔbʤɪkt] тип информационного объекта.@ Определение структуры объекта, разрешенных его значений и операций, которые можно над ним выполнять.

typeahead buffer ['taɪp,ə'hed 'blfə] буфер клавиатуры.@ Буфер, в который записываются символы раньше, чем они запрошены программой.

typed constant [taɪpt 'kɒnstənt] типизованная константа.@ Константа определенного типа данных. В языке со строгим контролем типов могут различаться константы, имеющие одно значение, но разные типы.

type-insensitive code [taɪp,ɪn'sensɪtɪv kɒd] программа, инвариантная к типу уравнения.@ Программа численного решения обыкновенных дифференциальных уравнений, которая должна успешно решать задачу независимо от того, является ли эта система уравнений жесткой или нежесткой.

type-out выводить, печатать (*о действиях программы*)

typical ['tɪpɪkəl] *adj.* типичный.

typically ['tɪpɪkəlɪ] *adv.* типично.

typify ['tɪpɪfaɪ] *v.* служить типичным примером (образцом); олицетворять

typing system ['taɪpɪŋ 'sɪstɪm] система типов.

U*

ultra-high [ˌʌltrə'haɪ] *adj.* сверхвысокий.@ **ultra-high frequency (UHF)** сверхвысокая частота.

unambiguous ['ʌnæm'bɪɡjuəs] *adj.* недвусмысленный, однозначный.@ **unambiguous solution** однозначное решение.@ **unambiguous decoding** однозначное декодирование.

unambiguous sentence ['ʌnæm'bɪɡjuəs 'sentəns] однозначное предложение.@ Предложение, которому соответствует ровно одно дерево вывода в порождающей язык грамматике.

unauthentic ['ʌn,ɔ:'θentɪk] *adj.* неаутентичный, фальсифицированный.@ **unauthentic message** неаутентичное (фальсифицированное) сообщение.

unauthorized ['ʌn,ɔ:θə'raɪzd] *adj.* несанкционированный (о действии, принятом без соответствующих полномочий).@ **unauthorized access** несанкционированный доступ.

unbreakability ['ʌn,breɪk,ə'bɪlɪtɪ] *n.* невскрываемость (шифра).

unbreakable ['ʌn,breɪk'eɪbl] *adj.* невскрываемый.@ **unbreakable by brute force** невскрываемый с помощью атаки с применением грубой силы.@ **unbreakable cipher** невскрываемый шифр.@ **unbreakable encryption (UBE)** невскрываемое шифрование.@ **unbreakable key** невскрываемый ключ.

unbroken ['ʌn'broukən] *adj.* невскрытый.@ **unbroken code** невскрытый код.

uncertainty ['ʌn'sə:tntɪ] *n.* неопределенность.@ **uncertainty of a secret key** неопределенность секретного ключа.

unchangeable ['ʌn'tʃeɪndʒəbl] *adj.* неизменяемый, постоянный.@ **unchangeable key** неизменяемый (постоянный) ключ.

unclassified ['ʌn'klæsɪfaɪd] *adj.* несекретный.@ **unclassified research in cryptography** несекретные исследования в области криптографии.

uncompromised ['ʌn'kɒmprəmaɪzd] *adj.* нескомпрометированный (нераскрытый).@ **uncompromised key** нескомпрометированный (нераскрытый) ключ (неизвестный противнику).

unconditionally ['ʌn,kən'dɪʃənli] *adv.* безусловно.@ **unconditionally secure authentication scheme** безусловно стойкая схема аутентификации (ее стойкость не зависит ни от вычислительной мощности, ни от времени, которыми может располагать противник).

uncrackable *adj.* = **unbreakable**

undecidable ['ʌn,dɪ'saɪdeɪbl] *adj.* нерешаемый, неразрешимый (о математической задаче).

undecipherable ['ʌn,dɪ'saɪfərəbl] *adj.* 1. не поддающийся расшифрованию (расшифровке); 2. не поддающийся дешифрованию (дешифровке).

undeciphered ['ʌn,dɪ'saɪfət] *adj.* 1. нерасшифрованный; 2. недешифрованный.

undecrypted *adj.* = **undeciphered**

undeniable ['ʌn,dɪ'naɪbl] *adj.* неоспоримый.@ **undeniable signature scheme** схема неоспоримой цифровой подписи.

under ['ʌndə] *prp.* 1. под, ниже; по; 2. в процессе.# **under consideration** рассматриваемый.# **under examination** рассматриваемый.# **under review** рассматриваемый.# **under investigation** исследуемый.# **under study** исследуемый.# **under observation** наблюдаемый.# **under test** испытываемый.# **under way** осуществляемый в данное время.

underlying ['ʌndə,lam] *adj.* 1. лежащий (размещенный) под чем-л.; 2. основной; 3. нижележащий; 4. исходный, соответствующий.@ **underlying plaintext** исходный (соответствующий) открытый текст.@ **underlying hardware** используемое оборудование; базовое оборудование.@ **underlying structure** глубинная структура; внутренняя структура.

undigested ['ʌn'daɪdʒest] *adj.* неотредактированный. @ **undigested decrypts** неотредактированные дешифровки.

unduplicatable ['ʌn'dju:plɪkɪtəbl] *adj.* неподдающийся копированию. @ **unduplicatable key** неподдающийся копированию ключ.

unencrypted ['ʌn,ɪn'kriptɪd] *adj.* незашифрованный.

unfavorable ['ʌn'feɪvərəbəl] *adj.* неразлагаемый на (простые) сомножители.

unicity ['ʌnɪsɪtɪ] *n.* единственность. @ **unicity distance** расстояние единственности (количество знаков шифртекста, необходимое криптоаналитику для вскрытия шифра).

unicity point = **unicity distance**

unidirectional *adj.* = **one-way**

uniform ['ju:nɪfɔ:m] *adj.* 1. одинаковый; однородный; равномерный; 2. постоянный, неизменный. @ **uniform acceleration** равномерное (равномерно изменяющееся) ускорение, равномерно ускоренное движение, разгон с постоянным ускорением. @ **uniform convergence** равномерная сходимость. @ **uniform distribution** равномерное распределение. @ **uniform norm** равномерная форма. @ **uniform protection** однородная защита.

uniform scaling ['ju:nɪfɔ:m skeɪlɪŋ] однородное масштабирование. @ В машинной гарфике – масштабирование с равными коэффициентами масштабирования по вертикали и горизонтали.

uniformity ['ju:nɪfɔ:mitɪ] *n.* однородность, равномерность.

uniformly ['ju:nɪfɔ:mlɪ] *adv.* однородно, равномерно. @ **uniformly distributed numbers** равномерно распределенные числа.

unilateral ['ju:nɪlətərəl] *adj.* односторонний; однобуквенный. @ **unilateral frequency distribution** распределение частот встречаемости букв (в тексте).

unique [ju:'ni:k] *adj.* 1. единственный в своем роде, уникальный, исключительный, своеобразный; 2. единый; 3. однозначный. @ **unique decryption** 1. однозначное расшифрование; 2. однозначное дешифрование. @ **unique identifier** уникальное имя; уникальный ключ.

unique name [ju:'nɪk neɪm] уникальное имя; уникальный ключ. @ Код, однозначно идентифицирующий объект вне зависимости от контекста употребления. Иногда от уникального имени требуется, чтобы имя, использованное для одного объекта, не использовалось для другого даже после уничтожения первого.

uniquely [ju:'ni:klɪ] *adv.* однозначно. @ **uniquely reversible** однозначно обратимый.

uniquely decodable (deciph-rable) [ju:'ni:klɪ dɪ'coudeɪbl] однозначно декодируемый. @ Термин, применяемый по отношению к кодам переменной длины: однозначная декодируемость гарантирует, что закодированные слова в полученном сигнале могут быть однозначно восприняты, так что процесс декодирования будет в точности противоположным процессу кодирования.

unit ['ju:nɪt] *n.* 1. (функциональное) устройство; 2. элемент, единица; 3. единица измерения; 4. модуль (программы). @ **unit distance code** 1. код с рас-

стоянием единица; 2. код с элементами, отличающимися на единицу. @ **unit distribution** распределение нормированной случайной величины. @ **unit fraction** дробь с числом единица. @ **unit measure** единица измерения. @ **unit (module) testing** модульное тестирование. @ **unit number** номер устройства. @ **unit of language** единица языка, языковая единица. @ **unit of operation** единица действия в машинном языке. @ **unit record (UR)** единичная запись. @ **unit separator (US)** разделитель элементов. @ **unit step input** входной сигнал в виде единичного скачка. @ **unit under test (UUT)** испытываемое устройство. @ **unit vector** единичный вектор.

unit address ['ju:nit ə'dres] адрес устройства. @ Число, идентифицирующее внешнее устройство для операционной системы.

united ['ju:nitɪd] *adj.* соединенный. @ **United Kingdom & United States (UKUSA)** Соединенное Королевство и Соединенные Штаты. @ **United States SIGINT System (USSS)** Система службы радиоэлектронной разведки Соединенных Штатов (включает NSA, CSS и некоторые подразделения других разведывательных ведомств USA).

unit(y) matrix ['ju:nit(ɪ) 'meɪtrɪks] единичная матрица. @ Диагональная матрица с единичными диагональными элементами.

unitary ['ju:nɪtəri] *adj.* унитарный. @ **unitary matrix** унитарная матрица. @ **unitary operator** унитарный оператор. @ **unitary semiring** унитарное полукольцо.

universal [ju:nɪ'vɜ:səl] *adj.* 1. всеобщий; всемирный; 2. для всего пригодный, универсальный. @ **universal algebra** универсальная алгебра. @ **universal character set (UCS)** универсальный набор символов. @ **Universal Decimal Classification (UDC)** Универсальная десятичная классификация, УДК. @ **universal digital computer** универсальная цифровая вычислительная машина. @ **universal digital processor industrial (UDPI)** универсальный цифровой процессор для промышленного применения. @ **universal element** универсальный элемент. @ **universal function** универсальная функция. @ **universal integrated communication (UICOM)** универсальная объединенная система связи. @ **universal key** универсальный ключ. @ **universal logic array (ULA)** универсальная логическая матрица. @ **universal logic module (ULM)** универсальный логический модуль. @ **universal power supply (UPS)** универсальный источник питания. @ **universal product code (UPC)** универсальный товарный код. @ **universal quantifier** квантор всеобщности. @ **universal synchrnous receiver/transmitter (USRT)** универсальный синхронный приемопередатчик. @ **universal synchrnous/asynchrnous receiver/transmitter (USART)** универсальный синхронно-асинхронный приемо-передатчик. @ **universal time (UT)** время по гринвическому меридиану, всемирное время. @ **universal transmitter clock (UTCLK)** синхросигнал универсального передатчика.

universal asynchronous receiver/transmitter (UART) [ju:nɪvɜ:səl eɪ'sɪŋkrənəs rɪ'si:və trænzmɪtə] универсальный асинхронный приемопередатчик (интерфейс). @ Интегральная логическая схема, преобразующая асинхронный последовательный поток данных в побайтовую параллельную форму и наоборот.

Используется при сопряжении линий передачи данных и периферийных устройств.

universal set [juːnɪˈvɜːsəl set] универсум, универсальное множество.@ Множество, (потенциально) включающее все рассматриваемые элементы.

unkeyed ['ʌnˈkiːd] *adj.* не имеющий ключей.@ **unkeyed device is unclassified** без ключей устройство несекретно.

unknown ['ʌnˈnəʊn] *adj.* неизвестный.@ **unknown key** неизвестный ключ.

unless [ənˈles] *conj.* если (только) ... не (к глаголу).# **unless otherwise mentioned (indicated, noted, specified, stated)** если не указано особо.

unlock ['ʌnˈlɒk] *v.* 1. вскрывать; 2. дешифровывать.@ **unlock a cipher** вскрывать шифр.@ **unlock information guarded by cryptography** дешифровывать защищенную криптографическими средствами информацию.

unorthodox ['ʌnˈɔːθədɒks] *adj.* оригинальный, нешаблонный.@ **unorthodox linear transform** оригинальное линейное преобразование (другое название псевдопреобразования Адамара).

unpredictable ['ʌnˈpredɪkəbl̩] *adj.* непредсказуемый.@ **unpredictable key** непредсказуемый ключ.

unpublished ['ʌnˈpʌblɪʃt] *adj.* секретный.@ **unpublished algorithm** секретный алгоритм.@ **unpublished key** секретный ключ (в криптосистеме с открытым ключом).

unravel ['ʌnˈrævəl] *v.* 1. распутывать; 2. объяснять.# **to unravel a mystery** разгадать тайну.

unreadable ['ʌnˈriːdeɪbl̩] *adj.* несчитываемый, невызываемый (из памяти компьютера или криптографического устройства).@ **unreadable key** несчитываемый ключ.

unscrambled ['ʌnˈskræmbld] *adj.* расшифрованный.

untappable ['ʌnˈtæpeɪbl̩] *adj.* защищенный от несанкционированного подключения.@ **untappable channel** канал с защитой от несанкционированного подключения.

until [ənˈtɪl] *prp.* до; *conj.* до тех пор, пока ... не (к глаголу).# **until recently** до недавнего времени.# **until then** до того времени, до тех пор.# **it was not until ... that** только в, и только когда (после).

untrustworthy ['ʌnˈtrʌstwəːθɪ] *adj.* незаслуживающий доверия.@ **untrustworthy participant** незаслуживающим доверия пользователь

unusually ['ʌnˈjuːzʊəli] *adv.* аномально.@ **unusually good simultaneous diophantine approximation (UGSDA)** аномально точные совместные диофантовы приближения.

update [ʌpˈdeɪt] *v.* обновлять.@ **update a key** обновлять ключ.

updated [ʌpˈdeɪtɪd] *adj.* обновленный.@ **updated key** обновленный ключ.

updatation [ʌpˈdeɪʃən] *n.* обновление.@ **updatation of cryptographic keys** обновление криптографических ключей.

upgrade [ʌpˈɡreɪd] *v.* модернизировать **upgrade cipher communications** модернизировать оборудование шифрсвязи.

upper ['ʌpə] *adj.* верхний; *n.* использование. @ **upper bound** верхняя граница. @ **upper of codes and ciphers** использование кодов и шифров. @ **upper of encryption** использование шифрования.

use [ju:s] *n.* 1. употребление, применение; 2. польза; *v.* использовать. # **used** + *inf.* обычно; бывало + *глагол в пр. вр.* @ **use strong cryptography** использовать стойкую криптографию. @ **use the same key in both directions** использовать один и тот же ключ для осуществления связи в обоих направлениях. # **use** используемый. # **to be of use** иметь применение. # **to make use of** использовать.

used [ju:st] *adj.* использованный. @ **used used** использованный ключ.

user ['ju:zə] *n.* пользователь. @ 1. Человек или юридическое лицо, применяющие вычислительную систему или программное средство. 2. Модуль программы или процесс, использующий средства, предоставляемые данным модулем или процессом. @ **user account** бюджет пользователя; данные о бюджете пользователя. @ **user authentication** аутентификация пользователя. @ **user guide** руководство пользователя. @ **user identification (USERID)** 1. идентификация пользователя (*для определения его полномочий*); 2. код пользователя. @ **user identification code** код пользователя. @ **user interface (UI)** интерфейс пользователя, пользовательский интерфейс. @ **user interface facilities** средства взаимодействия с пользователем. @ **user key** ключ пользователя. @ **user mode** непривилегированный режим, режим задачи. @ **user node** 1. абонент сети; 2. пользовательская станция, рабочая станция (*локальной сети*). @ **user number** код пользователя. @ **user process** пользовательский процесс, процесс пользователя. @ **user profile** параметры пользователя. @ **user state** режим пользователя, пользовательский режим. @ **user-assigned key** назначенный пользователем ключ. @ **user-defined macro** макрокоманда пользователя, определенная пользователем макрокоманда. @ **user-defined type** определенный пользователем тип (данных). @ **user-entered key** вводимый пользователем ключ. @ **user-oriented encryption** ориентированное на пользователя (учитывающее требования пользователя) шифрование. @ **user-oriented** ориентированный на пользователя. @ **user-programmable structure key** ключ с программируемой пользователем структурой. @ **user-selected key** выбранный пользователем ключ.

user-written пользовательский, написанный пользователем. @ О программе, написанной пользователем и вызываемой системной программой при определенных условиях.

user area ['ju:zə 'ɛəriə] память пользователя. @ Часть оперативной памяти, выделенная задаче пользователя.

user authorization file ['ju:zə ɔ:'θaɪ'zeɪʃən faɪl] файл информации о пользователях. @ Файл, содержащий информацию об именах, паролях и правах пользователей многопользовательской системы.

user break ['ju:zə breɪk] прерывание пользователем, прерывание от пользователя. @ Прерывание работы программы вследствие нажатия пользователем соответствующей управляющей клавиши.

user coordinates ['ju:zə kou-'ɔ:dnɪts] координаты пользователя.@ Координаты, задаваемые пользователем в системе координат, не зависящие от устройств.

user environment ['ju:zə in'vaɪənmənt] операционная среда.@ Часть операционной системы или настройка над операционной системой, предоставляющая пользователю средства непосредственного взаимодействия с прикладными программами, средства управления одновременным выполнением нескольких программ и средства информационного обмена между прикладными программами.

user group ['ju:zə gru:p] 1. организация пользователей; 2. группа пользователей.@ В развитой системе разделения времени – группа пользователей, имеющих некоторые общие ресурсы и общие права.

user manual ['ju:zə 'mænjuəl] руководство пользователя.@ Часть документации по программному продукту или устройству, описывающая его применение с точки зрения пользователя.

user of abstraction ['ju:zə ɔv 'æbstrækʃən] пользователь абстракции.@ Модуль программы, использующий абстракцию, определенную в другом модуле.

user-defined ['ju:zə,dɪ'faɪnd] определяемый пользователем.@ Об объектах или конструкциях программы, описываемых или задаваемых пользователем.

user-defined key ['ju:zə,dɪ'faɪnd ki:] 1. ключ пользователя.@ Элемент данных или группа элементов данных, указанная пользователем в качестве ключа для некоторой операции. 2. определенная пользователем клавиша.@ Клавиша клавиатуры терминала, выдающая заданную пользователем последовательность кодов или выполняющая заданную пользователем функцию.

user-friendly ['ju:zə'frendli] «дружественный».@ Об интерактивном программном средстве, обеспечивающем естественный для пользователя способ взаимодействия, защиту от ошибок и развитые средства подсказки и диалоговой документации.

user-written driver ['ju:zə'ɪtɪn 'draɪvə] драйвер пользователя.@ Драйвер для нестандартного устройства, который подключается к операционной системе и обеспечивает взаимодействие программ с этим устройством по стандартному интерфейсу.

user-authorized key = user-assigned key

user-defined key = user-assigned key

user-specific encryption = user-oriented encryption

user-to-user = end-to-end

V*

vacuum-cleaner ['vækjuəm'kli:nə] *n.* пылесос.@ "**vacuum-cleaner method**" метод "пылесоса" (позволяет перехватывать спутниковые радиопередачи с помощью наземного приемного устройства).

vain [veɪn] *adj.* тщетный, напрасный. # **in vain** напрасно.

valid ['vælid] *adj.* 1. допустимый; правильный; обоснованный; справедливый; 2. действительный, имеющий силу. @ **valid cryptogram** допустимая криптограмма.

validate [ˌvæliˈdeɪt] *v.* объявлять подлинным.

validation [ˌvæliˈdeɪʃən] *n.* 1. проверка (правильности) данных. @ Программная проверка входных параметров или вводимых данных. 2. аттестация; 3. проверка подлинности.

variable (var) ['vɛəriəbl] *n.* 1. переменная. @ Программный объект, обладающий именем и значением, которое может быть получено и изменено программой. 2. переменный, непостоянный, изменчивый; *adj.* изменяемый, переменный, регулируемый. @ **variable component** переменная составляющая. @ **variable cycle operation** работа с переменным циклом. @ **variable cycle** переменный цикл. @ **variable format** 1. переменный формат; 2. переменная длина слова. @ **variable identifier** идентификатор переменной. @ **variable instruction** переменная команда. @ **variable length format** переменная длина слова (кода). @ **variable name** имя переменной, идентификатор переменной. @ **variable range** 1. область значений переменной; 2. переменный диапазон. @ **variable type** тип переменной. @ **variable value** 1. значение переменной; 2. переменное значение. @ **variable word length** переменная длина слова (кода).

variable-length ['vɛəriəblˌleŋθ] переменной длины. @ **variable-length field** поле переменной длины. @ **variable-length instruction** команда переменной длины, инструкция переменной длины. @ **variable-length key** ключ с переменной длиной. @ **variable-length record system** система с записями переменной длины. @ **variable-size block cipher** блочный шифр с переменной длиной блока. @ **variable-width cipher** блочный шифр с переменной длиной блока.

variables generator = key stream generator

variable address ['vɛəriəbl əˈdres] адрес переменной. @ Адрес области памяти, соответствующей переменной.

variable declaration ['vɛəriəbl ˌdekləˈreɪʃən] описание переменной. @ Определение типа, размера, способа размещения и других характеристик переменной.

variable field ['vɛəriəbl fi:ld] 1. поле переменной. @ Часть команды (на языке ассемблера), предназначенная для записи имени переменной. 2. переменное поле. @ Элемент структуры данных, значение которого не постоянно. 3. поле переменной длины.

variable-length code ['vɛəriəbl ˈleŋθ koud] код переменной длины. @ Код, элементы которого имеют различную длину.

variable-length record ['vɛəriəbl ˈleŋθ ˈrekɔ:d] запись переменной длины. @ 1. Запись, длина которой может изменяться. 2. Запись файла, разные записи которого имеют разную длину.

variable-length vector ['vɛəriəbl ˈleŋθ ˈvektə] вектор переменной длины. @ Вектор, т. е. одномерный массив, который обычно имеет фиксированную

нижнюю границу, однако его верхняя граница может при этом изменяться согласно значениям, присвоенным этому массиву.

variance ['vɛəriəns] *n.* 1. дисперсия.@ Характеристика разброса случайной величины, равная среднему значению квадрата разности случайной величины и ее среднего значения. 2. среднее значение; 3. разногласие; 4. расхождение, несоответствие; 5. изменение; 6. отклонение.# **to be variance** расходиться во мнениях; противоречить.

variant ['vɛəriənt] *adj.* непостоянный.@ **variant cipher system** 1. непостоянная шифрсистема (с неравновероятными ключами); 2. вариантная шифрсистема (при зашифровании каждый символ открытого текста может заменяться на разные символы шифрованного).

variant *n.* = **modification**

variation *n.* = **modification**

variety [və'raɪəti] *n.* 1. разнообразие; 2. ряд, множество разнообразных (явлений и т. п.); 2. разновидность; вид.# **a variety of** целый ряд.# **for a variety of reasons** по ряду причин.

vector ['vektə] *n.* 1. вектор; 2. одномерный массив.@ Одномерный массив (вектор) широко используется в вычислительной технике, поскольку память представляет собой вектор слов. Способ записи векторов определяется языком программирования. *adj.* векторный.@ **vector algebra** векторная алгебра.@ **vector computer** векторный процессор; векторная ЭВМ.@ **vector descriptor** дескриптор массива, паспорт массива.@ **vector field (VF)** векторное поле.@ **vector function** векторная функция.@ **vector information** векторная информация.@ **vector norm** норма вектора.@ **vector processor** векторный процессор.@ **vector space** векторное пространство.

vector generator ['vektə 'dʒenəreɪtə] генератор векторов.@ Функциональное устройство.

vector graphics ['vektə g'ræfiks] векторная графика.@ Графика с представлением изображения в виде совокупности отрезков прямых (векторов).

vector processing ['vektə 'prəʊsesɪŋ] векторная обработка.@ Единообразная обработка последовательностей данных.

vectored interrupts ['vektəd ɪntə'rʌpts] векторные прерывания.@ Метод прерывания, реализуемый аппаратно при работе с множеством разнотипных устройств, каждое из которых способно формировать сигналы прерывания, причем для каждого типа устройства требуется своя программа обработки прерываний. Вектор прерываний – это массив таких программ.

vehicle ['vi:kl] *n.* 1. любое средство передвижения; 2. средство (способ) распространения (передачи); 3. среда; проводник.# **test vehicle** модель для испытаний.

vein [veɪn] *n.* 1. вена; 2. жилка, склонность; тенденция.# **in the same vein** в том же роде.

Venona decrypts дешифровки Веноны.

venture ['vɛntʃə] *n.* 1. рискованное предприятие; 2. попытка; *v.* рискнуть, отважиться, осмелиться (**on, upon**).# **at venture** наугад; наудачу.# **to run the venture** рисковать.

verification [ˌverɪfɪ'keɪʃən] 1. верификация.@ Формальное (обычно полуавтоматическое) доказательство правильности программы, использующее предусловия и постусловия для процедур и операторы контроля. 2. контроль, проверка (вводимых оператором данных).@ **verification condition** условие верификации.

verification and validation (V and V) [ˌverɪfɪ'keɪʃən ænd ˌvælɪ'deɪʃən] (приемочные) испытания.@ Всесторонняя проверка и тестирование системы, обычно при сдаче в эксплуатацию. «Verification» обычно относится к формальной проверке, а «validation» – общей субъективной оценке.

verifier ['verɪfaɪə] *n.* 1. верификатор, программа верификации; 2. программа контроля; 3. устройство контроля.

verify ['verɪfaɪ] *v.* 1. верифицировать; 2. проверять; 3. подтверждать; удостоверить.@ **verify a key** проверять подлинность ключа.@ **verify an authenticates** проверять аутентификатор.

Vernam cipher шифр Вернама.

version ['vɜːʃən] *n.* 1. версия.@ 1. Вариант программного продукта; 2. Файл, являющийся модификацией другого файла. 2. версия, толкование; вариант.@ **version number** номер версии.@ **version rollback attack** атака методом возврата к старой версии (разновидность криптоаналитической атаки против шифрсистемы, в которой для устранения ошибок были сделаны необходимые исправления, однако в целях совместимости оставлена возможность использования алгоритмов и протоколов более ранних версий).

version control ['vɜːʃən kən'troul] управление версиями.@ Управление созданием или использованием различных вариантов какого-либо объекта.

vertical ['vɜːtɪkəl] *adj.* вертикальный.@ **vertical check** вертикальный контроль.@ **vertical microinstruction** вертикальная микрокоманда.@ **vertical parity** продольный контроль четности.@ **vertical processor** процессор с вертикальным микропрограммированием.@ **vertical recording** вертикальная запись, перпендикулярная запись.@ **vertical scale (VS)** вертикальная шкала.@ **vertical spacing** интервал строк.@ **vertical substitution cipher** шифр вертикальной (колонной) замены.@ **vertical window (VWindow)** вертикальное окно.

vertical format unit (VFU) ['vɜːtɪkəl 'fɔːmæt 'juːnɪt] блок форматирования по вертикали.@ Часть электронного блока управления печатающим устройством, которая управляет вертикальным форматированием печатаемого документа.

vertical microprogramming ['vɜːtɪkəl 'maɪkrou'prougræmɪŋ] вертикальное микропрограммирование.@ Способ микропрограммирования, при котором микрокоманда задает отдельную микрооперацию над одним или двумя регистрами. Вертикальные микрокоманды состоят из нескольких бит и преобразуются в горизонтальные микрокоманды дешифратором микрокоманд.

vertical redundancy check ['və:tɪkəl rɪ'dʌndənsɪ tʃek] продольный контроль.@ Контроль за счет избыточности, при котором контрольная величина вычисляется для целого блока данных.

vertically ['və:tɪkəli] *adv.* вертикально.

vicinity [vi'sɪnɪti] *n.* 1. окрестности; 2. соседство, близость.# **in the vicinity of** около; в районе.

video ['vɪdeəu] *n.* видеосигнал.@ **video encryption** шифрование видеосигналов.

view [vju:] *n.* 1. представление.@ Представление о базе данных с точки зрения отдельного пользователя или прикладной программы. Обычно оформляется в виде подсистемы. 2. вид, видимое изображение; 3. проекция; *v.* обозревать, рассматривать.# **view point** точка зрения.# **point of view** точка зрения.# **in view of** в виду.# **object in view** поставленная цель.# **overall view** общее представление.# **with a view to** с целью; с тем, чтобы.# **with the view of** с целью; с тем, чтобы.# **with this end in view** с этой целью.# **to bring into view** обратить внимание.

Vigenere cipher шифр Вижинера.

Vigenere square квадрат Вижинера.

Vigenere table = **Vigenere square**

violate ['vaɪələt] *v.* нарушать.@ **violate matrix encryption** виртуально-матричное шифрование.@ **violate secrecy or privacy** нарушать секретность или конфиденциальность.

virtual ['vɜ:tʃuəl] *adj.* 1. виртуальный.@ Не имеющий физического воплощения или воспринимаемый иначе, чем реализован.@ **virtual block number** виртуальный номер блока.@ **virtual call** виртуальный вызов.@ **virtual device** виртуальное устройство.@ **virtual memory system (VMS)** система виртуальной памяти.@ **virtual memory (VM)** виртуальная память.@ **virtual storage interrupt** прерывание по отсутствию страницы.@ **virtual storage management** управление виртуальной памятью.@ **virtual value** действующее значение.@ **virtual-device interface (VDI)** интерфейс виртуального устройства.

virtual address ['vɜ:tʃuəl ə'dres] виртуальный адрес.@ Адрес ячейки виртуальной памяти; адрес виртуального объекта.

virtual address mode ['vɜ:tʃuəl ə'dres moud] режим виртуальной адресации.@ Режим работы процессора, при котором исполнительные адреса считаются виртуальными адресами и специальным образом преобразуются в физические.

virtual call service ['vɜ:tʃuəl kɔ:l 'sə:vɪs] служба виртуальных вызовов.@ В сети с коммутацией пакетов: техника образования виртуального соединения между терминалами, предшествующего передачи пользовательских данных.

virtual circuit ['vɜ:tʃuəl 'sə:kɪt] виртуальный канал.@ В сети коммутации пакетов – средства, обеспечивающие передачу пакетов между двумя узлами с сохранением исходной последовательности, даже если пакеты пересылаются

по различным физическим маршрутам. Виртуальный канал устанавливается при вызове и аннулируется после сеанса связи.

virtual connection ['və:tjuəl kə'nekʃən] виртуальное соединение.@ Логическое соединение между двумя точками линии передачи в сети, которое для окончательного оборудования выглядит как физическое соединение (обычно с некоторой задержкой).

virtual console ['və:tjuəl kən'soul] 1. виртуальный терминал.@ В многозадачной однопользовательской системе – средства одновременного запуска нескольких интерактивных программ при наличии одного терминала, предоставляющее каждой задаче отдельное окно и позволяющее пользователю переключаться между ними. 2. виртуальный пульт, виртуальная консоль.@ Терминал, временно используемый в качестве операторского (при наладке или отладке системы).

virtual derived data item ['və:tjuəl di'raɪvd 'deɪtə 'aɪtəm] виртуальный производный элемент данных.@ В сетевых базах данных – основной производный элемент данных.

virtual dick ['və:tjuəl disk] виртуальный диск.@ Логическое устройство, с которым программа взаимодействует как с диском, но соответствующее физическое устройство может быть не диском, а, например, лентой, областью оперативной памяти или областью физического диска.

virtual file ['və:tjuəl faɪl] виртуальный файл.@ Совокупность данных, к которым программа обращается операциями файлового обмена. Физически виртуальный файл может быть частью реального файла, или объединением группы реальных файлов, или являться средством межзадачного взаимодействия.

virtual image (vir) ['və:tjuəl 'ɪmɪdʒ] 1. мнимое изображение; 2. виртуальное изображение.@ Графическое представление, соответствующее всему закодированному изображению. Отображаемое изображение является, как правило, частью виртуального изображения.

virtual machine ['və:tjuəl mə'ʃi:n] виртуальная машина.@ Средство многозадачной операционной системы, предоставляющее каждой задаче функциональный эквивалент вычислительной системы.

virtual result data item ['və:tjuəl rɪ'zʌlt 'deɪtə 'aɪtəm] элемент данных – виртуальный результат.@ Виртуальный производный элемент данных, значения которого являются функцией значений других элементов данных.

virtual source data item ['və:tjuəl sɔ:s 'deɪtə 'aɪtəm] элемент данных – виртуальная копия источника.@ Виртуальный производный элемент данных, значения которого являются копией значения другого элемента данных.

virtual space ['və:tjuəl speɪs] виртуальное пространство.@ В машинной графике - пространство, в котором координаты элементов изображения выражены в не зависящим от устройства виде (в координатах пользователя).

virtual storage ['və:tjuəl 'stɔ:ɹɪdʒ] виртуальная память.@ Предоставляемая программе вычислительной системе возможность работать с памятью, размер

которой больше физической памяти используемой ЭВМ. Физическая память разбивается на блоки фиксированной длины (страницы) или переменной длины (сегменты). В основной (оперативной) памяти расположены используемые в данный момент данные и команды, образующие рабочее множество процесса или задачи. Виртуальные адреса, указанные в программе, преобразуются в физические адреса с помощью таблицы страниц или таблицы сегментов. Если виртуальный адрес не принадлежит рабочему множеству, происходит прерывание по отсутствию страницы, и нужная страница или сегмент подкачиваются из внешней памяти; при этом освобождается сегмент или страничный блок в оперативной памяти, и его содержимое сохраняется на внешнем устройстве.

virtual storage access method (VSAM) ['və:tjuəl 'stɔ:riɔz 'ækses 'meθəd] виртуальный метод доступа. @ Метод доступа OS IBM, обеспечивающий операции индексно-последовательного доступа вне зависимости от физической организации файла.

virtual storage allocation ['və:tjuəl 'stɔ:riɔz 'æləkeɪʃən] распределение виртуальной памяти. @ Распределение сегментов или страничных блоков основной памяти данных рабочих множеств процессов и пространства внешней памяти для их подкачки.

virtual telecommunication access method (VTAM) ['və:tjuəl 'telɪkəmjʊ:ni'keɪʃən 'ækses 'meθəd] виртуальный телекоммуникационный метод доступа. @ Метод доступа для работы с терминалом, обеспечивающий единообразную работу с различными физическими терминалами. Программы метода доступа переводят универсальные операции в команды конкретного устройства.

virtual terminal ['və:tjuəl 'tə:mɪnəl] виртуальный терминал. @ Обобщенный протокол взаимодействия для работы с реальными терминалами, принятый в вычислительной системе. Виртуальный терминал использует параметры терминала для преобразования универсальных команд в команды управления конкретным терминалом.

virtually ['və:tjuəli] *adv.* 1. виртуально; 2. фактически.

virtue ['vɜ:tju:] *n.* 1. добродетель, достоинство; 2. сила; 3. свойство. # **by (in) virtue of** благодаря (чему-л.); посредством (чего-л.); в силу, на основании (чего-л.).

vision ['vɪʒən] *n.* 1. зрение; 2. проникновение, проницаемость, предвидение; 3. вид. # **beyond our vision** вне нашего поля зрения.

visual ['vɪʒuəl] *adj.* визуальный, видимый. @ **visual cryptography** криптография для защиты изображений. @ **visual display** 1. экран визуального устройства вывода; 2. видимое изображение. @ **visual display terminal (VDT)** видеотерминал. @ **visual display unit (VDU)** устройство визуального отображения.

very ['vɛrɪ] *adj.* истинный, настоящий; *adv.* очень. @ **very large-scale integration logic (VLSI) implementation of a cryptoalgorithm** СБИС-реализация криптоалгоритма.

vocoder ['vɒkəʊdər] *n.* вокодер. @ Устройство компактного цифрового кодирования речи.

vocoding ['vɒkəʊdɪŋ] *n.* кодирование речевых сигналов.

vogue [voug] *n.* 1. мода; 2. популярность. # **to be in vogue** быть популярным.

voice [vɔɪs] *n.* телефонная (радиотелефонная) связь. @ **voice (grade) channel** речевой канал. @ **voice communication** речевая связь. @ **voice cryptography** криптограф для защиты телефонных переговоров. @ **voice encryption device** телефонный шифратор. @ **voice frequency (VF)** тональная частота. @ **voice input device** устройство речевого ввода. @ **voice scrambler device** телефонный скремблер. @ **voice security device** устройство засекречивания телефонных переговоров. @ **voice-mail encryption** шифрование речевых сообщений в системе электронной почты.

volume ['vɒljəm] *n.* 1. том. @ Носитель данных внешнего запоминающего устройства, обрабатываемый как единое целое; например, дисковый пакет, дискета, катушка магнитной ленты. 2. объем; масса; 3. пространство; 4. книга; том. @ **volume label** метка тома. @ **volume of traffic** объем трафика. @ **volume serial number (VOLSER)** номер тома (в многотомном файле). @ **volume table of contents (VTOC)** каталог тома.

volume identifier ['vɒljəm aɪ'dentɪfaɪər] идентификатор тома. @ Текстовое имя носителя данных – диска или магнитной ленты.

VORTEX = CHALET

vowel ['vaʊəl] *n.* буква, обозначающая гласный звук. @ **vowel-consonant relationship** взаимосвязь между буквами, обозначающими гласные и согласные звуки.

Voynich manuscript рукопись Войнича (манускрипт, приобретенный Войничем в Италии и содержащий шифрованный текст на неизвестном языке, который не поддается прочтению).

vulnerability ['vʌlnərəbɪlɪtɪ] *n.* уязвимость, слабость. @ **vulnerability of a cipher system** уязвимость шифрсистемы.

vulnerable ['vʌlnərəbl] *adj.* уязвимый, слабый. @ **vulnerable to a chosen-ciphertext attack** уязвимый по отношению к атаке на основе выбранного шифртекста. @ **vulnerable to break-ins** уязвимый против взлома.

W*

wake [weɪk] *n.* употребляются в выражении: # **in the wake (of)** вслед за.

Wassenaar Arrangement (WA) Вассенаарское соглашение (договор, подписанный 33 странами-участницами в июле 1996 г. в Голландском городе Вассенааре (**Wassenaar** = **Wassenaar**), о мерах по контролю над экспортом вооружений, а также технологий и товаров двойного назначения, включая стойкие средства шифрования).

Walsh transform (WT) преобразование Уолша.

Walsh-Hadamard transform (WHT) преобразование Уолша-Адамара.

want [wɒnt] *n.* 1. недостаток; отсутствие; 2. необходимость; нужда; *v.* 1. желать, хотеть; 2. недоставать; 3. нуждаться (**for**).# **for want of** из-за отсутствия.# **to be wanting** недоставать, отсутствовать.

way [weɪ] *n.* 1. путь; 2. способ; образ действия.# **way out** выход из создавшегося положения.# **by way of** в качестве; с целью; через; посредством, путем.# **by the way** между прочим.# **either way round** любым путем.# **in a way** в некотором отношении; в известном смысле; до некоторой степени.# **in a minor way** незначительно.# **in a rough way** приблизительно.# **in every way** во всех отношениях.# **in no way** никоим образом, никак.# **in one way or another** так или иначе.# **in such a way** так, чтобы.# **in the way of** в отношении.# **in this way** таким образом.# **one way or another** так или иначе.# **the other way** иначе.# **the other way round** наоборот.# **in other ways** в других отношениях.# **under way** осуществляемый в данное время.# **to be in the way** мешать.# **to be under way** проводится, быть в процессе выполнения.# **to give way to** уступать (место); поддаваться.# **to put the other way round** другими словами.

weak [wi:k] *adj.* слабый, нестойкий, вырожденный.@ **weak convergence** слабая сходимость.@ **weak key** нестойкий (вырожденный) ключ.

weak entity [wi:k 'entɪtɪ] слабая сущность, слабый объект.@ В моделях данных – объект, существование которого определяется наличием объектов, с которыми он связан.

weak external reference [wi:k eks'tɜːnl 'refrəns] слабая внешняя ссылка.@ Внешняя ссылка, получающая при компоновке значение только при наличии других ссылок на то же имя.

weaken ['wi:kən] *v.* ослаблять; понижать (стойкость шифра).@ **weaken a cipher unit** понижать стойкость криптоблока.

weakened ['wi:kənt] *adj.* ослабленный (по стойкости).@ **weakened DES** ослабленный DES алгоритм.

weakest precondition ['wi:kɪst pri:kən'dɪʃən] слабейшее предусловие; слабейшее входное условие.

weaking ['wi:kɪŋ] *n.* ослабление, ослабевание; снижение стойкости.

weakness ['wi:knis] *n.* слабость (снижающая стойкость шифра).@ **weakness of a cipher** слабость в шифре.

wear ['weə] *n.* износ.# **wear and tear** износ и разрыв.

weather ['weðə] *adj.* относящийся к погоде.@ **weather cipher** шифр для засекречивания прогноза погоды (применялся немецкими военными кораблями и подводными лодками во время второй мировой войны).

weather codebook = weather cipher

"Wehrmacht" "Enigma" "Энигма" "вермахта"

"Wehrmacht" *n.* нем. "вермахт" (сухопутные вооруженные силы Германии в 20-е - 40-е годы)

weight [weɪt] *n.* 1. вес, весовой коэффициент, тяжесть, весовая функция; 2. груз; 3. значение, влияние.# **dead (sole) weight** собственный вес, вес конструкции.

well [wel] *adv.* 1. хорошо, с успехом; 2. довольно, вполне; 3. значительно; 4. достаточно, как раз. @ **well-resourced attack** атака со стороны хорошо оснащенного противника. # **well above** значительно выше. # **well after** значительно позже. # **well in advance** значительно раньше. # **well nigh** почти. # **well over** значительно больше. # **as well** также; с таким же успехом. # **as well as** а также и; так же как и. # **it may well be** вполне возможно.

wheel [wi:l] *n.* колесо, ротор, шифрдиск.

whether ['weðə] *conj.* ли. # **whether ... or** или ... или; независимо от. # **whether it be** будь то.

which [wɪtʃ] *pron.* который; какой; кто; *conj.* который, какой; что

while [waɪl] *conj.* 1. в то время, как; пока; 2. несмотря на то, что; тогда как; хотя; *n.* время, промежуток времени. # **after a while** через некоторое время. # **for a while** на время. # **once in a while (way)** редко, изредка.

whispers ['wɪspəz] *n.* шуршание (звуки, издаваемые радиопередатчиком непосредственно перед посылкой зашифрованного сообщения).

white [waɪt] *adj.* белый. @ **white noise** "белый шум" (зашумление). @ **white noise encryption** шифрование "белым шумом"/зашумлением). @ **white-noise-based random generator** генератор случайных чисел на основе источника "белого шума" (зашумления).

whole ['houl] *adj.* 1. весь, целый; 2. цельный; *n.* 1. целое; 2. все. @ **whole multiple** целое (кратное). # **as a whole** в целом. # **on (upon) the whole** в целом; в общем.

wide [waɪd] *adj.* широкий. # **far and wide** повсюду. # **wide apart** на большом расстоянии друг от друга.

wideband ['waɪdbænd] *adj.* широкополосный. @ **wideband encryption** широкополосное шифрование речи (речевых сигналов).

will [wɪl] *n.* 1. воля; 2. желание. # **at will** по желанию; произвольно.

wireless ['waɪələs] *n.* радио, радиоприемник; *adj.* беспроводный, беспроводной. @ **wireless communication** радиосвязь. @ **wireless conversations** переговоры по радио. @ **wireless interception** радиоперехват. @ **wireless interceptor** оператор радиоперехвата. @ **wireless link** радиолиния. @ **wireless silence** радиомолчание.

wiretap ['waɪətæp] *n.* перехват, прослушивание; *v.* перехватывать, прослушивать (посредством подключения к проводному каналу связи, несанкционированного его пользователями). @ **wiretap attack secure** защищенный от атаки с перехватом информации посредством подключения к проводной линии связи. @ **wiretap attack** атака с перехватом информации посредством подключения к проводной линии связи. @ **wiretap law** закон о прослушивании.

wiretapped ['waɪətæpt] *adj.* перехваченный посредством подключения к проводной линии связи. @ **wiretapped ciphertext** шифртекст, перехваченный посредством подключения к проводной линии связи.

wiretapping *n.* = **wiretap**

wise [waɪz] *adj.* 1. мудрый; 2. целесообразный; *adv.* в сочетании с существительным образует наречие, например: **clockwise** по часовой стрелке; *n.* способ. # **in no wise** никоим образом.

wit [wɪt] *n.* 1. ум, разум; 2. употребляется в выражении: **to wit** а именно
with [wɪð] *prp.* 1. с; 2. в зависимости от; 3. у; в случае; 4. если; 5. при; 6. несмотря на. # **with few exceptions** за немногими исключениями.

within [wɪð'in] *prp.* 1. в пределах; 2. в, внутри; *adv.* внутри. # **within a matter of 3 hours** в течение 3-х часов. # **within recent years** за последние годы. # **within the limits (range)** в пределах, в диапазоне.

without [wɪð'out] *prp.* 1. без; 2. вне, за; 3. не; без того, чтобы (*перед ing-form*). # **without fail** непременно, обязательно. # **from without** извне.

withstand [wɪð'stænd] *v.* противостоять. @ **withstand a targeted attack** противостоять целенаправленной атаке. @ **withstand cryptanalysis** противостоять криптоанализу.

word [wɜ:d] *n.* слово. @ **word pattern** распределение слов (в тексте). @ **word-length aperiodic** апериодичный шифр многоалфавитной замены с пословной сменой алфавита. @ **word-usage frequency** частота употребления слов (в тексте).

work [wɜ:k] *n.* работа; *v.* 1. работать; 2. действовать; 3. разрабатывать (*out*); 4. оправдывать себя, например: **this idea work** эта идея себя оправдывает; *n.* работа; труд; занятие. @ **work characteristic reduction field** поле снижения рабочей характеристики (часть криптограммы, где хранится информация, которая позволяет снизить криптостойкость используемого шифра). @ **work characteristic** характеристика криптостойкости шифра (рабочая характеристика или коэффициент трудоемкости) (объем работы, которую надо выполнить для вскрытия шифра). @ **work on a cipher system** работа над вскрытием шифрсистемы. @ **work on the cryptanalysis of a cipher** заниматься криптоанализом шифра, работать над вскрытием шифра. # **to be at work** работать, действовать.

work key = working key

work factor (WF) = work characteristic

work factor reduction field (WFRF) = work characteristic reduction field

work function (WF) = work characteristic

working ['wɜ:kɪŋ] *adj.* рабочий, действующий. @ **working key** рабочий (действующий) ключ.

world [wɜ:ld] *adj.* мировые; всемирные. @ **World-Wide Web (WWW)** Всемирная информационная система ("Всемирная паутина").

world coordinates [wɜ:ld kou'ɔ:dnɪts] мировые координаты. @ Не зависящая от устройства декартова система координат, используемая программой для задания графических данных.

worst [wɜ:st] *adj.* наихудший, самый плохой. @ **worst case conditions** наихудшие условия (наихудшие для разработчика шифрсистем условия, при которых может производиться ее криптоанализ: (а) полное знание этой шифрсистемы противником; (б) наличие у противника достаточного объема перехваченного шифртекста; (в) знание противником отдельных отрезков открытого и

соответствующего ему шифрованного текстов).# **at worst** в (самом) худшем случае.

wrong [rɒŋ] *adj.* 1. неправильный, ошибочный; 2. несправедливый.@ **wrong key** неправильный (несоответствующий) ключ.

wrongly ['rɒŋli] *adv.* неправильно.@ **wrongly-entered key** неправильно введенный ключ.

X*

X-band ['eks,bænd] *n.* X диапазон.

X-distribution ['eks'distribution] *n.* X распределение.

X-text ['eks'tekst] *n.* зашифрованный текст, шифртекст.

Y*

year [jə:] *n.* год.# **year by year** каждый год.# **year in, year out** из года в год.# **from year to year** с каждым годом.

Z*

Zendian *adj.* зендийский (Zendia).@ **Zendian cipher** зендийский шифр.

zero ['ziərou] *adj.* нулевой; *n.* нуль.@ **zero information** нулевая информация.@ **zero initial condition** нулевое начальное условие.@ **zero insertion** вставка нулей, вставка битов.@ **zero level** нулевой уровень (уровень кода 0).@ **zero order** нулевой порядок.@ **zero-knowledge iterative proof (ZKIP)** итеративное доказательство с нулевым разглашением (конфиденциальной информации).@ **zero-knowledge proof (ZKP)** доказательство с нулевым разглашением (конфиденциальной информации).@ **zero-knowledge protocol (ZKP)** протокол обмена с нулевым разглашением (конфиденциальной информации).@ **zero-one distribution** распределение нулей и единиц.

zero flag ['ziərou flæg] признак нуля.@ Разряд слова состояния процессора, устанавливаемый в зависимости от равенства нулю результата последней арифметической или логической операции.

zeroization ['ziərouizeɪʃən] *n.* обнуление (процесс удаления ключа из криптографического оборудования или устройства ввода ключей).

zeroize ['ziərouɪz] *v.* обнулять (удалять ключ из криптографического оборудования или устройства ввода ключей).

Zimmermann telegram телеграмма Циммермана (прочитанная англичанами немецкая шифртелеграмма, содержание которой оказало существенное влияние на решение USA принять участие в первой мировой войне на стороне Антанты); 2. Циммерман Ф. (автор программы шифрования "PGP").

ИМЕНА СОБСТВЕННЫЕ

"Abwehr" нем. "абвер" (немецкая военная разведка во время второй мировой войны).

Adams Адамс К. (один из разработчиков блочного алгоритма шифрования КАСТ).

Adelman Адельман (американский криптолог)

Agnes Агнесса (название электромеханического устройства, которое во время второй мировой войны использовалось сотрудниками английской дешифровальной службы для автоматизации процесса вскрытия немецкой шифровальной машины "Энигма").

Alberti Альберти Л. (итальянский криптолог, автор самой старинной из сохранившихся на Западе рукописей, посвящённых криптоанализу)

"Alice" "Алиса" (гипотетическая личность, выполняющая необходимые действия при реализации криптографических протоколов).

Andreyev Андреев Н. (генерал КГБ, в 60-е – 70-е годы возглавлявший одно из главных управлений КГБ, в состав которого входили подразделения радиоразведки).

"Asiacrypt" "Азиякрипто" (название конференции по криптологии, которая проводится в Азиатско-Тихоокеанском регионе).

Beale Биль Т. (американский авантюрист, который, накопив вместе с сообщниками огромные сокровища, зарыл их где-то на территории штата Виржиния и с помощью трех шифров засекретил: (а) местонахождение этих сокровищ; (б) их подробное описание; (в) имена законных наследников).

Beaufort Бофор Ф. (адмирал английского флота).

Beurling Бёрлинг А. (известный шведский криптоаналитик, на счету которого имеется несколько успешных вскрытий советских и немецких шифров в 30 – 40 г.).

"Beurling code" "библейский" код (согласно гипотезе израильского математика Ильи Рипса, Библия содержит кодированный текст, дешифровав который можно узнать многое о событиях, произошедших спустя тысячи лет после ее написания).

"Big Brother" "Большой Брат" аллегория тотальной слежки со стороны государства за своими гражданами из романа английского писателя Дж. Оруэлла "1984".

Bletchley Park (BP) Блетчли-Парк (поместье викторианской эпохи примерно в 100 км от Лондона, где в годы Второй мировой войны находился английский дешифровальный центр, занимавшийся чтением немецкой шифрпереписки).

Bob Боб (гипотетическая личность, выполняющая необходимые действия при реализации криптографических протоколов, в которых имеется по крайней мере два участника).

"Bombe" "Бомба" название электромеханического устройства, созданного в годы Второй мировой войны англичанами для вскрытия немецкой шифровальной машины "Энигма".

Boole (George Boole) Буль Джордж (английский математик).

Caesar Цезарь Ю. (древнеримский император).

"CANYON" "Каньон" (серия разведывательных спутников NSA USA, первый из которых был выведен на орбиту в 1968 г.).

"CHALET" "Шале" (серия разведывательных спутников NSA USA, первый из которых был выведен на орбиту в 1978 г.).

Cheltenham Челтнем (курортный город в графстве Глостершир в Англии, где находится штаб-квартира ЦПС).

"Colossus" = **"Colossus"**

"Colossus" "Колосс" (название электронно-механического устройства, созданного в годы второй мировой войны англичанами для автоматизации процесса вскрытия немецкой шифровальной машины "Энигма").

"Crypto" "Крипто" (название ежегодной международной конференции по криптологии).

"Crypto A.G." "Крипто А.Г.." (одна из самых известных в мире фирм по производству коммерческих шифраторов).

"Cryptobytes" "Криптобайты" (периодический информационный бюллетень публикуемый американской компанией "RSA Laboratories").

"Crypto-Gram" "Крипто-Грамма" (ежемесячный криптоюгический информационный бюллетень, распространяемый в электронном виде среди пользователей, глобальной компьютерной сети "Интернет").

"Cryptologia" "Криптология" (ежеквартальный криптологический журнал выходящий в USA)

Cipher Bureau Шифровальное бюро (правительственное криптоаналитическое ведомство в Польше в период между двумя мировыми войнами).

Diffie Диффи У. (американский криптолог, один из родоначальников криптографии с открытым ключом).

Doyle Дойл А. К. (английский писатель, автор рассказа "Пляшущие человечки", в котором описано оригинальное криптоаналитическое исследование шифрованного текста).

Dreyfus Дрейфус А. (французский офицер, которому в 1894 г. было предъявлено обвинение в шпионаже в пользу Германии, при этом одной из основных улик послужила частично дешифрованная телеграмма итальянского военного атташе во Франции).

Dunlop Данлоп Дж. (американский сержант, служивший курьером в NSA в 50-е – 60-е годы и продававший секретную информацию об американских шифрах советской разведке).

"Echelon" "Эшелон" (комплекс технических средств, предназначенный для перехвата телефонных разговоров, электронной почты и телекоммуникационных сообщений с отбором по заданным ключевым словам и фразам)

Elgar (1857 – 1934) Элгар Э. (английский композитор, автор музыкального произведения под названием "Вариации на тему Энигмы", под влиянием которого немецкий инженер А Шербиус окрестил изобретенную им шифровальную машину "Энигмой").

Euler (1707 – 1783) Эйлер Л. (русский ученый математик).

Eurocrypt Еврокрипто (конференция по криптологии, с 1982 г. ежегодно проводимая в одной из европейских стран).

Feistel Фейстел Х. (американский криптограф, автор многочисленных криптографических патентов, в том числе алгоритма шифрования "Люцифер").

Fermat (1601 – 1665) Ферма П. (французский математик).

Fetterlein Феттерлейн Э. (русский криптоаналитик, после Октябрьской революции эмигрировавший в Англию).

Fibonacci (Leonardo Pisano) (1180 – 1240) Фибоначчи (итальянский математик).

Fort Meade Форт-Мид (город в американском штате Мэриленд, где расположена штаб-квартира NSA USA).

"Fortezza" "Фортецца" (название модельного ряда PCMCIA-карт, которые реализуют криптографические алгоритмы, разработанные в рамках американской правительственной программы "Кэпстоун").

Fourier (1768 – 1830) Фурье Ж. (французский математик).

Friedman Фридман У. (американский военный криптолог, незадолго до начала второй мировой войны вскрывший японскую "пурпурную" шифровальную машину).

"Gadsby" "Гэдсби" (роман американского писателя Э Райта, в котором нет ни единого слова, содержащего букву **e** английского алфавита)

Galois (1811 – 1832) Галуа Э. (французский математик).

Gifford Гиффорд Д. (сотрудник Массачусетского технологического института).

Golomb Голомб С. (американский криптолог).

Gouzenko Гузенко И. (шифровальщик посольства СССР в Оттаве, в 1945 г. попросивший политического убежища в Канаде и оказавший американцам существенную помощь в работе над вскрытием криптосистем, которые использовались для засекречивания переписки резидентуры советской разведки в Вашингтоне с Москвой).

Hadamard (1865 – 1963) Адамар Ж. (французский математик).

Hagelin Хагелин Б. (основатель и владелец швейцарской компании "Крипто А Г." - одной из самых известных в мире фирм по производству коммерческих шифраторов).

Hamming Хэмминг Р. (американский математик).

Hellman Хеллман М. (американский криптолог, один из родоначальников криптографии с открытым ключом).

Hill Хилл Л. (американский криптолог).

"Ivybells" "Вьюнок" (кодовое название радиоразведывательной операции, в ходе которой в конце 70-х годов NSA USA удалось подключиться к советскому коммуникационному кабелю, проложенному по дну Охотского моря для поддержания связи между материком и полуостровом Камчатка).

Jefferson (1743 – 1826) Джефферсон Т. (третий по счету президент USA).

Jevons (1835 – 1882) Джевонс У. (английский математик).

Kahn Кан Д. (американский писатель, автор фундаментальной монографии по истории криптологии под названием "Взломщики кодов").

Kasiski Казиский Ф. (немецкий криптолог).

Kerckhoff Керкхофф А. (голландский криптолог).

"Lucifer" "Люцифер" (название алгоритма шифрования, положенного в основу DES-алгоритма).

"Magic" "Магия" (условное наименование источника разведывательной информации, которую американские криптоаналитики добывали путем дешифрования японской шифрпереписки в 30-е – 40-е годы).

Makarov Макаров В. (сотрудник 16 управления КГБ, с 1985 по 1987 г. работавший на английскую разведку).

Markov МАРКОВ Андрей Андреевич (1856 – 1922) (русский математик).

Maslov Маслов И. (начальник 16 правления КГБ).

Massey Месси Дж. (американский криптолог).

Merkle Меркль Р. (американский криптолог, один из авторов метода "сведения к середине").

Mersenne (1588 – 1648) Мерсенн Марен (французский физик).

"Microsoft" "Майкрософт" (американская корпорация, крупнейший в мире производитель программного обеспечения).

Petsamo Петсамо (город в Финляндии, в котором в июне 1941 г. финские войска захватили кодовую книгу и другие криптографические материалы, принадлежавшие советскому консульству).

Playfair Плейфейер (английский политический деятель, член палаты лордов парламента Англии).

Poe ПО Эдгар Аллан (1809 – 1849) (американский писатель и криптолог-любитель).

Porta Порта Дж. (итальянский криптолог, который предвосхитил всех других специалистов, описав в своем трактате то, что считается вторым в значимости приемом в современном криптоанализе).

"Production" "Производство" (подразделение NSA USA, специализирующееся на вскрытии шифрсистем и чтении шифрпереписки).

"Rainbow Series" "Радужная серия" (серия дополнений к "Оранжевой книге", названная так по цвету ее обложек).

Rejevski Режевский М. (польский криптоаналитик, внесший наибольший вклад во вскрытие поляками немецкой шифровальной машины "Энигма" перед второй мировой войной).

Rip van Winkle Рип ван Винкль (герой одноименного рассказа американского писателя В. Ирвинга).

Rivest Ривест Р. (американский криптолог, один из авторов алгоритма шифрования PIA).

Scherbius Шербиус А. (немецкий инженер, изобретатель шифровальной машины "Энигма").

Schmidt Шмидт Г. (немецкий офицер, с 1931 по 1943 г. продававший ключи и схемы шифровальной машины "Энигма" сначала французам, а затем англичанам).

Shamir Шамир А. (американский криптолог, один из авторов алгоритма шифрования RSA).

Shannon (1916 – 2001) Шеннон К. (американский математик).

"Shark" "Акула" (модификация немецкой шифровальной машины "Энигма", использовавшаяся подводным флотом Германии во время второй мировой войны).

Stimson Стимсон Г. (государственный секретарь USA, автор крылатой фразы "Джентльмены не читают переписку друг друга", произнесенной в оправдание принятого им решения прекратить в 1929 г. финансирование "Американского черного кабинета").

"SWORD" "Булат" (суперкомпьютер, который использовался в 16 управлениях КГБ для решения дешифровальных задач).

Szek Сцек А. (чешский инженер, во время первой мировой войны работавший на радиостанции в Брюсселе и выкравший оттуда немецкий дипломатический код, который впоследствии был использован англичанами, чтобы прочесть одну из шифртелеграмм министра иностранных дел Германии Циммермана).

Tanneberg сражение при Таннеберге (город в Восточной Пруссии) между Германией и Россией в августе 1914 г. (первая битва в мировой истории, решающее влияние на исход которой оказала несостоятельность в вопросах криптографии).

Tavares Таварес С. (один из разработчиков блочного алгоритма шифрования KACT).

Tolstoy Толстой С. (советский криптоаналитик, в 1941 г. вскрывший японский "пурпурный" шифр).

"Triton" "Тритон" (четырёхроторная модификация немецкой шифровальной машины "Энигма", использовавшаяся ВМС Германии во время второй мировой войны).

Turing (1912 – 1954) Тьюринг Алан Матисон (английский математик).

Ultra "Ультра" (условное наименование источника разведывательной информации, которую английские криптоаналитики добывали путем чтения немецкой шифрпереписки в годы второй мировой войны).

Venona Венона (условное наименование источника разведывательной информации, которую американские и английские криптоаналитики добывали путем чтения шифрпереписки советской разведсети на Западе в 40-е – 50-е годы).

Vernam Вернам Г. (американский инженер).

Vigenere Вижинер Б. (французский криптограф).

Voynich Войнич У. (американский торговец редкими книгами, муж известной английской писательницы Э. Войнич, автора романа "Овод").

Walker Уокер Дж. (офицер ВМС USA, на протяжении 17 лет продававший советской разведке криптографические ключи и схемы американских шифраторов).

Walsh Уолш Дж. (американский математик).

Wright Райт Э. (американский писатель, автор романа "Гэдсби", в котором нет ни единого слова, содержащего букву "е" английского алфавита).

Yardley Ярдли Г. (американский криптоаналитик).

"Yellow Book" "Желтая книга" (определяет правила применения критериев американской "Оранжевой книги").

Yurchenko Юрченко В. (высокопоставленный сотрудник КГБ, в 1985 г. убежавший на Запад и предположительно выдавший нескольких агентов советской разведки в USA, в том числе – Р. Пелтона, бывшего сотрудника CIA).

Zendia Зендиа (вымышленное государство, вскрытием шифров которого занимаются сотрудники NSA USA на курсах повышения квалификации).

Zimmermann Циммерман А. (германский министр иностранных дел в годы первой мировой войны).

УКАЗАТЕЛЬ АНГЛИЙСКИХ СОКРАЩЕНИЙ

- (**AUX, aux**) (auxiliary) 17
A²-code (authentication code with arbitration) 320
ABC (American Black Chamber) 10
ACCSA (Allied Communications and Computer Security Agency) 9
ACE (automated computing equipment) 17
ACF (autocorrelation function) 16
ACIA (asynchronous communications interface adapter) 14
ACID (automated classification and interface adapter) 17
A-code (authentication code) 16
ADK (additional decryption key) 6
ADP (automated data processing) 17
AES (Advanced Encryption Standard) 7
AKDC (automatic key distribution center) 17
AKDS (automated key distribution system) 17
A-key (auxiliary key) 17
ALG (algorithm) 8
A-mode (asynchronous mode) 14
ANF (algebraic normal form) 8
ANSI (American National Standards Institute) 10
APNF (almost perfect non-linear function) 9
ASCII (American Standard Code for Information Interchange) 10
AST (asynchronous system trap) 15
ATDM (asynchronous time division multiplexing) 15
BAC (binary asymmetric channel) 23
BACE (basic automatic checkout equipment) 20
BAK (backup) 18
BB, bb (broadband) 33
BC (block chaining) 30
BCD (binary coded decimal) 23
BCDD (binary-coded decimal digit) 26
BCFSK (binary-coded frequent-cy-shift keying) 24
BCI (binary coded information) 23
B-Crypt (British Telecom Cryptological algorithm) 33
Bd, bd 1. (band); 2. (binary-to-decimal) 19, 25
BDAM (basic direct access method) 20
B-Dienst (от нем. Beobachtungs-Dienst) 21
BDOS (basic disk operating system) 20
BILBO (built-in logic block observer) 34
BIP (built-in pulser) 34
BISAM (basic indexed sequential access method) 20
BO (blocking oscillator) 31
BPAM (basic partitioned access method) 20
BPF (bandpass filter) 20
BPI, bpi (bits per inch) 28
BPM (bandpass limiter) 19
BPS, bps (bits per second) 28
BPU (basic processing unit) 20
BS (binary scale) 24
BSAM (basic sequential access method) 21
BSC, bisync (binary synchronous communication) 26
BSDC (binary symmetric dependent channel) 24
BTAM (basic telecommunication access method) 21
BTF (binary transversal filter) 24
BTR (bit-timing recovery) 28
BW, bw (bandwidth) 20
C (confidential) 63
CA (certification authority) 41

- CAG** (cyclic address generator) 79
- CAPI, cryptoAPI** (Cryptographic Application Programming Interface) 73
- car** (carrier) 38
- CAST** (блочный алгоритм шифрования, разработанный сотрудниками транснациональной корпорации "Нортел Нетворкс" Карлайслом Адамсом и Стэффордом Таваресом) 39
- CAV** (constant angular velocity) 64
- CBC** (cipher block chaining) 46
- CBMS** (computer-based message system) 59
- CC** (control computer) 65
- CCB** (Central Cipher Bureau) 40
- CCCC** (Centralized COMINT Communications Center) 40
- CCCEP** (Commercial Communications Security Endorsement Program) 54
- CCH** (Center for Cryptologic History) 40
- CCI** (controlled cryptographic item) 66
- CCM** (control computer module) 65
- CCSC** (Commercial Computer Security Center) 54
- CCSK** (cyclic(al) code-shift keying) 79
- CDK** (cryptodeveloper kit) 72
- CDL** (Computer Description Language) 59
- CER** (cryptographic equipment room) 73
- CF** (constant frequency) 64
- CFAR** (constant-false-alarm rate) 64
- CFB** (cipher feedback) 47
- CFM** (cipher feedback mode) 46
- CFVD(S)** (constant-frequency variable-dot system) 64
- CGM** (computer graphics metafile) 60
- char** (character) 42
- CHF** (characteristic frequency) 44
- CI** (computer interface) 59
- CIA** (Central Intelligence Agency), (computer intelligence access) 40, 59
- CIB** (Communications Intelligence Board) 55
- cifax** (ciphered facsimile communication) 47
- CK** (cryptoignition key) 75
- CKA** (central keying authority) 40
- CLIP** (cellular logic image processor) 40
- CMLE** (conditional maximum likelihood estimate) 62
- CNK** (cryptonet key) 76
- com, comm** (communication) 10
- COMINT** (communications intelligence) 40
- compaction** (data compression) 82
- COMPUSEC** (Computer Security) 59
- COMSAT** (Communications Satellite) 55
- COMSEC** (Communications Security) 55
- COND** (condition) 61
- CONELRAD** (control of electromagnetic radiation) 65
- COS** (code operated switch) 51
- CP** (control program) 66
- cpd** (compound) 58
- CRC** (cyclic redundancy check); (cyclical redundancy code) 79
- CRG** (Cryptological Readiness Group) 76
- CRL** (certificate revocation list) 41
- CRNG** (cryptographic random number generator) 74
- cryptoequipment** (cryptographic equipment) 72
- cryptofiction** (cryptographic fiction) 73
- cryptosync** (cryptosynchronization) 78
- cryptosystem** (cryptographic system) 74
- cryptovvariable, CV** (cryptographic variable) 74
- CS** (cryptosystem) 78
- CS, CSECT** (control section) 66
- CSA** (carry-save adder) 39

CSD (communications security device) 56

CSE (Communications Security Establishment); (control and switching equipment) 56, 65

CSL (control storage load) 65

CSMA (carrier-sense multiple access) 38

CSMA/CD (carrier-sense multiple access and collision detection) 38

CSP (cryptographic service provider) 74

CSPDK (Cryptographic Service Provider Developer Kit) 74

CSRNG (cryptographically secure random number generator) 75

CSS (Central Security Service) 40

CSSIS (Central Service for Security and Information Systems) 40

CTAK (ciphertext autokey) 47

CTRL (control) 65

CTT (cryptological-technician) 76

CZ (call of zero) 37

D (decipher); (deciphering); (diplomatic) 86, 86, 96

DA (design automation); (demand assignment) 90, 88

D-A, D/A (digital-to-analog(ue)) 95

DAC (data authentication code); (digital-to-analog(ue) conversion); (digital-to-analog(ue) converter); (digital-to-synchro converter) 82, 95, 95, 95

DAM (direct-access method) 97

DAMA (demand assignment multiple access) 88

DARPA (Defense Advanced Research Projects Agency) 87

DASD (direct-access storage device) 97

DC (device control); (direct coupling) 92, 96

DCB (data control block) 80

DCE (data communication equipment) 80

DCO (digital control oscillator) 94

DCP (data ciphering processor) 81

DD (digital display); (double-density disk) 94, 103

DD/D (data dictionary/directory) 80

DDA (digital differential analyzer) 94

DDC (direct digital control) 96

DDE (direct data entry) 96

DDL (data description language); (digital system design language) 83, 95

ddname (data definition name) 83

DDR (digital data receiver) 94

DDT (digital data transmitter) 94

DEA (Data Encryption Algorithm) 93

DECK (decipher key) 86

DEE (data encryption equipment) 80

DEK (data enciphering key); (data exchange key) 80, 80

DEP (data encryption processor) 81

DES (Data Encryption Standard) 90

DFB (distributed feedback) 100

DFSK (double frequency-shift keying) 102

DFT (discrete Fourier transform) 98

D-H (Diffie-Hellman) 94

DIA (Defense Intelligence Agency) 87

DID (digital information display); (direct inward dialing) 95, 97

dif (differential file) 94

DIM (digital input module) 95

dina (digital network analyzer) 95

DIRNSA (director of NSA) 98

DIVOT (digital-to-voice translation) 95

DL (delay line); (discrete logarithm) 88, 98

DLE (data link encryptor) 81

DLP (discrete logarithm problem) 98

DM (demand meter) 88

DMA (direct memory access) 97

DMAC (direct memory access controller) 97

DMC (data management system); (digital microcircuit) 81, 95

DMF (digital matched filter) 95
DMM (digital multimeter) 95
DMS (Defense Message System) 87
DNC (direct numerical control) 97
DNF (disjunctive normal form) 99
DOD (Department of Defense); (direct outward dialing) 89, 97
DOM (digital output module) 95
DON (Defense Data Network) 87
DPCM (differential pulse-code modulation) 94
DPLL (digital phase locked loop) 95
DPM (digital panel meter) 95
DPO (delay pulse oscillator) 88
DPSK (differential phase-shift keying) 94
DR (data rate), (data register), (dynamic range) 81, 81, 104
DRAW (direct read after write) 97
DRC (data recording control) 81
DRD (data recording device) 81
DS (delay-and-sum), (distributed system), (dynamic scattering), (dynamic switching) 88, 101, 104, 104
DSA (differential synthesis algorithm); (Digital Signature Algorithm) 94, 95
DSCR (descrambler) 90
DSD (data security device) 81
DSDL (Data Storage Description Language) 81
DSE (data switching exchange) 81
DSG (digital signature) 95
DSP (digital signal processing) 95
DSS (Digital Signature Standard) 95
DSSA (distributed system security architecture) 100
DSU (digital storage unit) 95
DSW (device status word) 93
DT (data transmission) 81
DTE (data terminal equipment) 81
DTF (tracking filter) 104
DTO (data take-off) 81
DTU (data transfer unit) 85
DUT (device under test) 92
DVM (digital voltmeter) 95

DVR (digital video recording) 95
E, ECPH (encipher); (enciphering) 109, 110
EALM (electronically addressed light modulator) 107
EBCDIC (extended binary-coded decimal interchange code) 119
EBDA (encipher below decipher above) 109
EBNF (extended Backus-Naur form) 119
E-box (expansion box) 117
EC (electronically controlled) 107
ECAP (electronic circuit analysis program) 106
ECB (electronic code book) 106
ECCM (electronic counter-countermeasures) 107
ECPL (Endorsed Cryptographic Products List) 113
e-d (encryption-decryption) 112
EDA (exploratory data analysis) 118
EDGE (electronic data gathering equipment) 107
EDN (elementary digital network) 108
EDP (electronic data processing) 107
EDPM (electronic data processing machine) 107
EDPS (electronic data processing system) 107
EEC (external error control) 120
EFT (Electronic Funds Transfer) 107
EKMS (electronic key management system) 107
EM (electromagnetic) 106
E-mail (electronic mail) 107
EMC (electromagnetic compatibility) 106
EMI (electromagnetic interference) 106
EMIFIL (electromagnetic interference filter) 106

- EMR** (electromagnetic radiation) 106
- EMSEC** (emission security) 109
- ENC** (encryption); (encryption key) 111, 111
- EOA** (end of address) 112
- EOB** (end of block) 112
- EOV** (end of volume) 112
- EPDCC** (elementary potential digital computing component) 108
- EPP** (electronic post-production) 107
- EQ** (equal) 114
- eq.**, **eqn.** (equation) 114
- ERDL** (encipher right decipher left) 109
- ESM** (electronic signal monitoring) 107
- ESS** (electronic switching system) 107
- EVFU** (electronic vertical format unit) 107
- EXP** (electronic crosspoint) 107
- EMP** (Encrypted Messaging Protocol) 111
- ETE** (end-to-end encryption) 112
- FAPSI** (Federal Agency for Government Communications and Information) 124
- fax**, **fac**s (facsimile) 121
- FBI** (Federal Bureau of Investigation) 124
- FD** (fill device) 124
- FDC** (French diplomatic communications) 128
- FDF** (Fast Data Finder) 123
- FDM** (frequency division multiplexing) 128
- FEAL** (Fast Encryption Algorithm) 123
- FEC** (forward error correction) 128
- FFT** (fast Fourier transform) 123
- FIMAS** (Financial Institution Message Authentication Standard) 125
- FIPS 140-1** (Federal Information Processing Standard 140-1) 124
- FISA** (Federal Information Security Agency) 89
- FRM** (frame) 128
- FWT** (Fast Walsh Transform) 123
- FAC** (factorization) 122
- FACC** (factorization cryptosystem) 122
- GA** (genetic algorithm) 131
- GC** (global control) 132
- GC&CS** (Government Code and Cipher School) 132
- GCD** (greatest common divisor) 133
- GDES** (Generalized DES) 130
- GF(p)** (Galois field) 216
- GLDL** (geometrical layout description language) 131
- gnd** (ground) 133
- GPKI** (global public key infrastructure) 132
- GSC&C** (Governmental School of Codes and Ciphers) 132
- GTD** (geometrical theory of diffraction) 131
- HW**, **hdw** (hardware) 136
- hex** (hexadecimal) 137
- HUMINT** (human intelligence) 140
- IACR** (International Association for Cryptologic Research) 152
- IC** (index of coincidence) 143
- ID**, **id** 1. (identification); 2. (identity) 140, 141
- IDEA** (International Data Encryption Algorithm) 152
- IDFT** (inverse discrete Fourier transform) 153
- IDS** (interactive design system) 150
- IEC** (internal error control) 151
- IES** (information exchange system) 144
- IFAC** (International Federation of Automatic Control) 152
- IFE** (intelligent front end) 149

-
- IFIP** (International Federation for Information Processing) 152
 - IGS** (interactive graphics system) 150
 - IIR** (infinite impulse response) 144
 - IK** (interchange key) 151
 - IMS** (Information Management System) 145
 - inf** (information) 144
 - INFOSEC** (information security) 145
 - infowar** (information war) 145
 - inh** (inhibit input) 146
 - IP** (initial permutation) 146
 - IPACS** (interactive pattern analysis and classification system) 150
 - IPHT** (Inverse Pseudo-Hadamard transform) 153
 - IPI** (intelligent peripheral interface) 149
 - IPL** (initial program loader) 147
 - IPSEC** (Internet Secure Protocol) 153
 - IS** (information separator) 145
 - ISAM** (index sequential access method) 143
 - ISI** (intersymbol interference) 153
 - ISO** (International Standards Organization) 152
 - ISP** (indexed sequential processing) 143
 - IT** (information technology) 145
 - ITAR** (International Traffic in Arms Regulations) 152
 - IV** (initialization vector) 147
 - k** (key) 156
 - KD** (key directory) 157
 - KDC** (key distribution center) 157
 - KDP** (key distribution protocol) 157
 - KDS** (key distribution system) 157
 - KEA** (key exchange algorithm) 157
 - KES** (key escrow system) 157
 - KG, Key-Gen** (key generator) 110
 - KIN** (key identification number) 157
 - KK, KEK** (key-encrypting key) 159
 - KMF** (key management facilities) 158
 - KMP** (key management protocol) 158
 - KMS** (key management system) 158
 - KN** (knapsack) 160
 - KNS** (key notarization system) 158
 - KPS** (key predistribution scheme) 158
 - KSU** (key storage unit) 159
 - KV** (key variable) 159
 - KAK** (key-autokey) 159
 - KAC** (key authentication center) 156
 - KMC** (key management center) 158
 - KP** (key processor) 158
 - KPK** (key production key) 158
 - KCA** (key certification authority) 157
 - KCC** (key certification center) 157
 - LAN** (local area network) 167
 - LBA** (linear-bounded automation) 165
 - LCG** (linear congruential generator) 164
 - LCM** (least common multiple) 162
 - LDM** (linear delta modulation) 164
 - LEAF** (law enforcement access field) 164
 - LFSR** (linear feedback shift register) 164
 - lim** (limit) 163
 - LIOCS** (logical input/output control system) 169
 - LMK** (local master key) 167
 - LO** (local oscillator) 171
 - LOCI** (logarithmic computing instrument) 168
 - LP** (linear programming) 165
 - LPC** (linear predictive coding) 164
 - LPS** (local periodic structure) 167
 - LRSM** (linear restricted scattering matrix) 164
 - LS, LSTOR** (local storage) 167

- LSAR** (local storage address register) 167
- ltr** (letter) 163
- M** (mega-) 179
- MAC** (memory access controller); (message authenticating code); (message authentication code) 179, 181, 181
- MAT** (memory address test) 179
- Mbit** (megabit) 179
- Mbyte** (megabyte) 179
- MCU** (microprocessor control unit) 182
- MD** (Message Digest) 197
- MDR** (memory data register) 179
- MF** (matched filter) 176
- MI** (memory interface) 179
- MIMD** (multiple-instruction multiple-data) 186
- MITM** (meet-in-the-middle) 178
- MITMA** (meet-in-the-middle attack) 178
- M-key, MK** (master key) 175
- MLE** (maximum likelihood estimate) 177
- ML-sequence** (maximal length sequence) 177
- ML-sequence** (maximal length sequence) 177
- MLSR** (maximal length shift register) 177
- MMAR** (main memory address register) 173
- MMR** (main memory register) 173
- MMU** (memory management unit) 179
- mot-key** (modified one-time key) 183
- MOV** (memory-to-memory move instruction) 179
- MPPE** (Microsoft Point-to-Point Encryption protocol) 182
- MPQS** (Multiple-Polynomial Quadratic Sieve) 186
- MPU, μ P** (microprocessor unit) 182
- MS** (Microsoft) 182
- MS CHAP** (Microsoft Challenge Handshake Authentication Protocol) 182
- MSDR** (main storage data register) 173
- MSF** (matched spatial filter) 176
- MSG** (message) 180
- MSP** (Message Security Protocol) 181
- MTC** (memory test computer) 179
- multisubstitution** (multiple substitution) 186
- MUX, mux, MPX** (multiplexer) 186
- MK** (message key) 181
- NA** (numerical aperture) 194
- NBS** (National Bureau of Standards) 188
- NC** (numerical control) 194
- NCSC** (National Computer Security Center) 188
- NDC** (non-uniform diplomatic communications) 192
- NDL** (network description language) 190
- NEP** (noise-equivalent power) 191
- NET, net** (noise-equivalent temperature); (network) 191, 189
- NF** (noise factor) 191
- NFS** (network file system) 111
- NIST** (National Institute of Standards and Technology) 188
- NIZK** (non-iterative zero-knowledge proof) 192
- NL, NLT** (noise limiter) 191
- NLFSR** (non-linear feedback shift register) 192
- NOFORN** (no foreigners) 191
- NPR** (noise power ratio) 191
- NR** (noise reduction) 191
- NRS** (noise reduction system) 191
- NSA** (National Security Agency) 189
- NSASAB** (National Security Scientific Advisory Board) 189
- NSC** (noise suppression circuit) 191
- NSGN** (noise generator) 191

-
- NSR** (noise-to-signal ratio) 191
 - OBFB** (output block feedback) 201
 - O-book** ("Orange Book") 200
 - OC** (open circuit) 197
 - OCSP** (on-line certificate status protocol) 196
 - oct** (octal) 195
 - OFB** (output feedback) 201
 - OG** (output generator) 201
 - OHW** (output highway) 201
 - OL** (open loop) 197
 - OLTF** (open loop transfer function) 197
 - op** (operator) 198
 - Op Cd** (operation code) 198
 - OR** (ordering register) 200
 - OSA** (open systems architecture) 197
 - OSI** (open systems interconnection) 197
 - OTAD** (over-the-air key distribution) 202
 - OTAR** (over-the-air rekeying) 202
 - OTAT** (over-the-air key transfer) 202
 - OTK** (one-time key) 202
 - OTP** (one-time pad) 30
 - OWF** (one-way function) 136
 - OWHF** (one-way hash function) 196
 - PAD** (packet assembly and disassembly) 203
 - P-box** (permutation box) 209
 - PC** (permutation code) 209
 - PC, P-counter** (program counter) 222
 - PCBC** (propagating cipher block chaining) 225
 - PDL** (program design language) 222
 - PDS** (program development system) 223
 - PEAK** (Parametrically Extensible Algorithmic Key) 206
 - PERT** (Project Evaluation and Review Technique) 224
 - PFB** (plaintext feedback) 211
 - PGP** (Pretty Good Privacy) 215
 - PIC** (programmable interrupt controller) 224
 - PIN** (personal identification number) 211
 - PIO** (programmable input-output chip) 224
 - PKC** (public-key cryptosystem) 228
 - PKCS** (Public-Key Cryptography Standard) 227
 - p-key** (public-key) 227
 - PKSD** (programmable key storage device) 224
 - PLA** (programmable logic array) 224
 - placode** (plain code) 211
 - PN** (pseudonoise) 226
 - poly time** (polynomial time) 86
 - POS expression** (product of sums expression) 220
 - PRBS** (pseudorandom binary sequence) 226
 - PRN** (pseudo-random number) 192
 - PROD** (Production) 221
 - PROM** (programmable read only memory) 224
 - PSN** (packet switching network) 204
 - PSW** (process status word); (program status word) 219, 222
 - P** (plaintext); (police) 211, 212
 - PB** (plug-board) 212
 - PBC** (plaintext block chaining) 211
 - PEK** (password encryption key) 207
 - PEM** (Privacy Enhanced Mail) 217
 - PKA** (public-key algorithm) 227
 - PHT** (Pseudo-Hadamard transform) 226
 - QC** (quantum cryptography) 229
 - QRC** (quadratic residue cipher) 229
 - RAVR** (receiver) 235

-
- RC** (redundancy check); (Rivest's Code) 238, 247
 - ret** (return) 245
 - RF** (radio frequency) 230
 - RISC** (reduced instruction set computer); (reduced instruction set computer architecture) 237, 237
 - RKG** (running-key generator) 249
 - RN** (random number); (radio noise) 231, 230
 - rot13** (rotate alphabet 13 places) 247
 - RPN** (reverse Polish notation) 245
 - RSA** (R. Rivest, A. Shamir and L. Adelman) 248
 - RSADSI** (RSA Data Security Incorporated) 248
 - RSALABS** (RSA Laboratories) 248
 - RTC** (real-time clock) 233
 - SAC** (strict avalanche criterion) 274
 - SAFER** (Secure And Fast Encryption Routine) 253
 - S-box** (substitution box) 275
 - SCC** (single-chip controller) 264
 - SCG** (synchronous command generator) 279
 - SCORE** (Special Committee on Compromising Emanation) 268
 - SCR** (scrambler) 251
 - SCS** (Special Collection Service) 268
 - SD** (single-density disk) 264
 - SDC** (serial data controller) 257
 - SDLC** (synchronous data link control) 279
 - SDR** (statistical data recorder) 271
 - SEAL** (Software-optimized Encryption Algorithm) 266
 - secal, selcal** (selective calling) 255
 - SEEK** (secure electronic exchange of keys) 253
 - SETAR** (serial event timer and recorder) 257
 - SHA** (Secure Hash Algorithm) 253
 - SHS** (Secure Hash Standard) 253
 - SHTTP** (Secure Hypertext Transfer Protocol) 253
 - SID** (single-sideband frequency modulation); (system for interactive design) 264, 280
 - SIDS** (symbolic interactive design system) 278
 - SIG** (signature) 261
 - SIGINT** (signals intelligence) 261
 - SIGSUM** (SIGINT summary) 261
 - SIMD** (Single-Instruction Multiple Data stream) 264
 - SIRT** (simultaneous iterative reconstruction technique) 263
 - SISD** (Single-Instruction Single Data) 264
 - SISO** (serial in serial out) 257
 - SK, s-key** (session key) 258
 - SKMP** (Secure Key Management Protocol) 253
 - SLDL** (symbolic layout description language) 278
 - SM** (secondary memory) 252
 - SMB** (system message block) 280
 - SMIME** (Secure Multipurpose Internet Mail Extensions) 253
 - SNA** (system network architecture) 281
 - SPCS** (satellite personal communications system) 250
 - SPE** (single processing element) 263
 - SPI** (single program initiator) 263
 - SPKM** (Simple Public-Key Mechanism) 262
 - SPM** (scratch-pad memory) 251
 - SPN** (substitution-permutation network) 276
 - SPS** (scratch pad store) 251
 - SPU** (system processing unit) 280
 - SQC** (statistical quality control) 271
 - SRI** (signal related information) 261
 - SRT** (standard remote terminal) 270
 - SSA** (serial shift arrangement) 257
 - SSD** (Special Signals Division) 269
 - SSL** (Secure Sockets Layer) 253
 - SST** (synchronous system trap) 279

SSTR (synchronous system trap routine) 279

STD (standard) 270

STDM (synchronous time division multiplexing) 279

STM (system test mode) 280

STOR (storage) 272

STR (synchronous transmitter-receiver) 279

super (superimpose) 277

SWAN (Secure Wide Area Network) 253

TARE (telemetry automatic reduction equipment) 284

TAREX (Target Exploitation) 283

TCAM (telecommunication access method) 284

TCP (transmission control protocol) 291

TCSEC (Trusted Computing System Evaluation Criteria) 293

TCU (terminal cryptographic unit); (transmission control unit) 285, 291

TD (transmission and distribution) 291

TDM (time division multiplexing) 287

TDMS (transmission distortion measuring set) 291

TE, TME (telemetric equipment) 284

TEA (Tiny Encryption Algorithm) 288

TECHINS (technical instructions) 284

TEX, TLX (telex) 284

TIS (telemetry information system) 284

TKDC (trusted key distribution center) 294

TP monitor (transaction processing monitor) 288

TR (transaction-routing) 289

TST (test) 285

TXT (text) 285

TEK (traffic encryption key) 288

TEXTA (technical extracts of traffic) 284

TM (transformation matrix) 290

TTP (Trusted Third Party) 294

UART (universal asynchronous receiver/transmitter) 299

UBE (unbreakable encryption) 296

UCS (universal character set) 298

UDC (Universal Decimal Classification) 299

UDPI (universal digital processor industrial) 299

UGSDA (unusually good simultaneous diophantine approximation) 300

UHF (ultra-high frequency) 296

UICOM (universal integrated communication) 299

UKUSA (United Kingdom & United States of America) 298

ULA (universal logic array) 299

ULM (universal logic module) 299

UPC (universal product code) 299

UPS (universal power supply) 299

UR (unit record) 298

US (unit separator) 298

USART (universal synchronous/asynchronous receiver/transmitter) 299

USRT (universal synchronous receiver/transmitter) 299

USSS (United States SIGINT System) 298

UT (universal time) 299

UTCLK (universal transmitter clock) 299

UUT (unit under test) 298

V and V (verification and validation) 304

VDI (virtual-device interface) 306

VDT (visual display terminal) 308

VDU (visual display unit) 308

VF 1. (vector field); (voice frequency) 308

VFU (vertical format unit)

VLSI (very large-scale integration logic) 308

- VM** (virtual memory) 306
- VMS** (virtual memory system) 306
- VOLSER** (volume serial number)
308
- VS** (vertical scale) 305
- VSAM** (virtual storage access
method) 307
- VTAM** (virtual telecommunication
access method) 307
- VTOC** (volume table of contents)
308

- WA** (Wassenaar Arrangement) 309
- WF** (work factor); (work function)
312, 312
- WHT** (Walsh-Hadamard transform)
309
- WFRF** (work factor reduction field)
312
- WT** (Walsh transform) 309
- WWW** (World-Wide Web) 312

- xfer** (transfer) 289
- XOR** (exclusive-OR) 116

- ZKIP** (zero-knowledge iterative
proof) 313
- ZKP** (zero-knowledge proof); (zero-
knowledge protocol) 313