СЛОВАРЬ

КРИПТОГРАФИЧЕСКИХ ТЕРМИНОВ

Московский государственный университет им. М.В. Ломоносова
АКАДЕМИЯ КРИПТОГРАФИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЛОВАРЬ КРИПТОГРАФИЧЕСКИХ ТЕРМИНОВ

Под редакцией Б. А. Погорелова и В. Н. Сачкова

Москва
Издательство МЦНМО
2006

ББК 32.81в6
С48

Словарь криптографических терминов / Под ред. Б. А. Погорелова и В. Н. Сачкова. — М.: МЦНМО, 2006. — 94 с.

ISBN 5-94057-257-X

Словарь содержит более 500 наиболее важных криптографических терминов. Классификация проводилась по следующим основным рубрикам: основания криптографии, синтез криптографических систем, криптографический анализ, криптографические протоколы, ключи, особенности реализации криптосистем в компьютерных сетях, математические термины.

Словарь предназначен для специалистов в области криптографии.

ББК 32.81в6

Издание подготовлено и выпущено при поддержке Научного комитета Россия-НАТО в рамках проекта «A Process for Developing a Common Vocabulary in the Information Security Area», reference HSD.NR.NRARW 982506.

ISBN 5-94057-257-X

ВВЕДЕНИЕ

В последней четверти XX и начале XXI столетий интенсивное развитие телекоммуникационных и информационных систем и расширение круга их пользователей обострили проблему защиты информации в подобных системах. Важными пользователями систем защиты информации стали не только государственные организации, но и коммерческие структуры, частные лица. Эти же процессы значительно повлияли на пути дальнейшего развития как криптографических систем (криптосистем) — важнейшей составляющей любой надёжной системы защиты информации, так и в целом на развитие криптографии. Компьютеризация распределённых информационных систем, систем управления и финансовых расчётов поставила ряд новых проблем защиты информации с учётом множественности доступа к средствам хранения, обработки и передачи информации по каналам связи.

Для решения этих проблем кроме использования традиционных методов криптографической защиты информации и предотвращения несанкционированного доступа к средствам её обработки потребовались разработка методов обеспечения целостности информации, аутентификации сообщений и абонентов, контроля доступа к программному обеспечению и техническому оборудованию средств связи и хранения информационных ресурсов.

Автоматизация способов обработки информации и её передачи по высокоскоростным каналам связи привела к необходимости использования разнообразных протоколов, представляющих собой распределённые алгоритмы, реализация которых осуществляется несколькими участниками. Примерами являются протоколы аутентификации сообщений, протоколы аутентификации абонентов, схема подписи цифровой, протокол распределения ключей и др. Разработка подобных протоколов и анализ их уязвимости представляет собой активно развивающееся направление современной криптографии.

Революционное влияние на развитие криптографии оказало появление в 70-х годах прошлого столетия асимметричных шифрсистем, использующих открытое распределение ключей. Криптографическая стойкость этих систем основывается на большой вычислительной сложности решения некоторых математических задач.

Особенностью современной криптографии является и широкое использование стандартов обеспечения безопасности информации. Разработаны общедоступные стандарты шифрования DES, ГОСТ 28147-89,

AES, стандарт цифровой подписи DSS, стандарты электронной цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001, стандарты функции хеширования SHS и ГОСТ Р 34.11-94. К разработке и исследованию этих стандартов привлекается внимание большого количества математиков и криптографов. Их исследования публикуются в ряде существовавших ранее и вновь созданных научных журналов и в специальных монографиях. Для обсуждения результатов анализа криптографической стойкости различных криптосистем организуются конференции, в которых участвуют криптографы со всего мира. Например, CRYPTO, EUROCRYPT, ASIACRYPT, FSE, PKC.

Существенное расширение предмета исследований и круга исследователей стало источником появления в криптографии новых понятий и терминов, используемых в научных публикациях и в докладах на конференциях. Одновременно с этим в научных докладах, статьях и монографиях стали обсуждаться и традиционные проблемы криптографии, которые до этих пор были достоянием только закрытых коллективов государственных специальных служб. В результате одни и те же криптографические объекты стали обозначаться различными терминами, в том числе и экзотическими. Многие публикации по криптографии на русском языке появляются как переводы или обзоры англоязычной литературы. При этом не всегда имеет место адекватный перевод понятий, допускаются терминологические неточности, порой проявляется недостаточное знание соответствующей предметной области.

Быстрое и широкое распространение криптографических методов для защиты информации юридических и физических лиц, развёртывание соответствующих направлений подготовки студентов в учебных заведениях создают потребность в монографической и учебной литературе. С другой стороны, в настоящее время наблюдается недостаток качественной общедоступной литературы на русском языке, в которой вопросы криптографии излагались бы с соблюдением ясной и последовательной терминологии. Некоторые публикации по криптографии, к сожалению, оставляют впечатление конъюнктурности и непрофессионализма. Причем проблемы начинаются на уровне основных терминов: криптография, криптология, шифр, дешифрование, гамма и т. д.

В этих условиях создание единой криптографической терминологии стало насущной задачей совершенствования научного обмена для специалистов по криптографии и информационной безопасности, обеспечения учебного процесса. Делались многократные попытки создания глоссариев как приложений к монографиям и справочным пособиям по криптографии. Однако проблема создания словаря основных крипто-

графических понятий и терминов на русском языке оказалась слишком сложной и до последнего времени не находила своего достаточно приемлемого решения.

В течение трёх последних лет в Академии криптографии Российской Федерации при участии Института проблем информационной безопасности МГУ им. М. В. Ломоносова проводилась научно-исследовательская работа по совершенствованию понятийного аппарата и разработке терминологической базы криптографии, используемой в открытых работах по вопросам криптографии и информационной безопасности. Целью этой работы являлось создание на первом этапе компактного словаря с единой системой трактовки терминов. На основе изучения всех доступных публикаций по криптографии было выделено несколько тысяч русскоязычных и англоязычных терминов и понятий. Затем были разработаны принципы классификации выделенных терминов и понятий. Эти принципы позволили установить иерархическую зависимость терминов и выделить из них 550 наиболее важных, требующих первоочередного толкования. Классификация проводилась по следующим основным рубрикам: основания криптографии, синтез криптографических систем, криптографический анализ, криптографические протоколы, ключи, особенности реализации криптосистем в компьютерных сетях, математические термины.

При составлении словаря в основу были положены, как правило, устоявшиеся в криптографической литературе толкования терминов и понятий. Одной из важных особенностей предлагаемого словаря является стремление к достаточно полному соответствию его терминологии и терминологии в существующих стандартах в области информационной безопасности. Однако привести трактовки сотен терминов в полное соответствие со всеми имеющимися нормативными актами ввиду наличия расхождений в понимании содержания некоторых криптографических понятий и терминов, на взгляд авторов невозможно.

По некоторым терминам и авторы словаря имели разные взгляды на трактовку, и окончательный результат порой являлся компромиссом. Другие термины, на взгляд авторов, являются неудачной калькой с англоязычных терминов, но стали достаточно широко употребительными. Например: устанавливать подлинность, аутентифицировать (authenticate); дифференциальный метод и более удачный русскоязычный вариант разностный метод; метод встречи посередине и т. д.

При реализации корневых и перекрестных ссылок пришлось ввести некоторые дополнительные термины (например, блочный базовый алгоритм зашифрования), разделить понятия нарушитель и противник.

В итоге предлагаемый вариант толкования терминов является компромиссом между полнотой. компактностью, ранее сложившимися вариантами толкования, различными нормативными актами и единством толкования. Приведенные в словаре английские эквиваленты терминов также порой являются компромиссом между сложившейся практикой и предлагаемой авторами системой криптографических терминов.

Основным источником включённых в словарь понятий и терминов является криптография. Небольшое число терминов относится к более широкой области информационной безопасности. В словарь не вошли многочисленные специфические термины, касающиеся описания конкретных криптосистем, так как их включение потребовало бы привести и описания самих этих криптосистем, что представляется задачей, не соответствующей предназначению данного словаря. За редкими исключениями в словарь не вошли термины и понятия, связанные с историей криптографии, персоналиями и организациями. Эта заслуживающая внимания тематика требует отдельного рассмотрения.

Кратко остановимся на трактовке основных понятий и терминов.

Прежде всего, о самом термине криптография, толкование которого имеется в ряде изданий, в том числе энциклопедических. В данном словаре криптография определяется как область научных, инженерно-технических, прикладных, исследований и практической деятельности, которая связана с разработкой, анализом и обоснованием криптографической стойкости криптографических средств защиты информации от угроз со стороны противника и/или нарушителя. С некоторой долей условности криптография делится на две части: криптосинтез и криптоанализ. Криптография включает в себя криптологию. Одновременно с этим криптология рассматривается как отрасль математики и математической кибернетики, изучающая различные математические модели криптографических систем. Представляется, что подобная трактовка, устанавливающая соответствие между терминами криптография и криптология, отражает исторически сложившуюся связь между теоретической и прикладной криптографией и роль в этом взаимодействии математики, математической кибернетики, физики, теории связи и др.

Одним из основных понятий криптографии является понятие криптографической системы (криптосистемы). Под криптосистемой понимается система обеспечения безопасности информации криптографическими методами в части конфиденциальности, целостности, аутентификации, невозможности отказа и неотслеживаемости. В качестве подсистем криптосистема может включать системы шифрования, системы идентификации, системы имитозащиты, системы цифровой подписи и др.,

а также систему ключевую, обеспечивающую работу остальных систем. В свою очередь, система шифрования предназначена для защиты информации от ознакомления с её содержанием со стороны лиц, не имеющих права доступа к ней. Защита обеспечивается путем зашифрования информации. Понятие системы шифрования включает в себя понятия шифра, ключевой системы и способов кодирования исходной и выходной информации. Наконец, шифр определяется как семейство обратимых отображений (функций шифрования) множества блоков открытых текстов (сообщений) в множество блоков шифрованных текстов (сообщений) и обратно. Каждое из отображений определяется значением некоторого параметра, называемого ключом, и описывается некоторым алгоритмом шифрования. Математическая модель шифра включает в себя алгоритм зашифрования, алгоритм расшифрования, определение режимов шифрования, а также модель множества открытых текстов.

Основным требованием к криптосистемам и вместе с тем одним из фундаментальных понятий криптографии является стойкость. Криптографическая стойкость (криптосистемы, криптопротокола) определяется как способность противостоять атакам противника или нарушителя, как правило, имеющим целью получить секретный ключ или открытое сообщение. Имеются два основных подхода к определению и оценке стойкости — теоретическая стойкость и практическая стойкость. Оценивается стойкость в процессе проведения криптографического анализа. Такой анализ проводится, с одной стороны, разработчиками и законными пользователями криптосистемы с целью оценки эффективности системы защиты информации от атаки потенциального противника или нарушителя, а с другой стороны — противником или нарушителем с целью подготовки и реализации атаки на криптосистему. В процессе проведения криптоанализа криптосистем используются известные и разрабатываются новые методы криптоанализа, связанные с построением алгоритмов дешифрования и оценкой возможности их программно-аппаратной реализации. Под практической стойкостью понимается вычислительная сложность алгоритма, реализующего наилучшую в определённом смысле атаку на криптосистему. Определение теоретической стойкости зависит от выбранной математической модели. Основные подходы к определению теоретической стойкости в настоящее время: стойкость теоретико-информационную, когда применяется теоретико-информационная модель; и стойкость теоретико-сложностная, когда применяется теоретико-сложностная модель. Рассмотрение теоретической стойкости в рамках абстрактных математических моделей позволяет говорить о доказуемой стойкости.

Большое значение в криптографии имеет и понятие алгоритма. Так, формальное описание функций, реализуемых шифрсистемой, определяется соответствующими алгоритмами зашифрования и алгоритмами расшифрования. Для других типов криптосистем рассматривают алгоритмы формирования цифровой подписи, алгоритмы имитозащищающего кодирования и др. В зависимости от способов обработки информации алгоритмы зашифрования подразделяются на два типа — поточные и блочные. Базовый блочный алгоритм зашифрования реализует для каждого блока открытого текста фиксированной длины одну и туже, зависящую от ключа, обратимую функцию зашифрования, т. е. представляет собой алгоритм простой замены блоков фиксированной длины. В этом смысле ГОСТ-28147-89, DES, AES являются базовыми алгоритмами. Конкретный блочный алгоритм зашифрования задаётся базовым блочным алгоритмом зашифрования и режимом шифрования. Поточная шифрсистема реализует для каждого блока открытого текста, вообще говоря, свою, зависящую от ключа, функцию зашифрования.

Функции и отображения, необходимые для реализации криптографических систем, принято называть криптографическими функциями. Такие функции используются при выработке ключей, псевдослучайных последовательностей, определяют процессы зашифрования и расшифрования и другие процессы, обеспечивающие имитостойкость и выработку цифровой подписи. Криптографическими алгоритмами называются алгоритмы, реализующие вычисление криптографических функций.

Под криптографическими операциями понимаются зашифрование и расшифрование данных или ключей, формирование и проверка цифровой подписи или кода аутентификации сообщений, вычисление значения хэш-функции и протокол выработки ключей. Трактовка последнего термина, как и нескольких других, заимствована из стандарта ISO/IEC 15408-99.

В криптографическом анализе основными терминами являются метод криптографического анализа, атака на криптосистему, предположения криптоанализа. Ещё раз подчеркнём, что в процессе проведения криптографического анализа должны получаться обоснованные оценки криптографической стойкости криптосистем. Под методом криптографического анализа понимается совокупность приемов и способов, направленных на исследование криптографической стойкости криптосистемы и объединённых одной или несколькими идеями (математическими, техническими или другими). Под атакой на криптосистему понимается попытка нарушения противником и/или нарушителем без-

опасности конкретной реализации криптосистемы. При этом атаки на криптосистему основываются на определённых методах криптоанализа и проводятся с учетом выполнения некоторых предположений криптоанализа.

В словаре приведены лишь основные, наиболее известные методы криптоанализа. Среди них стоит выделить следующие методы: метод полного (тотального) опробования ключей, метод «встреча посередине», метод на основе эквивалентных ключей, дифференциальный метод, линейный метод, корреляционный метод. В соответствии с этими (и другими) методами криптоанализа в словаре рассматриваются и основные виды атак на криптосистемы.

Первая группа терминов, связанных с криптографическим синтезом, служит для определения и характеризации классов криптосистем. Так, шифрсистемы разделяются на симметричные и асимметричные. В симметричной шифрсистеме симметричным образом используются секретные ключи зашифрования и ключи расшифрования. Асимметричные шифрсистемы используют алгоритмы выработки открытых ключей для формирования ключа зашифрования. Наиболее важными классами алгоритмов зашифрования являются поточные алгоритмы зашифрования и блочные алгоритмы зашифрования, используемые в разных режимах шифрования. Криптографическая хеш-функция определяется свойством трудной обнаруживаемости коллизий и коллизий второго прообраза. С системой имитозащиты связаны термины имитовставка и имитостойкость.

Вторая группа терминов в области криптографического синтеза связана с криптографическими примитивами и отдельными типовыми модулями, используемыми при построении криптосистем. К числу первых относятся генератор псевдослучайных последовательностей, комбинирующий генератор, линейный конгруэнтный генератор, фильтрующий генератор, функция усложнения, фильтрующая функция. Практику криптографического синтеза отражают термины управляющая последовательность, управляющий модуль поточной шифрсистемы, шифрующий модуль поточной шифрсистемы, вектор инициализации (синхропосылка).

К третьей группе относятся термины, связанные с реализацией криптосистем: аутентифицированный канал связи, защищенный канал связи, криптографическое устройство, аппаратное шифрование, программное шифрование и т. д.

Современная криптография активно проникает в смежные области информационной безопасности компьютерных систем. Многие новые

криптографические идеи и понятия появились именно благодаря такому проникновению.

В настоящее время в этих смежных областях в основном используются английские термины. При этом у большинства терминов нет устоявшегося и общепринятого перевода на русский язык. Поэтому часто возникают ситуации, когда один и тот же объект имеет много различных названий, например, система разделения доступа, система управления доступом, система контроля доступа. Кроме того, нередко термины в разных источниках определяются по-разному, а термины со сходными названиями несут различную смысловую нагрузку. Например, электронная подпись, в зависимости от ситуации, может означать цифровую подпись, код аутентификации сообщения или некоторую аутентификационную биометрическую информацию.

При этом и в англоязычной литературе система терминов также сформировалась не до конца. В разных общепризнанных источниках используются разные термины. Например, для обозначения свойств хеш-функций с трудно обнаруживаемыми коллизиями используются такие термины, как strongly collision free, collision free, collision resistant, collision intractable, without existential collision и др.

В последние годы одним из основных понятий криптографии стало понятие криптографического протокола, т. е. протокола, предназначенного для выполнения функций криптографической системы, в процессе выполнения которого участники используют алгоритмы криптографические. Дело в том, что в современных распределённых системах существенно расширился круг задач, относящихся к обеспечению безопасности как самой системы, так и циркулирующей в ней информации, причем во многих случаях эти задачи решаются именно криптографическими методами. Поэтому в современную криптографию вошли многие, по сути, интерактивные протоколы, в которых может быть несколько участников, выполняющих свои особые роли. Возможны также различные предположения о том, как строятся отношения доверия межу участниками, и ограничения на порядок взаимодействия.

Криптографические протоколы могут рассматриваться как сами по себе, так и как часть конкретной криптографической системы. Они могут иметь как общий, так и чисто прикладной характер, например, системы электронного документооборота, системы платежей электронных, протоколы голосования и т. п. На данный момент существует не менее двух десятков различных типов криптографических протоколов (тип определяется задачей, решаемой этим протоколом), многие из которых делятся на подтипы. Примером может служить протокол циф-

ровой подписи, имеющий многочисленные подтипы: групповая подпись, пороговая подпись, подпись вслепую, конфиденциальная подпись и т. д. Понятно, что в словаре рассмотрены только общие понятия, относящиеся к криптографическим протоколам, связанные со спецификой криптосистемы, в которую они интегрируются, с учётом принятой в словаре классификации криптосистем. Понятие стойкости криптографического протокола также допускает много различных толкований, зависящих от цели, для которой предназначен протокол, и предположений, в которых производится его анализ.

Важный смысловой ряд терминов словаря группируется вокруг другого основного понятия криптографии — ключа (криптосистемы) — изменяемого элемента (параметра), каждому значению которого однозначно соответствует одно из отображений, реализуемое криптосистемой. Значение этого понятия подчёркивается общепринятым правилом Керкгоффса, согласно которому при криптографическом анализе считают, что описание криптосистемы (протокола криптографического) полностью известно противнику, а криптографическая стойкость основана только на том, что противнику не известен ключ (секретный).

Все возможные значения ключа составляют ключевое множество криптосистемы, которое, как правило, обладает определённой иерархией ключей, т. е. структурностью, связанной с различными функциями, выполняемыми отдельными частями составного ключа.

Важной частью любой криптосистемы является ключевая система, состоящая из ключевого множества и двух подсистем: системы установки ключей (определяющей порядок регистрации ключей, их использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или уничтожения ключей) и системы управления ключами (определяющей алгоритмы и процедуры генерации, распределения, передачи и проверки ключей). Таким образом, определяется весь жизненный цикл ключей, т. е. последовательность стадий, которые проходят ключи от момента генерации до момента уничтожения.

Для надёжных и практически приемлемых ключевых систем требуются такие структуры, как, например, протокол распределения ключей, схема предварительного распределения ключей, открытое распределение ключей или инфраструктура открытых ключей.

Многочисленные функции, выполняемые ключами, свойства ключей и преобразования, выполняемые над ключами, раскрываются в ряде более частных терминов, например, главный ключ, долговременный

ключ, разовый ключ, ключ шифрования данных, ключ шифрования ключей, секретный ключ, открытый ключ, ключ зашифрования, ключ расшифрования, сеансовый ключ, цикловой (раундовый) ключ, развёртывание ключа и др.

Математические термины включались в словарь только в тех случаях, когда они имеют прямое отношение к толкованию тех или иных понятий криптографии. Эти термины принадлежат различным разделам современной математики.

Наиболее многочисленной является группа терминов, берущих свое начало от термина дискретная функция. Большинство этих терминов посвящено толкованию криптографических свойств дискретных функций: аффинное приближение, бент-функция, запрет функции, группа инерции функции, лавинный критерий, корреляционно-иммунное отображение, сбалансированная функция, эластичная функция и др.

Другую важную группу образуют термины теории вероятностей и математической статистики, часто используемые в работах по криптографии. Здесь центральное место занимают понятия истинной случайности и псевдослучайности. Соответственно, в словарь включены термины сложность последовательности по Колмогорову, псевдослучайная последовательность, истинно случайная последовательность, случайная идеальная последовательность, энтропия. Отдельная группа терминов относится к области проверки качества псевдослучайных последовательностей.

Поскольку большинство генераторов псевдослучайных последовательностей вырабатывают рекуррентные последовательности, то в словаре присутствует значительное число терминов по этой тематике: линейная рекуррентная последовательность, многочлен максимального периода, линейная сложность последовательности, усложнение линейной рекуррентной последовательности и др.

Следует привести также примеры отдельных важных математических терминов, включенных в словарь и не входящих в упомянутые выше большие группы: латинский квадрат, дискретный логарифм в конечной группе, регистр сдвига, система уравнений с искажёнными правыми частями, временная сложность алгоритма, хеш-функция, односторонняя хеш-функция, группа точек эллиптической кривой.

Существенной трудностью при работе над математическими терминами являлась необходимость давать краткие, но вместе с тем и математически строгие определения терминов и использовать как можно меньше вспомогательных понятий. К сожалению, это оказалось не всегда возможным.

Для облегчения поиска терминов в словаре принят следующий единый порядок их написания: сначала указывается существительное, а затем — прилагательное и другие части речи.

Работа по составлению словаря выполнялась под научным руководством Б. А. Погорелова и В. Н. Сачкова большим коллективом специалистов. В разное время в ней участвовали В. Д. Аносов. М. И. Анохин, С. М. Буравлёв, Н. П. Варновский, С. А. Гизунов, С. В. Глухов, М. М. Глухов, С. П. Горшков, П. Н. Голованов, А. М. Зубков, А. М. Ивашко, В. Ф. Колчин, А. В. Корольков, В. А. Леонов, О. А. Логачёв, В. А. Носов, А. Б. Пичкур, И. Г. Савастеев, А. А. Сальников, М. Э. Тужилин, М. В. Федюкин, В. М. Фомичёв, И. В. Харламов, А. В. Черемушкин, С. И. Чечёта, А. М. Шойтов, И. А. Юров, В. В. Ященко.

А

Автомат шифрующий [ciphering automaton] — автомат, реализующий *шифрование*. Точнее, автомат, зависящий от параметра, реализующий *зашифрование* или *расшифрование*. Параметр а. ш. (*ключ*) принимает конечное множество значений. От ключа могут зависеть начальное состояние, функции переходов и выходов. При каждом фиксированном значении ключа а. ш. становится обратимым инициальным автоматом.

Алгоритм генерации подписи цифровой [signature generation algorithm] — см. *алгоритм формирования подписи цифровой*.

Алгоритм зашифрования [encryption algorithm] — *алгоритм криптографический*, реализующий *функцию зашифрования*. В случае *шифрсистем блочных* получается использованием *алгоритма зашифрования блочного базового* в конкретном *режиме шифрования*.

Алгоритм зашифрования блочный [block encryption algorithm, block cipher] — *алгоритм зашифрования*, задаваемый *алгоритмом зашифрования блочным базовым* в конкретном *режиме шифрования*.

Алгоритм зашифрования блочный базовый [basic block encryption algorithm] — *алгоритм зашифрования*, реализующий при каждом фиксированном значении *ключа* одно обратимое отображение множества *блоков текста открытого*, имеющих фиксированную длину. Представляет собой алгоритм простой замены блоков текста фиксированной длины.

Алгоритм зашифрования поточный [stream encryption algorithm, stream cipher] — *алгоритм зашифрования*, реализующий при каждом фиксированном значении *ключа* последовательность обратимых отображений (вообще говоря, различных), действующую на последовательность *блоков текста открытого*.

Алгоритм кодирования имитозащищающего [integrity protection algorithm] — *алгоритм криптографический* преобразования информации, обеспечивающий контроль ее *целостности* (как правило за счет внесения избыточности). В отличие от *алгоритма формирования подписи цифровой* использует *криптосистемы симметричные*. Примерами а. к. и. являются *код аутентификации*, некоторые автоматные преобразования и *алгоритмы шифрования*.

Алгоритм криптографический [cryptographic algorithm] — алгоритм, реализующий вычисление одной из *функций криптографических*.

Алгоритм проверки подписи цифровой [signature verification algorithm] — составная часть *схемы подписи цифровой*. Алгоритм, на вход которого подаются *подпись цифровая*, *ключ открытый* и другие откры-

тые параметры схемы подписи цифровой. В схемах *подписи цифровой с восстановлением сообщения* результатом работы алгоритма является заключение о корректности подписи и, если она корректна, — само сообщение, извлеченное из подписи. В остальных случаях сообщение является частью входных данных, и алгоритм проверки выдает лишь заключение о корректности подписи. В некоторых разновидностях схемы подписи цифровой при проверке подписи используется *протокол интерактивный*.

Алгоритм расшифрования [decryption algorithm, deciphering] — *алгоритм криптографический*, обратный к *алгоритму зашифрования* и реализующий *функцию расшифрования*.

Алгоритм формирования подписи цифровой [signature generation algorithm, син. *алгоритм генерации подписи цифровой*] — составная часть *схемы подписи цифровой*. Алгоритм (вообще говоря, рандомизированный), на вход которого подаются подписываемое сообщение, *ключ секретный*, а также открытые параметры схемы подписи цифровой. Результатом работы алгоритма является *подпись цифровая*. В некоторых разновидностях схемы подписи цифровой при формировании подписи используется *протокол*.

Алгоритм хеширования [hashing algorithm] — в *криптографии* — алгоритм, реализующий *хеш-функцию криптографическую*. В математике и программировании — алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале — от всех). Обычно, а. х. преобразует строки произвольной длины в строки фиксированной длины.

Алгоритм шифрования [encryption algorithm] — под алгоритмом шифрования в зависимости от контекста понимается *алгоритм зашифрования* или *алгоритм расшифрования*.

Алгоритм шифрования инволютивный [involutive encryption algorithm] — *алгоритм шифрования*, для которого *алгоритмы зашифрования и расшифрования* совпадают. Другими словами, если к *тексту открытому* дважды применить алгоритм зашифрования, то получится тот же самый открытый текст. Исторически для таких алгоритмов употребляется название «обратимый», но правильно называть их именно «инволютивными», в соответствии с общим пониманием инволюции в математике.

Алгоритм шифрования итеративный [iterative encryption algorithm] — *алгоритм шифрования*, для которого соответствующие *алгоритм зашифрования* и *алгоритм расшифрования* состоят из после-

довательных однотипных *циклов шифрования*. Подобные алгоритмы относительно просто реализуются и позволяют обеспечивать, в частности, *свойство перемешивания*, *свойство рассеивания* и *свойство усложнения*.

Алгоритм шифрования RSA [RSA encryption algorithm] — *алгоритм шифрования*, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения *шифрсистем асимметричных*. Основан на возведении в степень в кольце вычетов по модулю, являющемуся произведением двух больших простых чисел.

Анализ криптографический [cryptanalysis, син. *криптоанализ*] — исследование *системы криптографической* с целью получения обоснованных оценок ее *стойкости криптографической*. Результаты а. к. могут использоваться разработчиком и *пользователем законным криптосистемы* для оценки эффективности системы защиты информации от потенциального *противника* и/или *нарушителя*, а потенциальным противником и/или нарушителем — для подготовки и реализации *атаки на криптосистему*. А. к. проводится путем исследования криптосистемы, а также моделирования (выполнения) различных атак на криптосистему.

Анализ трафика [traffic analysis] — анализ совокупности *сообщений шифрованных*, передаваемых по системе связи, не приводящий к *дешифрованию*, но позволяющий *противнику* и/или *нарушителю* получить косвенную информацию о передаваемых *сообщениях открытых* и в целом о функционировании наблюдаемой системы связи. А. т. использует особенности оформления сообщений шифрованных, их длину, время передачи, данные об отправителе и получателе и т. п.

Анонимность [anonymity] — понятие, родственное *неотслеживаемости*. Выражает предоставляемую *участникам* (*протокола*) возможность выполнять какое-либо действие анонимно, т. е. не идентифицируя себя. При этом, однако, участник обязан доказать свое право на выполнение этого действия. Анонимность бывает абсолютной и отзываемой. В последнем случае в системе есть выделенный участник, *арбитр*, который при определенных условиях может нарушать анонимность и идентифицировать участника, выполнившего данное конкретное действие.

Аппроксимация аффинная [affine approximation] — см. *приближение аффинное*.

Аппроксимация аффинная наилучшая [the best affine approximation] — см. *приближение аффинное наилучшее*.

Арбитр [arbiter] — *участник протокола с арбитром*, выполняющий процедуру *арбитража*.

Арбитраж [arbitration] — формализованная процедура разрешения споров о трактовке результатов выполнения *протокола криптографического*. Такая процедура необходима для многих *протоколов криптографических прикладных*, в т. ч. *схем подписи цифровой*, *протоколов подписания контракта*, *систем платежей электронных* и т. п., и должна рассматриваться как неотъемлемая часть этих протоколов. Для самой процедуры арбитража требуется либо алгоритм, выполняемый арбитром на входных данных, предоставленных ему заявителем (заявителями), либо специальный протокол с участием всех заинтересованных сторон.

Атака адаптивная [adaptive attack] — *атака на криптосистему*, при которой характер воздействия *противника* и/или *нарушителя* может изменяться во времени в зависимости от действий *пользователей законных криптосистемы* или от других условий. Например, противник может подбирать различные исходные данные для воздействия на криптосистему.

Атака адаптивная на основе подобранного сообщения открытого [adaptive chosen-plaintext attack, син. *атака адаптивная по сообщению выбранному*] — *атака адаптивная*, при которой *противник* и/или *нарушитель* имеет возможность вынудить *пользователя законного криптосистемы* к обработке (*зашифрованию*) некоторого *сообщения открытого*, выбранного противником и/или нарушителем, и наблюдать соответствующее *сообщение шифрованное*.

Атака адаптивная на основе подобранного сообщения шифрованного [adaptive chosen-ciphertext attack] — *атака адаптивная*, при которой *противник* и/или *нарушитель* имеет возможность вынудить *пользователя законного криптосистемы* к обработке (*расшифрованию*) некоторого *сообщения шифрованного*, выбранного противником и/или нарушителем, и наблюдать соответствующее *сообщение открытое*.

Атака адаптивная по сообщению выбранному [adaptive chosen-plaintext attack] — см. *атака адаптивная на основе подобранного сообщения открытого*.

Атака активная [active attack] — *атака на криптосистему* или на *протокол криптографический*, при которой *противник* и/или *нарушитель* может влиять на действия *пользователя законного*, например, подменять или удалять сообщения пользователя законного, создавать и передавать сообщения от его имени и т. п.

Атака «встреча посередине» [meet-in-the-middle attack] — *атака на криптосистему*, основанная на *методе «встреча посередине»*.

Атака дифференциальная [differential attack] — см. *атака разностная*.

Атака дифференциально-линейная [differential-linear attack] — см. *атака разностно-линейная*.

Атака корреляционная [correlation attack] — *атака на криптосистему*, основанная на *методе корреляционном*.

Атака линейная [linear attack] — *атака на криптосистему*, основанная на *методе линейном*.

Атака лобовая [brute-force attack] — *атака на криптосистему*, основанная на *методе полного (тотального) опробования ключей*.

Атака на криптосистему [attack on the cryptosystem] — попытка *противника* и/или *нарушителя* понизить уровень безопасности конкретной *системы криптографической* на основе определенных *методов криптоанализа* и при некоторых *предположениях криптоанализа*. Разработчик, *пользователь законный* и противник при проведении *анализа криптографического* моделируют атаки на криптосистему. Совокупность различных атак постоянно расширяется за счет развития теоретических методов и возможностей техники.

Атака на криптосистему на основе известного текста открытого [known plaintext attack] — *атака на криптосистему*, при которой *противнику* и/или *нарушителю* известен *текст открытый*.

Атака на криптосистему на основе только текста шифрованного [ciphertext-only attack] — *атака на криптосистему*, при которой *противнику* и/или *нарушителю* известен *текст шифрованный* и не известен *текст открытый*.

Атака на основе ключей эквивалентных [equivalent keys attack] — *атака на криптосистему*, основанная на *методе ключей эквивалентных*.

Атака на протокол криптографический [attack on the protocol] — попытка проведения анализа сообщений *протокола* и/или выполнения не предусмотренных протоколом действий с целью нарушения работы протокола и/или получения информации, составляющей секрет его *участников*.

Атака на протокол с передачей повторной [replay attack] — *атака на протокол криптографический*, при которой *противник* и/или *нарушитель* записывает все передаваемые сообщения и впоследствии повторно передает их от имени *пользователя законного*.

Атака опробованием последовательным [sequential key search] — *атака на криптосистему*, основанная на *методе последовательного опробования ключа*.

Атака опробованием с использованием памяти [memory using attack, memory-used search attack] — *атака на криптосистему*, основанная на *методе, существенно использующем память*.

Атака пассивная [passive attack] — *атака на криптосистему* или *протокол криптографический*, при которой *противник* и или *нарушитель* наблюдает и использует передаваемые *сообщения шифрованные*, но не влияет на действия *пользователей законных*.

Атака «противник в середине» [man-in-the-middle attack] *атака на протокол криптографический*, в которой *противник* С выполняет этот протокол как с *участником* А, так и с участником В. Противник С выполняет сеанс с участником А от имени В, а с участником В — от имени А. В процессе выполнения противник пересылает сообщения от А к В и обратно, возможно, подменяя их (отсюда название атаки). В частности, в случае *протокола аутентификации абонента* успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для В под именем А. Для осуществления атаки «противник в середине» необходимо обеспечивать синхронизацию двух сеансов протокола.

Атака протяжкой слова вероятного [moving probable word attack] — *атака на криптосистему*, основанная на *методе протяжки слова вероятного*.

Атака разностная [differential attack, син. *атака дифференциальная*] — *атака на криптосистему*, основанная на *методе разностном*.

Атака разностная на основе искажений [differential fault attack] — *атака на криптосистему*, основанная на *методе искажений разностном*.

Атака разностно-линейная [differential-linear attack, син. *атака дифференциально-линейная*] — *атака на криптосистему*, основанная на *методе разностно-линейном*.

Атака со словарем [dictionary attack] — *атака на криптосистему*, использующая словарь элементов *текста открытого*.

Атака со словарем паролей [password attack] — *атака на криптосистему*, основанная на переборе значений *пароля*.

Аутентификация [authentication] — установление (то есть проверка и подтверждение) подлинности различных аспектов информационного взаимодействия: содержания и источника передаваемых сообщений, сеанса связи, времени взаимодействия и т. д. Является важной составной частью проблемы обеспечения достоверности получаемой информации. Особенно остро эта проблема стоит в случае не доверяющих друг другу сторон, когда источником *угроз* может служить не только третья

сторона (*противник*), но и сторона, с которой осуществляется информационное взаимодействие (*нарушитель*).

Аутентификация абонента (пользователя) [user authentication] доказательство абонентом (*пользователем законным*) соответствия своему имени как *участника протокола*. Проводится с целью проверки прав и полномочий абонента. Как правило, осуществляется посредством *протокола идентификации*. См. также *аутентификация сторон*.

Аутентификация взаимная [mutual authentication] — вариант *аутентификации сторон*, при котором каждая из сторон проверяет, что взаимодействующая с ней сторона — именно та, за которую себя выдает. А. в. реализуется таким *протоколом идентификации*, в котором каждый из *участников* является одновременно и доказывающим, и проверяющим. Это позволяет за один сеанс выполнения протокола каждым из участников доказать другому участнику свою идентичность.

Аутентификация интерактивная [interactive authentication] — *аутентификация*, осуществляемая с помощью *протокола интерактивного*.

Аутентификация источника данных [data origin authentication] — проверка и подтверждение того, что набор данных (сообщение, документ) был создан именно заявленным источником. Не надо путать с *аутентификацией* отправителя, так как он мог передать документ, созданный и подписанный другим лицом. А. и. д. предполагает и проверку *целостности*, так как если данные подверглись модификации, то они уже имеют другой источник. Если стороны доверяют друг другу, то А. и. д. можно осуществить применением *шифрсистемы симметричной*, так как правильно *расшифрованное*, либо сообщение с верным значением *кода аутентичности сообщения* подтверждает знание отправителем их общего *ключа секретного*. Для не доверяющих друг другу сторон необходимо использовать *шифрсистему асимметричную*.

Аутентификация квантовая [quantum authentication] — выполнение *аутентификации* с помощью *протокола криптографического квантового*.

Аутентификация односторонняя [one-way authentication] *аутентификация сторон*, при которой одна из сторон проверяет, что взаимодействующая с ней сторона — именно та, за которую себя выдает. А. о. реализуется *протоколом идентификации* с двумя участниками: доказывающим и проверяющим. Термин «односторонняя» используют, чтобы отличить ее от *аутентификации взаимной*.

Аутентификация сообщения [message authentication] — проверка того, что сообщение было получено неповрежденным, неизмененным (с момента отправления), то есть проверка *целостности*. Если стороны доверяют друг другу, то а. с. осуществляется применением *системы имитозащиты*. Для не доверяющих друг другу сторон необходимо использовать *систему подписи цифровой*.

Аутентификация сторон [entity authentication] — проверка одной из сторон (или обеими сторонами) того, что взаимодействующая с ней сторона — именно та, за которую себя выдает. Если стороны доверяют друг другу, то а. с. можно осуществить применением *шифрсистемы симметричной* (или *системы имитозащиты*), так как сообщение, правильно *расшифрованное* либо с верным значением *кода аутентичности сообщения* подтверждает знание отправителем их общего *ключа секретного*. Для не доверяющих друг другу сторон необходимо использовать *шифрсистему асимметричную* (*систему идентификации* или *систему подписи цифровой*).

Б

Бент-отображение [bent mapping] — отображение $f\colon Z_q^n \to Z_q^m$, у которого для любого фиксированного ненулевого элемента $w \in Z_q^n$ разность $f(x+w) - f(x)$ принимает каждое значение $v \in Z_q^m$ ровно для q^{n-m} значений $x \in Z_q^n$.

Бент-функция булева [bent function] — булева функция, для которой модули всех коэффициентов Уолша—Адамара равны между собой. Класс б.-ф. б. совпадает с классом *функций совершенно нелинейных*. См. также *преобразование Уолша—Адамара*.

Бент-функция q-значная [q-value bent function] — 1. *Бент-отображение* $f\colon Z_q^n \to Z_q^m$ при $m = 1$. Это понятие совпадает с понятием *функции негомоморфной совершенно*. 2. В терминах преобразования Фурье *функция дискретная* f называется *бент-функцией q-значной*, если модули всех коэффициентов Фурье для нетривиальных характеров функции f равны между собой.

Биграмма [digram] — пара букв (символов), *блоков текста*.

Блок текста [text block] — *мультиграмма* текста (*текста открытого*, *текста шифрованного* или промежуточного), составленная из подряд идущих знаков. Обычно текст разбивается на блоки одинаковой длины.

Блокнот одноразовый [one-time pad] — записанный на некотором материальном носителе (например, в специальных бумажных блокно-

тах) набор данных, используемых для получения *последовательностей управляющих* для однократного *шифрования*. Этот набор данных, обладающий определенными свойствами, должен обеспечивать *стойкость* (*шифрсистемы*) *совершенную* при однократном применении.

Бумажник электронный [e-wallet, wallet] — специальное электронное устройство, предназначенное для решения *проблемы повторной траты денег электронных*. Б. э., выдаваемый клиенту банка, состоит из компьютера, которому доверяет клиент, и защищенного модуля, называемого *наблюдателем*, которому доверяет банк. Наблюдатель имеет возможность общаться с «внешним миром» только через компьютер клиента. Клиент не может потратить *деньги цифровые* без санкции наблюдателя; тем самым предотвращается повторная трата денег электронных. *Протоколы криптографические системы платежей электронных автономной* с б. э. обеспечивают *неотслеживаемость* действий клиентов, даже если и банк, и наблюдатель нечестные, и информация, накопленная банком, сопоставляется с содержимым наблюдателя.

В

Вектор инициализации [initialization vector] — вектор, который передается по каналу управления и используется для инициализации *алгоритма шифрования*. См. также *синхропосылка*.

Вес функции булевой [weight of Boolean function] — число двоичных наборов в табличном задании булевой функции, на которых функция принимает значение «1».

Время жизни ключа [key life period, key life time] — временной интервал *цикла жизненного ключа* от генерации до уничтожения.

Г

Гамма (шифра) [keystream, ciphering sequence, key sequence] — *последовательность управляющая* знаков (блоков) алфавита, используемая в *шифрсистемах поточных*, реализующих *гаммирование*. Для обеспечения *стойкости криптографической* г. должна удовлетворять ряду требований, в частности, быть близкой по своим свойствам к реализации *последовательности случайной идеальной*.

Гаммирование [running key ciphering, one-time padding] — *шифрование*, в котором *функция зашифрования* $f(\gamma, x)$ обратима по каждой переменной (γ обозначает знак (блок) *гаммы шифра*, x — знак (блок)

текста открытого, значение функции $f(\gamma, x)$ — знак (блок) *текста шифрованного*). Важным частным случаем является так называемое модульное гаммирование, когда $f(\gamma, x) = x + \gamma \pmod N$, где N — размер числового алфавита $\{0, 1, \ldots, N-1\}$, из которого выбираются γ и x.

Генератор битов псевдослучайных криптографически сильный [cryptographically strong pseudorandom bit generator] — см. *генератор последовательностей псевдослучайных криптографически сильный.*

Генератор ключей [key generator] — техническое устройство или программа, предназначенные для выработки массивов чисел или других данных, используемых в качестве ключей (криптосистемы), последовательности ключевой, векторов инициализации и т. п.

Генератор комбинирующий [combination generator, combiner] — генератор, у которого выходная последовательность $v(1), v(2), \ldots$ образована с использованием n *последовательностей линейных рекуррентных* $u_j(1), u_j(2), \ldots$ $(j = 1, \ldots, n)$ над кольцом R и функции $f(x_1, \ldots, x_n)\colon R^n \to R$, называемой *функцией усложнения*, по следующему правилу: $v(i) = f(u_1(i), \ldots, u_n(i))$, $i = 1, 2, \ldots$

Генератор линейный конгруэнтный [linear congruent generator] — генератор, порождающий *последовательность линейную конгруэнтную* $v(1), v(2), \ldots$

Генератор подстановок псевдослучайных [pseudorandom permutation generator] — *генератор функций псевдослучайных* из семейства, в котором каждая функция является подстановкой.

Генератор последовательностей псевдослучайных [pseudorandom generator] — техническое устройство или программа для выработки *последовательностей псевдослучайных.*

Генератор последовательностей псевдослучайных квантовый [quantum pseudorandom generator] — *генератор последовательностей псевдослучайных*, основанный на использовании квантовых эффектов.

Генератор последовательностей псевдослучайных криптографически сильный [cryptographically strong pseudorandom bit generator, син. *генератор битов псевдослучайных криптографически сильный*] — математическая модель *генератора последовательностей псевдослучайных*, выходом которого являются *последовательности псевдослучайные*, неотличимые эффективно (с полиномиальной сложностью) статистическими тестами от *последовательностей случайных идеальных.*

Генератор с неравномерным движением [irregularly clocked generator, clock-controlled generator] — генератор, построенный на основе

регистров сдвига, при этом выходные последовательности одних регистров используются для управления движением других регистров. Такой способ позволяет строить на основе линейных отображений, реализуемых регистрами сдвига, нелинейные преобразования множества состояний генератора.

Генератор фильтрующий [filter generator] — генератор *последовательности управляющей* $v(1), v(2), \ldots$, образованной с использованием *последовательности линейной рекуррентной* $u(1), u(2), \ldots$ над кольцом R и *функции усложнения* $f\colon R^n \to R$, называемой *функцией фильтрующей*, по следующему правилу: $v(i) = f(u(i), \ldots, u(i+n-1))$, $i = 1, 2, \ldots$

Генератор функций псевдослучайных [pseudorandom function generator] — алгоритм, который псевдослучайным образом выбирает функцию из заданного *семейства функций псевдослучайных*.

Генератор функций с секретом [trapdoor function generator] — см. *функция с секретом*.

Группа инерции функции [stabilizer group of function] — для *функции дискретной* $f\colon X^n \to X$ и некоторой группы преобразований G множества X^n группу инерции функции f относительно группы G образуют все $g \in G$, для которых $f(g(x_1, \ldots, x_n)) \equiv f(x_1, \ldots, x_n)$.

Группа точек кривой эллиптической [elliptic curve group] — абелева группа на множестве точек эллиптической кривой над некоторым полем P. Точками эллиптической кривой являются пары (x, y), удовлетворяющие уравнению $y^2 = x^3 + a \cdot x + b$, $a, b \in P$, $4a^3 + 27b^2 \neq 0$, и специальный дополнительный элемент. Г. т. к. э. применяются при построении *систем криптографических*, при решении *задачи логарифмирования дискретного*, *задачи факторизации чисел целых* и др.

Д

Деньги виртуальные [virtual money] — платежные средства, представляющие собой записи (в т. н. виртуальном бумажнике или персональном компьютере) о наличии условных единиц, приобретаемых заранее в качестве предоплаты конкретных услуг (телефонные карты, электронные жетоны и др.). Имеют заранее определенное назначение и ограниченное хождение. Обеспечивают возможность отслеживания транзакций.

Деньги цифровые [digital money, digiCash, WEB-money, e-cash, e-coin] — платежные средства, представляющие собой зашифрованные

записи (в т. н. *бумажнике электронном*), используемые для взаиморасчетов в компьютерной сети и существующие исключительно в электронной форме (электронная наличность (e-cash), *монета электронная* (e-coin)). Достоверность д. ц. проверяется с помощью *ключа открытого подписи цифровой* банка-эмитента. Целью защиты является невозможность подделки и повторной траты д. ц., а также обеспечение *анонимности* покупателя. Создание *системы платежей электронных* с использованием д. ц. требует решения таких задач, как: обеспечение *конфиденциальности*, *целостности*, *аутентификации*, *невозможности отказа*, *анонимности* и *неотслеживаемости*. Одной из характеристик, отличающих д. ц. от других электронных средств платежа, является возможность совершения полностью анонимных транзакций, в которых отсутствует связь между платежными средствами и личностью их держателя.

Деньги электронные [electronic money, e-money] — банковские платежные средства, представляющие собой записи (в так называемом электронном кошельке) о наличии реальных денежных средств, которыми обладает некоторое лицо. Реализованы в системах смарт-карт. Защита хранимого значения основывается на невозможности создания фальшивой карты или осуществления операций с использованием чужой карты. Для защиты платежей применяются *системы криптографические*, обеспечивающие *конфиденциальность*, *целостность*, *аутентификацию* и *невозможность отказа*. В широком смысле, д. э. — форма организации денежного обращения с использованием компьютерных сетей.

Депонирование ключей [key escrow] — хранение копии *ключа криптосистемы* у доверенного лица (организации, *участника протокола* и т. п.) с целью восстановления работоспособности *криптосистемы*, например, в случае утери ключа.

Дешифрование [decryption, breaking of cryptosystem] — процесс аналитического раскрытия *противником* и/или *нарушителем сообщения открытого* без предварительного полного знания всех элементов *системы криптографической*. Если этот процесс поддается математической формализации, говорят об алгоритме дешифрования.

Длина (размер) ключа [key length] — длина слова в определённом алфавите, представляющего *ключ*. Длина *ключа бинарного* измеряется в битах.

Длина покрытия группы [group cover length] — наименьшее k, для которого конечная группа G с системой образующих M представима в виде $G = M \cup M^2 \cup \ldots \cup M^k$.

Доказательство знания [proof of knowledge, син. *протокол доказательства знания*] — *доказательство интерактивное*, при котором доказывающий убеждает проверяющего в том, что он владеет секретной информацией, не раскрывая её. Д. з. характеризуется двумя свойствами: *полнотой* (*протокола*) и *корректностью* (*протокола*). К категории д. з. относятся *протоколы идентификации*.

Доказательство интерактивное [interactive proof] — понятие теории сложности вычислений, составляющее основу понятия *доказательства с разглашением нулевым*. Д. и. — доказательство путем выполнения *протокола* с двумя *участниками*, доказывающим и проверяющим, в процессе работы которых участники обмениваются сообщениями (запросы и ответы), обычно зависящими от случайных чисел, которые могут содержаться в секрете. Цель доказывающего — убедить проверяющего в истинности некоторого утверждения. Проверяющий либо принимает, либо отвергает доказательство. В отличие от обычного математического понятия доказательства в данном случае доказательство носит не абсолютный, а вероятностный характер и характеризуется двумя вероятностями. Если доказываемое утверждение верно, то доказательство должно быть верным с вероятностью, стремящейся к единице при увеличении числа *циклов протокола*. Если же доказываемое утверждение ложно, то при увеличении числа *циклов протокола* вероятность правильности доказательства должна стремиться к нулю. Криптографическое качество протокола д. и. характеризуется свойствами *полноты*, *корректности* и *разглашения нулевого*.

Доказательство не интерактивное с разглашением нулевым [noninteractive zero-knowledge proof] — *доказательство с разглашением нулевым*, выполняемое за один *цикл* (*протокола*): доказывающий посылает сообщение проверяющему, который на основе анализа этого сообщения либо принимает, либо отвергает доказательство.

Доказательство с разглашением минимальным [minimum-knowledge proof] — вид *доказательства интерактивного*, решающего задачу распознавания языка, и удовлетворяющего требованиям к *стойкости криптографической*, которые аналогичны требованиям к стойкости *доказательств с разглашением нулевым*. В д. с р. м. для данного фиксированного языка L общим входом доказывающего и проверяющего может быть произвольная строка x. Доказывающий должен определить, принадлежит ли эта строка языку L, и сообщить результат ($x \in L$ или $x \notin L$) проверяющему. При этом проверяющий, даже нечестный, не получает по завершении доказательства никакой дополнительной информации, за исключением значения предиката $x \in L$. Для *противника*,

перехватывающего сообщения в процессе доказательства, случаи $x \in L$ и $x \notin L$ должны быть неразличимы.

Доказательство с разглашением нулевым [zero-knowledge proof] — *доказательство знания*, которое обладает свойством *разглашения нулевого*.

Доказательство с разглашением нулевым совершенное [perfect zero-knowledge proof] — предельный случай *доказательства с разглашением нулевым*, в котором количество дополнительной информации, которую может получить проверяющий в результате выполнения *протокола*, равно нулю.

Доля секрета [share, secret share] — ключевая информация, получаемая отдельным *участником схемы разделения секрета*, позволяющая ему вместе с другими участниками правомочной коалиции восстановить значение секрета. См. также *структура доступа*.

З

Загрузчик ключевой [key gun] — устройство для безопасной транспортировки и загрузки *ключа* (*криптосистемы*). Имеет физическую и логическую защиту от несанкционированного считывания.

Задача логарифмирования дискретного [discrete logarithm problem] — задача нахождения *логарифма дискретного в группе конечной*. В последние десятилетия интерес к з. л. д. существенно усилился в связи с синтезом *шифрсистем асимметричных*. Разработан ряд алгоритмов логарифмирования в мультипликативных группах конечных полей и других конечных группах.

Задача факторизации чисел целых [integer factoring problem] — задача разложения целого положительного числа в произведение простых чисел. З. ф. ч. ц. является классической математической задачей. В последние десятилетия интерес к ней существенно усилился в связи с синтезом *шифрсистем асимметричных*. Разработан ряд алгоритмов факторизации целых чисел.

Запрет функции [interdiction of function, prohibition of function] — для *функции дискретной* $f\colon X^n \to X$ запрет — это упорядоченный набор знаков $a_1, \ldots, a_t$ алфавита X, для которого система уравнений $f(b_i, \ldots, b_{i+n}) = a_i$, $i = 1, 2, \ldots, t$ относительно неизвестных $b_1, \ldots, b_{t+n}$ не имеет решений. В *криптографии* понятие з. ф. возникает в связи с анализом *генераторов фильтрующих*.

Зашифрование [encryption, enciphering] — процесс преобразования $f_k\colon x \to y$ *сообщения открытого* x *в сообщение шифрованное* y с помо-

щью инъективной функции f_k, зависящей от *ключа* k из *множества ключевого* (*криптосистемы*). З. должно нарушать лингвистические и статистические связи в исходном открытом сообщении. *Функция зашифрования* f_k и *функция расшифрования* f_k^{-1} при любом значении ключа k должны допускать простую техническую реализацию. При неизвестном *ключе секретном* для каждого открытого сообщения x задача определения этого сообщения, или хотя бы близкого к нему (в некотором смысле), исходя из заданного множества $\{x_s = f_s^{-1}(y_k) \mid s \in K\}$, должна с заданной надежностью характеризоваться высокой сложностью (теоретико-информационной, алгоритмической и вычислительной). См. также *алгоритм зашифрования*, *стойкость криптографическая*.

И

Идентификатор ключа [key identifier] — указатель на *ключ*, представляющий собой системное имя ключа в программной реализации *алгоритма криптографического* и имеющий установленный в системе формат. Используется в качестве переменной при записи различных *операций криптографических* в тексте программы.

Идентификация [identification] — процедура установления присвоенного данной стороне уникального системного имени — идентификатора, которое позволяет отличать ее от других сторон. Обычно процедура идентификации заключается в предъявлении этого имени и предшествует процедуре *аутентификации*, то есть подтверждению правильности идентификации. Термин и. часто для краткости используют для обозначения общей процедуры идентификации/аутентификации сторон (см., например, *протокол идентификации*).

Идентификация пользователя (в системе информационной) [user identification in an information system] — присвоение пользователям идентификаторов и проверка вхождения предъявляемых идентификаторов в список присвоенных идентификаторов. Обязательно должна дополняться *аутентификацией* — проверкой принадлежности пользователю предъявленного им идентификатора.

Идентификация с разглашением нулевым [zero-knowledge identification] — вид *доказательства с разглашением нулевым*, целью которого является *аутентификация сторон*, т. е. доказательство одним из участников своей идентичности.

Иерархия ключей [hierarchy of keys] — структура *множества ключевого криптосистемы*, отражающая различные функции, выполня-

емые отдельными частями *ключа составного*. Например, множество ключевое криптосистемы может иметь древовидную структуру, если каждый ключ состоит из двух подключей: общего для всех *пользователей законных* сети связи *ключа долговременного* и уникального для каждого сеанса связи *ключа разового*. Ключевое множество может иметь также матричную структуру, если каждый ключ состоит из трёх подключей: уникального для каждой пары пользователей и каждого сеанса связи *ключа разового*, уникального для каждой пары пользователей *ключа долговременного* для шифрования разовых ключей и индивидуального *ключа главного* пользователя для хранения в зашифрованном виде долговременного ключа.

Имитация [imitation] — *атака активная* на *протокол криптографический*, целью которой является навязывание *противником* и/или *нарушителем* одной из сторон сообщения от имени другой стороны, которое не будет отвергнуто при приеме.

Имитовставка [massage authentication code] — см. *код аутентичности сообщения*.

Имитозащита [integrity protection, protection from imitation] — защита сообщений в системе связи от навязывания ложных данных.

Имитостойкость [imitation resistance] — свойство *системы криптографической* (*протокола криптографического*), характеризующее способность противостоять *атакам активным* со стороны *противника* и/или *нарушителя*, целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных.

Инфраструктура ключей открытых [public key infrastructure] — подсистема *системы ключевой шифрсистемы асимметричной*. Предназначена для обеспечения (с помощью *сертификатов ключей*) доверия *пользователей законных* к подлинности *ключей*, соответствия ключей пользователям и оговоренным условиям их применения.

K

Канал связи [communication channel] — совокупность технических устройств, обеспечивающих передачу информации.

Канал связи аутентифицированный [authenticated communication channel] — *канал связи*, обеспечивающий *целостность* передаваемой по нему информации.

Канал связи защищенный [private communication channel] — *канал связи*, обеспечивающий недоступность пересылаемой по нему ин-

формации *противнику пассивному*. К. с. з. моделируется протоколом конфиденциальной передачи сообщений. Для других типов *протоколов криптографических* к. с. з. может служить *примитивом криптографическим*.

Канал связи квантовый [quantum communication channel] — *канал связи* для передачи информации, основанный на принципах квантовой физики.

Квадрат латинский [Latin square] — матрица размеров $n \times n$, у которой каждая строка и каждый столбец являются перестановкой элементов некоторого конечного алфавита из n элементов. В *криптографии* к. л. используются, например, для задания *функции зашифрования* при *гаммировании*.

Квадраты латинские ортогональные [orthogonal Latin squares] — два *квадрата латинских* размера $n \times n$, составленные из элементов множества $\{1, 2, \ldots, n\}$, при совмещении которых друг с другом получается таблица, содержащая в своих клетках все n^2 возможных упорядоченных пар чисел. В *криптографии* к. л. о. используются, например, для обеспечения *имитостойкости*.

Ключ «отбеливания» [whitening key] — бинарный подключ *алгоритма зашифрования блочного базового*, размер которого совпадает с размером *блока текста* и который используется в первом и последнем *цикле шифрования*. Обычно используется пара к. о., один из них поразрядно складывается по модулю 2 с *блоком текста открытого*, после чего эта сумма преобразуется в блок текста, сумма которого по модулю 2 с другим к. о. образует *блок текста шифрованного*.

Ключ (криптосистемы) [key (of a cryptosystem)] — изменяемый элемент (параметр), каждому значению которого однозначно соответствует одно из отображений, реализуемых *криптосистемой*. Все возможные значения ключа составляют *множество ключевое криптосистемы*. Ключи могут быть составными, т. е. содержать несколько частей, обеспечивающих различные функции криптосистемы. Например, при реализации *алгоритма шифрования* электронной схемой в качестве ключей могут использоваться начальные состояния элементов памяти схемы, функциональные узлы и др.

Ключ бинарный [binary key] — *ключ*, заданный вектором с двоичными координатами.

Ключ главный [master key] — элемент *ключа составного*, который используется для шифрования *ключей шифрования ключей*, предназначенных для шифрования *ключей разовых* или для генерации других видов ключей посредством *шифрования* определённых данных.

Ключ долговременный [long-term key] — элемент *ключей составных*, действующий в неизменном виде длительное время.

Ключ зашифрования [enciphering key] — *ключ*, используемый при *зашифровании*.

Ключ коммутаторный [commutation key] — *ключ*, являющийся подстановкой степени n или бесповторной выборкой размера m из n элементов, $m < n$. Например, в *шифре замены простой* ключ представляет собой подстановку на множестве *блоков текста*.

Ключ открытый [public key] — несекретный *ключ шифрсистемы асимметричной*.

Ключ разовый [once-only key] — *ключ*, однократно используемый для *шифрования* в *цикле жизненном ключей*. Обычно не подлежит хранению и является элементом *ключа составного*.

Ключ расшифрования [decryption key] — *ключ*, используемый при *расшифровании*.

Ключ сеансовый [session key] — *ключ*, специально сгенерированный для одного сеанса связи между двумя *участниками* (*протокола*).

Ключ секретный [secret key] — *ключ*, сохраняемый в секрете от лиц, не имеющих допуска к ключам данной *шифрсистемы симметричной* или к использованию некоторых функций данной *шифрсистемы асимметричной*.

Ключ секретный квантовый [quantum secret key] — *ключ секретный*, полученный в ходе реализации *распределения ключей квантового*. Выделен как самостоятельный термин ввиду принципиальной важности задачи безопасного распределения секретных ключей среди участников защищенной сети; эта задача может быть удовлетворительно решена только при помощи *канала связи*, гарантированно защищенного от перехвата, например, *канала связи квантового*.

Ключ скомпрометированный [compromised key] — *ключ секретный*, ставший доступным лицам, не имеющим допуска к ключам данной *шифрсистемы симметричной* или к использованию некоторых функций данной *шифрсистемы асимметричной*.

Ключ слабый [weak key] — *ключ криптосистемы*, при котором заметно ухудшаются характеристики *стойкости криптографической* криптосистемы по сравнению со средними значениями тех же характеристик при ключе, случайно равновероятно выбранном из *множества ключевого криптосистемы*.

Ключ составной [composite key] — см. *ключ* (*криптосистемы*).

Ключ цикловой (раундовый) [round key] — набор, вычисляемый по *ключу секретному алгоритма шифрования итеративного* в про-

цессе *развертывания ключа*. Используется для преобразования блока информации на одном из *циклов* (*раундов*) *шифрования*.

Ключ шифрования данных [data encryption key] — элемент *ключа составного*, предназначенный для *шифрования* данных.

Ключ шифрования ключей [key enciphering key (KEK)] — элемент *ключа составного*, используемый для шифрования *ключей разовых*.

Ключи эквивалентные [equivalent keys] — *ключи*, при которых *криптосистема* реализует одинаковые отображения.

Код аутентификации [authentication code, син. *хеш-функция криптографическая задаваемая ключом*] — вид *алгоритма кодирования имитозащищающего* информации. Как правило, к. а. сопоставляет сообщению его *код аутентичности сообщения*. Алгоритм принятия решения о подлинности информации основан на проверке значения кода аутентичности сообщения. К к. а. предъявляются требования: невозможность вычисления кода аутентичности для заданного сообщения без знания *ключа*; невозможность подбора для одного или нескольких сообщений с известными значениями кода аутентичности другого сообщения с известным значением кода аутентичности без знания ключа.

Код аутентичности сообщения [message authentication code, seal; integrity check value, син. *имитовставка*] — в *протоколах аутентификации сообщений* с доверяющими друг другу *участниками* — специальный набор символов, добавляемый к сообщению и предназначенный для обеспечения его *целостности* и *аутентификации источника данных*.

Коллизия [collision, existential collision] — для *хеш-функции* h — такая пара значений x, y ее аргумента, что $x \neq y$ и $h(x) = h(y)$.

Коллизия прообраза второго [second preimage collision, син. *коллизия специфическая*] — для *хеш-функции* h и заданного значения x ее аргумента — значение аргумента y ($\neq x$) такое, что $h(x) = h(y)$.

Коллизия специфическая [specific collision] — см. *коллизия прообраза второго*.

Компрометация абонента [compromise of a party] — факт ознакомления *противника* и/или *нарушителя* с *ключами секретными* абонента защищенной сети связи (*пользователя законного*, *участника* (*протокола*)). Может иметь явный или тайный характер.

Конфиденциальность (информации) [privacy, confidentiality] — означает, что информация предназначена только определенному кругу лиц и должна храниться в тайне от всех остальных.

Конфиденциальность трафика [traffic (flaw) confidentiality] — свойство, характеризующее защищенность системы связи от получения *противником* и/или *нарушителем* информации о передаваемых в си-

стеме данных и/или функционировании системы в целом путем *анализа трафика*. Защита от анализа трафика обеспечивается путем сокрытия идентификаторов и адресов отправителя и получателя, длин пакетов, интенсивности передач, и т. п.

Корректность (протокола) [soundness property] — способность *протокола криптографического* противостоять *угрозам* со стороны *противника* и/или *нарушителя*, не располагающего необходимой секретной информацией, но пытающегося выполнить протокол за *участника*, который по определению должен такой информацией владеть.

Корреляция функций [correlation of functions] — см. *коэффициент корреляции функций*.

Коэффициент корреляции функций [correlation coefficient of functions] — коэффициент корреляции для булевых функций f и g от n переменных — это рациональное число

$$C(f;\, g) = \frac{1}{2^n} \cdot \sum_{x \in \{0,1\}^n} (-1)^{f(x)+g(x)}.$$

В терминах *функции кросс-корреляции* имеет место равенство $C(f;\, g) = C_{f,g}(0)$.

Крипто API [crypto API (application programming interface)] — криптографический интерфейс прикладного программирования, определяющий порядок обращения прикладных программ к библиотеке функций/программ, реализующих элементарные *функции криптографические* и *операции криптографические*.

Криптоанализ [cryptanalysis] — см. *анализ криптографический*.

Криптоанализ квантовый [quantum cryptanalysis] — *анализ криптографический*, основанный на применении алгоритмов квантовых вычислений.

Криптоаналитик [cryptanalyst] — специалист, занимающийся *анализом криптографическим криптосистем*.

Криптограмма [cryptogram] — *сообщение шифрованное*, оформленное по действующим правилам пользования *системой шифрования*. Содержит, кроме *текста шифрованного*, адрес, грифы срочности и др. служебную информацию.

Криптография [cryptography] — область научных, прикладных, инженерно-технических исследований и практической деятельности, которая связана с разработкой *средств криптографических* защиты информации от *угроз* со стороны *противника* и/или *нарушителя*, а также анализом и обоснованием их *стойкости криптографической*. В настоящее время основными задачами к. являются обеспечение *конфиденци-*

альности, *целостности*, *аутентификации*, *невозможности отказа*, *неотслеживаемости*. В отличие от организационных и других способов защиты информации, под криптографическими понимаются такие, которые используют математические методы преобразования защищаемой информации. К., с некоторой долей условности, делится на: *криптосинтез* и *криптоанализ*; к. включает *криптологию*.

Криптография квантовая [quantum cryptography] — раздел *криптографии*, посвященный применению методов квантовой физики для синтеза и анализа *систем криптографических*.

Криптография компьютерная [computer cryptography] — общее название области криптографических исследований, связанной с применением *криптографии* для обеспечения компьютерной безопасности. Изучает особенности реализации *систем криптографических* в операционных системах, компьютерных сетях, системах управления базами данных и т. п.

Криптология (математическая криптография) [cryptology (mathematical cryptography)] — отрасль *криптографии*, математики и математической кибернетики, изучающая математические модели *систем криптографических*. Так же, как и *криптография*, условно делится на две части: *криптосинтез* и *криптоанализ*.

Криптомаршрутизатор [cryptorouter] — программное средство (маршрутизатор), осуществляющее *туннелирование* исходящих и входящих пакетов, а также *зашифрование* исходящих и *расшифрование* входящих пакетов. Множество закрытых маршрутов всех взаимодействующих к. образует виртуальную частную сеть в общей сети. Информация, пересылаемая к., зашифрована на *ключах* парной связи между соответствующими к. Обмен *ключами* по сети отсутствует. Для закрытия информации и топологии внутренних подсетей применяется принцип инкапсуляции, то есть вложения передаваемых пакетов в другие, со скрытием внутренних адресов.

Криптопровайдер [cryptoprovider] — программное средство, обеспечивающее работу пользователя с *множеством ключевым криптосистемы* без получения непосредственного доступа к нему. К. должен соответствовать действующим стандартам, реализовывать *алгоритмы шифрования*, *алгоритмы формирования подписи цифровой*, *алгоритмы проверки подписи цифровой*, обеспечивая защиту множества ключевого криптосистемы от непреднамеренной или случайной компрометации.

Криптопротокол [cryptoprotocol] — см. *протокол криптографический*.

Криптосервер [cryptoserver] — особо выделенная в сети рабочая станция, на которой создана доверенная среда и локализовано хранение информации о *ключах*, и выполнение *операций криптографических*. Обращение к к. осуществляется посредством вызовов функций, реализованных в его программном обеспечении.

Криптосинтез [cryptosynthesis] — см. *синтез криптографический*.

Криптосистема [cryptosystem] — см. *система криптографическая*.

Криптофильтр [cryptofilter] — устройство, осуществляющее автоматическое *шифрование* пакетов, имеющее ровно два интерфейса и не имеющее своих сетевых адресов. Для обеспечения нормальной работы к. должен содержать: список сетевых адресов подсетей, с которыми может осуществляться связь; матрицу *ключей* парной связи между подсетями; список сетевых адресов компьютеров внутренней подсети, доступных извне для генерации пакетов и формирования ответов маршрутизатору; сетевой адрес маршрутизатора, подключенного к внешнему интерфейсу.

Критерий лавинный [avalanche criterion] — условие на отображение $f\colon \{0,1\}^n \to \{0,1\}^m$, состоящее в выполнении равенств

$$\sum_{x\in\{0,1\}^n} \|f(x)+f(x+e_i)\| = m\cdot 2^{n-1} \quad \text{для всех } i\in\{1,\ldots,n\}.$$

Здесь $\|a\|$ — вес Хемминга вектора $a\in\{0,1\}^m$, а $e_1,\ldots,e_n$ — стандартный базис пространства $\{0,1\}^n$.

Критерий лавинный строгий [strict avalanche criterion] — условие на отображение $f\colon \{0,1\}^n \to \{0,1\}^m$, состоящее в том, что всех $i\in\{1,\ldots,n\}$ целочисленная покоординатная сумма

$$\sum_{x\in\{0,1\}^n} (f(x)+f(x+e_i))$$

равна $(2^{n-1},\ldots,2^{n-1})$. Здесь $e_1,\ldots,e_n$ — стандартный базис пространства $\{0,1\}^n$. Отображение f, удовлетворяющее к. л. с., удовлетворяет и *критерию лавинному*.

Критерий лавинный строгий порядка m [strict avalanche criterion of order m] — условие на булеву функцию f от n переменных, состоящее в том, что при любой фиксации не более, чем m переменных, получающаяся функция удовлетворяет *критерию лавинному строгому*.

Критерий распространения относительно вектора [propagation criterion with respect to a vector] — условие на булеву функ-

цию f от n переменных и вектор $\alpha \in \{0, 1\}^n$, состоящее в том, что $f(x) + f(x + \alpha)$ — *функция сбалансированная*.

Критерий распространения степени k [propagation criterion of degree k] — булева функция f от n переменных удовлетворяет критерию распространения степени k, если она удовлетворяет *критерию распространения относительно* любого ненулевого *вектора*, вес которого не превосходит k. Данное понятие обобщает понятие *критерия лавинного* для булевых функций.

Критерий распространения степени k порядка m [propagation criterion of degree k and order m] — условие на булеву функцию f от n переменных, состоящее в том, что при любой фиксации любых m переменных получающаяся функция удовлетворяет *критерию распространения степени k*.

Л

Логарифм дискретный в группе конечной [discrete logarithm in a finite group] — минимальное целое положительное решение x уравнения $a^x = b$, где a, b — элементы конечной группы G. Наиболее часто в *криптографии* при анализе *шифрсистем асимметричных* рассматривают *логарифм дискретный в поле конечном* и логарифм дискретный в *группе точек кривой эллиптической*.

Логарифм дискретный в поле конечном [discrete logarithm in a finite field] — *логарифм дискретный в группе конечной* в случае, когда группа является мультипликативной группой конечного поля.

М

Матрица Адамара [Hadamard matrix] — матрица H размера $n \times n$ с элементами 1 или -1 такая, что $HH^t = nE_n$, где H^t — транспонированная матрица H, а E_n — единичная матрица.

Матрица разреженная [sparse matrix] — матрица с малым числом ненулевых элементов. Для систем линейных уравнений с разреженными матрицами существуют эффективные методы решения. Такие системы возникают, например, при решении *задачи логарифмирования дискретного* и *задачи факторизации чисел целых*.

Матрица Сильвестра—Адамара [Sylvester—Hadamard matrix, син. *матрица Уолша—Адамара*] — частный случай *матрицы Адамара*. Матрица H_m размера $2^m \times 2^m$, которая порождается с помощью опе-

рации тензорного произведения матриц рекуррентным соотношением $H_m = H_1 \otimes H_{m-1}$, $m = 2, 3, \ldots$, $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Матрица Уолша—Адамара [Walsh—Hadamard matrix] — см. *матрица Сильвестра—Адамара.*

Метка временная [timestamp] — информация о времени создания сообщения (электронного документа), добавляемая к этому сообщению (документу) с целью ее использования при проверке и подтверждении *целостности* документа. М. в. должна обладать свойствами, напоминающими свойства *подписи цифровой*: невозможность *подмены* (в т. ч. перенесения на другой электронный документ), невозможность изменения даты и (или) времени и т. д.

Метод анализа криптографического (криптоанализа) [cryptanalytic method, method of cryptanalysis] — совокупность приемов и способов, направленных на исследование *стойкости криптографической криптосистемы*, объединенных одной или несколькими идеями (математическими, техническими или другими). Можно предположить, что и разработчик криптосистем, и *противник* и/или *нарушитель* используют одну и ту же совокупность м. к. а. В качестве наиболее важных характеристик м. к. а. обычно рассматривают трудоемкость м. а. к. и надежность м. а. к.

Метод «встреча посередине» [meet-in-the-middle attack] — *метод анализа криптографического*, состоящий из двух этапов. Первоначально *ключ* разбивается на две части, на первом этапе производятся вычисления для одной части ключа, результаты которых записываются в память, на втором этапе определяется ключ путем последовательного обращения к памяти.

Метод дифференциально-линейный [differential-linear cryptanalysis] — см. *метод разностно-линейный.*

Метод дифференциальный [differential cryptanalysis] — см. *метод разностный.*

Метод искажений дифференциальный [differential fault cryptanalysis] — см. *метод искажений разностный.*

Метод искажений разностный [differential fault cryptanalysis, син. *метод искажений дифференциальный*] — *метод анализа криптографического*, использующий выходную информацию *шифрсистемы* как при нормальном ее функционировании, так и при инвертировании одного или нескольких битов в процессе *шифрования.*

Метод ключей эквивалентных [equivalent keys cryptanalysis] — *метод анализа криптографического*, основанный на возможности объ-

единения *ключей криптосистемы* в классы эквивалентности и опробования только одного ключа из каждого класса.

Метод коллизий [cryptanalysis based on collision search] — *метод анализа криптографического*, основанный на возможности (при определенных условиях) использования *коллизий*.

Метод корреляционный [correlation cryptanalysis] — *метод анализа криптографического*, использующий статистические зависимости между внутренними состояниями *криптосистемы* (как автомата) и значениями входной и выходной последовательностей.

Метод линейный [linear cryptanalysis] — *метод анализа криптографического*, основанный на использовании *приближений аффинных* для некоторых отображений (булевых функций и т. п.), реализуемых в *криптосистеме*. Различают разновидности метода для *шифрсистем поточных* и *шифрсистем блочных*.

Метод на основе парадокса дней рождения [birthday attack] — *метод анализа криптографического*, основанный на использовании *парадокса дней рождения*.

Метод полного (тотального) опробования ключей [exhaustive key search, brute-force attack] — *метод анализа криптографического*, состоящий в переборе всех возможных *ключей криптосистемы* с отбраковкой ложных вариантов по некоторому критерию.

Метод последовательного опробования ключа [sequential key search] — *метод анализа криптографического*, состоящий в последовательном опробовании и отбраковке *ключей криптосистемы* в соответствии с некоторыми упорядочениями на множестве ключей. Как правило, применяются специально подобранные упорядочения *множества ключевого*, например, с учетом вероятностей появления ключей.

Метод протяжки слова вероятного [moving probable word cryptanalysis] — *метод анализа криптографического*, состоящий в последовательном опробовании места в *тексте шифрованном*, соответствующего вероятному фрагменту *текста открытого*. При истинном варианте опробования возможно составление и решение уравнений относительно неизвестного *ключа*.

Метод разностно-линейный [differential-linear cryptanalysis, син. *метод дифференциально-линейный*] — *метод анализа криптографического*, объединяющий *метод разностный* и *метод линейный*.

Метод разностный [differential cryptanalysis, син. *метод дифференциальный*] — *метод анализа криптографического* (в основном применимый к *шифрсистемам блочным*), использующий неравномерность условного распределения разностей между блоками *текста шифрован-*

ного при некоторых значениях разности между блоками *текста открытого*. Имеет ряд модификаций, например, усеченный, метод бумеранга и др.

Метод статистический [statistical cryptanalysis] — *метод анализа криптографического*, основанный на использовании методов математической статистики.

Метод, существенно использующий память [memory using cryptanalysis] — *метод анализа криптографического*, основанный на использовании массива памяти, значительно превосходящего по объему память, необходимую для записи исходной задачи.

Метод частотный [frequency cryptanalysis] — *метод анализа криптографического*, основанный на изучении частотных характеристик *текстов открытого и шифрованного*.

Метрика Хемминга [Hamming metric] — метрика, определенная на множестве векторов одинаковой длины и равная *расстоянию Хемминга* между парами векторов.

Механизм (средство) заполнения трафика [traffic padding] — средство заполнения пауз между передаваемыми сообщениями или их частями для сокрытия передаваемой информации в общем потоке передаваемых данных. Наиболее эффективным способом заполнения трафика является *шифрование* всего трафика, включая заполняющую паузы информацию.

Механизм криптографический [cryptographic mechanism] — термин, принятый в *стандарте ISO 7498.2* для обозначения механизмов безопасности, использующих *алгоритмы криптографические* и *протоколы криптографические*. Устаревший синоним термина *операция криптографическая*, принятого в *стандарте ISO/IEC 15408-99*.

Механизм (средство) разграничения доступа [access control mechanism] — средство реализации *идентификации*, проверки полномочий пользователя и разрешения или отказа в доступе к объекту. Для этого могут использоваться различные средства: списки полномочий, *системы идентификации*, специальные режимы и особенности работы, метки, временные ограничения и выделенные маршруты. Наиболее надежно эти средства реализуются на основе *системы управления ключами*, дающими право доступа к соответствующей информации.

Многочлен периода максимального [maximal period polynomial] — см. *многочлен примитивный*.

Многочлен примитивный [primitive polynomial, син. *многочлен периода максимального*] — неприводимый многочлен степени m над по-

лем $GF(q)$, порядок корней которого в поле разложения $GF(q^m)$ максимален и равен $q^m - 1$.

Многочлен разреженный [sparse polynomial] — многочлен, имеющий мало ненулевых коэффициентов по сравнению со своей степенью. Свойство разреженности многочлена находит применение в некоторых *методах анализа криптографического*.

Множество ключевое (криптосистемы) [key set (of a cryptosystem)] — множество всех возможных значений *ключа криптосистемы*.

Модель текста открытого [plain text model] — математическая модель, описывающая свойства реальных *текстов открытых*, вырабатываемых определенными источниками, либо естественными (осмысленный текст на каком-то языке), либо искусственными (межмашинный обмен, телеметрия и др.). Простейшими м. т. о. являются последовательность независимых испытаний и цепь Маркова. М. т. о. лежат в основе различных подходов к определению *стойкости криптографической*, а также *методов анализа криптографического*.

Модуль управляющий шифрсистемы поточной [stream cipher control module] — часть *шифрсистемы поточной*, генерирующая в зависимости от *ключа криптосистемы последовательность ключевую* (*управляющую*), определяющую в каждом такте выбор отображения для шифрования очередного *блока текста*.

Модуль шифрующий шифрсистемы поточной [stream cipher ciphering module] — часть *шифрсистемы поточной*, реализующая под воздействием *последовательности ключевой* (*управляющей*) *шифрование* очередного *блока текста*.

Монета электронная [e-coin] — название электронных платежных средств, используемых в *системах платежей электронных автономных*. Такая трактовка термина не является общепринятой. Многие авторы называют м. э. любое электронное платежное средство. См. также *деньги электронные*, *деньги цифровые*.

Мультиграмма (m-грамма) [m-tuple] — набор из m знаков алфавита. Обычно рассматривается случай $m \geqslant 2$.

Н

Наблюдатель [observer] — термин, применяемый в *системах платежей электронных* и обозначающий защищенный модуль *бумажника электронного*, которому доверяет банк.

Набор ключей конфиденциальный [validator] — комплект, состоящий из *ключа секретного схемы подписи цифровой*, соответствующего

ключа открытого и его *сертификата ключа*, используемый в *системах платежей электронных автономных* с *бумажниками электронными*. Н. к. к. выдается специальным органом (центром выдачи н. к. к.), создаваемым для этих целей, вслепую так, что впоследствии центр выдачи н. к. к. не сможет идентифицировать клиента, которому был выдан данный н. к. к. Тем самым обеспечивается *неотслеживаемость* клиентов.

Набор тестов статистических [battery of tests] — в *криптографии* — совокупность статистических критериев (тестов), предназначенная для проверки соответствия анализируемой последовательности гипотезе о независимости и равновероятности ее элементов. Каждый тест состоит в вычислении по анализируемой последовательности некоторой статистики, имеющей известное распределение для *последовательности случайной идеальной*, и использовании критерия согласия. Стандартными н. т. с. являются набор тестов Д. Кнута, пакет DIEHARD (Дж. Марсальи), набор тестов NIST (Института стандартов США), пакет TestU01 (Л'Экуйера). В эти наборы входят *тест автокорреляции*, *тест бита следующего*, *тест профиля сложности линейной*, *тест серий*, *тест универсальный Маурера*, *тест частотный* и другие.

Нарушитель [adversary, син. *участник нечестный, нарушитель внутренний*] — *участник протокола*, нарушающий предписанные *протоколом* действия.

Нарушитель активный [active adversary] — *нарушитель*, который недопустимым образом влияет на ход выполнения *протокола криптографического*. Как правило, полный анализ всех результатов однократного выполнения криптографического протокола позволяет обнаружить присутствие н. а.

Нарушитель внешний [outside adversary] — см. *противник*. Рекомендуется использовать термин *противник*.

Нарушитель внутренний [inside adversary] — см. *нарушитель*. Рекомендуется использовать термин *нарушитель*.

Нарушитель пассивный [passive adversary, eavesdropper] — *нарушитель*, который ограничивается сбором и анализом информации о ходе выполнения *протокола криптографического*, но не вмешивается в него. Полный анализ результатов неоднократного выполнения криптографического протокола не позволяет обнаружить присутствие н. п.

Невозможность отказа [non repudiation] — свойство *протокола криптографического*, состоящее в том, что его *участники* (все или некоторые) не могут отказаться от факта совершения определенных действий. Обеспечивается *системой подписи цифровой*.

Нелинейность функции булевой [nonlinearity of Boolean function] — *расстояние от функции булевой до класса функций* аффинных.

Неотслеживаемость [untracebility] — свойство, означающее невозможность получения *противником* и/или *нарушителем* сведений о действиях *участников* (*протокола*). Определяется для *систем криптографических* с большим количеством участников: *систем платежей электронных*, систем доступа к электронным информационным фондам и т. п. Родственные понятия — *анонимность* и *несвязываемость*.

Несвязываемость [unlinkability] — свойство, родственное *неотслеживаемости* и означающее, что *противник* и/или *нарушитель* не только не может установить, кто именно выполнил данное конкретное действие, но даже выяснить, были ли разные действия выполнены одним и тем же *участником*.

О

Обновление ключей [key updating] — способ смены *ключей*, при котором новый ключ генерируется с помощью вычисления значения функции (обычно *функции однонаправленной*) от аргумента, определяемого предыдущим ключом и, возможно, другими данными.

Оператор редуцирования [reduction operator] — отображение r группы подстановок G на множестве X в группу подстановок H на множестве $Y \subset X$, при котором подстановка $r(g)$, $g \in G$, получается путём удаления из цикловой записи подстановки g всех элементов множества $X \backslash Y$.

Операция криптографическая [cryptographic operation] — термин, принятый в *криптографии компьютерной* и введенный в *стандарте ISO/IEC 15408-99* для обозначения *алгоритмов криптографических* и *протоколов криптографических*. Под о. к. понимаются: *зашифрование* и *расшифрование* данных или *ключей*, *алгоритм формирования подписи цифровой*, *алгоритм проверки подписи цифровой*, вычисление *кода аутентичности сообщения*, вычисление значения *хеш-функции*, протокол выработки ключей и др. В более ранних стандартах использовался термин *механизм криптографический*.

Отображение корреляционно-иммунное [correlation immune mapping] — отображение, являющееся *отображением k-корреляционно-иммунным* для некоторого k.

Отображение k-корреляционно-иммунное [k-correlation immune mapping] — отображение $f\colon X^n \to X^m$, для которого при незави-

симых и равномерно распределенных на X значениях $x_1, \ldots, x_n$

$$P\big(f(x_1, \ldots, x_n) = y \mid x_{i_1} = a_{i_1}, \ldots, x_{i_k} = a_{i_k}\big) = P(f(x_1, \ldots, x_n) = y)$$

для любых $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и любых $a_{i_1}, \ldots, a_{i_k} \in X$.

Отображение, не размножающее искажений [mapping free of error propagation] — см. *отображение, не распространяющее искажений.*

Отображение, не распространяющее искажений [mapping free of error propagation, син. *отображение, не размножающее искажений*] — отображение множества всех слов конечных длин в алфавите X в множество всех слов конечных длин в алфавите Y, сохраняющее длины слов, для которого *расстояние Хемминга* между образами любых слов одинаковой длины не превосходит расстояния Хемминга между исходными словами. Вместе с описанными искажениями типа замены букв, иногда рассматривают искажения типа пропуска букв, вставки букв и др. (с соответствующей заменой метрики).

Отображение некоррелированное [uncorrelated mapping] — отображение $f\colon X^n \to X^m$, для которого при случайном равновероятном выборе аргументов $x \in X^n$ совместное распределение j-ой координатной функции отображения $f(x)$ и i-й координаты аргумента x является равномерным на X^2 для всех $i \in \{1, \ldots, n\}$, и всех $j \in \{1, \ldots, m\}$. Это свойство отображения влияет на применимость *методов корреляционных*.

Отображение равновероятное [balanced mapping] — см. *отображение сбалансированное.*

Отображение сбалансированное [balanced mapping, син. *отображение равновероятное*] — отображение $f\colon X^n \to X^m$, для которого при всех $x \in X^m$ мощности полных прообразов $f^{-1}(x)$ одинаковы.

П

Парадокс дней рождения [birthday paradox] — свойство выборки из t независимых случайных знаков n-элементного алфавита, состоящее в том, что вероятность появления в выборке двух одинаковых знаков не меньше $1 - e^{-\alpha}$, если $C_t^2 > \alpha \cdot n > 0$. П. д. р. используется в *криптографии* для оценки различных характеристик *криптосистем*, например, для оценки длины *текста шифрованного*, позволяющего составить уравнения относительно неизвестного *ключа.*

Пароль [password] — последовательность символов, задающая *ключ* или служащая для получения доступа к *средствам криптографическим*, вычислительным средствам и пр. Часто п. обладают лингвистическими особенностями, способствующими их запоминанию.

Перекрытие гаммы [repeated use of a key sequence] — полное или частичное повторное использование *гаммы* (*последовательности управляющей*) при *зашифровании* двух или более различных *текстов открытых*.

Подделка подписи цифровой [forgery] — реализация *атаки* на *систему подписи цифровой*. Состоит в создании *противником* и/или *нарушителем*, не владеющим *ключом секретным*, пары (сообщение, подпись), которая будет принята как корректная *алгоритмом проверки подписи цифровой*. В зависимости от того, для каких сообщений противник и/или нарушитель может подделывать подписи, различают *подделку подписи цифровой универсальную*, *подделку подписи цифровой экзистенциальную* и *подделку подписи цифровой выборочную*.

Подделка подписи цифровой выборочная [selective forgery] — *подделка подписи цифровой*, при которой *противник* и/или *нарушитель*, не владеющий *ключом секретным*, выбирает сообщение (отсюда название *угрозы*), и затем, получив *ключ открытый*, подделывает *подпись цифровую* для этого сообщения.

Подделка подписи цифровой универсальная [universal forgery] — *подделка подписи цифровой*, при которой *противник* и/или *нарушитель*, не владеющий *ключом секретным*, создает алгоритм, функционально эквивалентный *алгоритму генерации подписи цифровой*. Тем самым он может подделывать *подписи цифровые* для любых сообщений.

Подделка подписи цифровой экзистенциальная [existential forgery] — *подделка подписи цифровой*, при которой *противник* и/или *нарушитель*, не владеющий *ключом секретным*, получает *ключ открытый* и создает пару (сообщение, подпись), которая будет принята *алгоритмом проверки подписи цифровой*. При этом противник никак не контролирует выбор того сообщения, для которого в итоге будет подделана подпись. Вероятно, это сообщение будет бессмысленным. *Стойкость криптографическая* против п. п. ц. э. — основная тема теоретических исследований *схем подписи цифровой*.

Подмена [substitution] — *атака на криптосистему*, состоящая в перехвате *противником* и/или *нарушителем* сообщения, и замене его другим сообщением. При этом выбор последнего может зависеть от перехваченного сообщения.

Подпись цифровая (сообщения или документа) [digital signature] — представляет собой строку в некотором алфавите (например, цифровую), зависящую от сообщения или документа и от некоторого *ключа секретного*, известного только подписывающему субъекту. Предполагается, что п. ц. должна быть легко проверяемой без по-

лучения доступа к *ключу секретному*. При возникновении спорной ситуации, связанной с отказом подписывающего от факта п. ц. некоторого сообщения либо с попыткой подделки подписи, третья сторона должна иметь возможность разрешить спор. Реализуется *системой подписи цифровой*. П. ц. позволяет решить следующие три задачи: осуществить *аутентификацию источника данных*, установить *целостность* сообщения или электронного документа, обеспечить *невозможность отказа* от факта подписи конкретного сообщения или документа.

Подпись цифровая групповая [group digital signature] — *подпись цифровая*, сформированная с использованием *схемы подписи цифровой групповой*.

Подпись цифровая многократная [multiple digital signature] — *подпись цифровая*, сформированная с использованием *схемы подписи цифровой*, и не являющаяся *подписью цифровой одноразовой*.

Подпись цифровая одноразовая [one-time digital signature] — *подпись цифровая*, сформированная с использованием *схемы подписи цифровой*, в которой после проведения процедуры проверки правильности подписи цифровой необходимо осуществить смену *ключей*.

Подпись цифровая с восстановлением сообщения [digital signature with message recovery] — *подпись цифровая*, сформированная с использованием разновидности *схемы подписи цифровой*, в которой получателю передается только подпись цифровая, а сообщение извлекается из нее *алгоритмом проверки подписи цифровой*.

Подпись цифровая слепая [blind digital signature] — *подпись цифровая*, сформированная с использованием *схемы подписи цифровой вслепую*.

Подпись цифровая, не допускающая отказа [undeniable digital signature] — *подпись цифровая*, сформированная с использованием *схемы подписи цифровой конфиденциальной*.

Подпись электронная [electronic signature] — термин, применяемый в международных правовых актах для электронной идентификационной информации, добавляемой в качестве атрибута к электронному документу. Позволяет идентифицировать физических лиц путем сличения их подписей. Охватывает различные технологии, в том числе использующие биометрические характеристики, временные и физические характеристики процесса собственноручной подписи, *подписи цифровые*, ключи электронные, пластиковые карты и др. Основное назначение: *идентификация пользователя* (*в системе информационной*), подтверждение *целостности* подписываемого документа, а также обеспечение *невозможности отказа* от факта подписи. В настоящее вре-

мя всем трем целям удовлетворяет только технология *подписи цифровой*.

Подпись электронная цифровая (ЭЦП) [electronic digital signature] — юридический термин, относящийся к технологии *подписи цифровой* применительно к электронным документам. Является частным случаем *подписи электронной*. Основной проблемой является определение условий, при которых п. э. ц. в электронном документе юридически равнозначна собственноручной подписи в документе на бумажном носителе. Например, в соответствии с Федеральным законом Российской Федерации от 10 января 2002 года №1-ФЗ «Об электронной цифровой подписи» «электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий: *сертификат ключа* подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания; подтверждена подлинность электронной цифровой подписи в электронном документе; электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи».

Подстановка односторонняя [one-way permutation] — взаимно однозначная *функция односторонняя*.

Полнота (протокола) [completeness property] — свойство *протокола криптографического*, означающее, что при выполнении *участниками честными* протокол решает ту задачу, для которой он создан.

Пользователь законный [legal user] — официально зарегистрированный в системе пользователь.

Помехоустойчивость шифра [noise stability of a cipher] — способность *шифра* противостоять действию случайных помех (в отличие от целенаправленных действий *противника*), возникающих при передаче *сообщения шифрованного* по *каналу связи*.

Последовательность истинно случайная [true random sequence] — последовательность, порожденная недетерминированным физическим устройством или процессом. Такая последовательность (в отличие от *последовательности псевдослучайной*) непредсказуема и невоспроизводима. Статистические свойства п. и. с. могут отличаться от статистических свойств *последовательности случайной идеальной*.

Последовательность ключевая [key stream] — в *шифрсистемах поточных — последовательность управляющая*, однозначно определяющая в каждом такте выбор *функции зашифрования* для *зашифрования*

очередного знака *текста открытого*. Иногда термин п. к. используется в качестве синонима *гаммы* в *шифре гаммирования*.

Последовательность линейная конгруэнтная [linear congruent sequence] — *последовательность рекуррентная* $v(1)$, $v(2)$, ... над кольцом вычетов Z_N с законом рекурсии $v(i+1) \equiv a \cdot v(i) + b \pmod{N}$, $i = 1, 2, \ldots$

Последовательность линейная рекуррентная [linear recurrent sequence] — *последовательность рекуррентная* $u(1)$, $u(2)$, ... над кольцом R с линейным законом рекурсии

$$u(i+m) = \sum_{k=0}^{m-1} f_k \cdot u(i+k)$$

$f_0, \ldots, f_{m-1} \in R$. Многочлен $f(x) = x^m - \sum_{k=0}^{m-1} f_k \cdot x^k$ называют характеристическим многочленом п. л. р., а целое число $m > 0$ — ее порядком.

Последовательность линейная рекуррентная периода максимального [maximal period linear recurrent sequence] — ненулевая *последовательность линейная рекуррентная* порядка m над полем $GF(q)$, у которой период максимально возможный и равен $q^m - 1$.

Последовательность псевдослучайная [pseudo-random sequence] — последовательность, порожденная детерминированным устройством или программой. Важной задачей *криптографии* является построение п. п., обладающих свойствами, близкими к свойствам типичных реализаций *последовательности случайной идеальной*. См. также *генератор последовательностей псевдослучайных криптографически сильный*.

Последовательность псевдослучайная криптографически сильная [cryptographically strong pseudorandom sequence] — *последовательность псевдослучайная* вырабатываемая *генератором последовательностей псевдослучайных криптографически сильным*.

Последовательность рекуррентная [recurrent sequence] — последовательность, в которой каждый элемент однозначно определяется некоторым фиксированным числом ее предыдущих элементов с помощью функции, именуемой законом рекурсии.

Последовательность сбалансированная [balanced sequence] — последовательность знаков конечного алфавита X, в которой все элементы из X встречаются одинаковое число раз.

Последовательность случайная идеальная [ideal random sequence] — последовательность, являющаяся реализацией последователь-

ности независимых случайных величин, имеющих равномерное распределение на заданном конечном алфавите.

Последовательность управляющая [control sequence] — *последовательность псевдослучайная* или *последовательность истинно случайная*, используемая при реализации *алгоритма криптографического*. Частными случаями являются *гамма шифра* и *последовательность ключевая*.

Постулаты Голомба [Golomb postulates] — сформулированные С. Голомбом постулаты для *последовательностей псевдослучайных* двоичных, используемых в криптографических приложениях. Согласно им последовательность должна удовлетворять определенным ограничениям на встречаемость знаков, *мультиграмм* и *функцию автокорреляционную последовательности*. Последовательности, удовлетворяющие п. Г., иногда называют псевдошумовыми.

Правило Керкгоффса [Kerckhoffs assumption] — общепринятое в *криптографии* предположение проведения *криптоанализа*, впервые сформулированное голландским криптографом Н. Керкгоффсом («компрометация системы не должна причинять неудобств корреспондентам»). В современном понимании это правило означает, что описание *криптосистемы* (*криптопротокола*) может быть полностью известно *противнику* и/или *нарушителю*, а *стойкость криптографическая* основана только на том, что не известен *ключ* (*секретный*).

Предположение криптографическое (криптологическое) [cryptographic assumption] — предположение о вычислительной сложности какой-либо математической задачи, на основе которого доказывается *стойкость теоретико-сложностная криптосистем* и *протоколов криптографических*. Примерами п. к. являются предположения о существовании *функций односторонних*, *функций с секретом*, о вычислительной сложности *задачи логарифмирования дискретного*, *задачи факторизации чисел целых*.

Предположение о ящике черном [black box assumption] — *предположение криптоанализа*, означающее, что *алгоритм шифрования* неизвестен, и возможно лишь наблюдение выхода алгоритма при любом заданном входе. См. также *ящик черный*.

Предположения криптоанализа [cryptanalytic assumptions] — совокупность условий и допущений, при которых проводится анализ *системы криптографической*. Фактически предположения разработчика и *пользователя законного* описывают модель *противника* и/или *нарушителя*, т. е. его цели, возможности и имеющиеся исходные данные. Предположения *противника* и/или *нарушителя* обычно описы-

вают свойства криптосистемы и особенности ее реализации и применения.

Преобразование, не распространяющее искажений [transform free of error propagation] — *отображение, не распространяющее искажений*, множества слов из некоторого алфавита в себя. Все обратимые отображения такого типа описаны А. А. Марковым.

Преобразование перемешивания [mixing transform] — преобразование, с помощью которого разработчики *криптосистем* стремятся обеспечить *свойство перемешивания*.

Преобразование рассеивания [diffusion transform] — преобразование, с помощью которого разработчики *криптосистем* стремятся обеспечить *свойство рассеивания*.

Преобразование Уолша [Walsh transform] — см. *преобразование Уолша—Адамара*.

Преобразование Уолша—Адамара [Walsh—Hadamard transform, син. *преобразование Уолша*] — преобразование вектора значений булевой функции $(f(x) \mid x \in \{0, 1\}^n)$ в целочисленный вектор $(\tilde{f}(x) \mid x \in \{0, 1\}^n)$, где $\tilde{f}(x) = \sum\limits_{u \in \{0,1\}^n} (-1)^{f(u)+(x,u)}$. Числа $\tilde{f}(x)$ называются коэффициентами Уолша—Адамара.

Преобразование усложнения [confusion transform] — преобразование, с помощью которого разработчики *криптосистем* стремятся обеспечить *свойство усложнения*.

Преобразование Фейстеля (Файштеля) [Feistel transform] — см. *схема Фейстеля (Файштеля)*.

Приближение аффинное [affine approximation, син. *аппроксимация аффинная*] — функция $g(x_1, \ldots, x_n) = \sum\limits_{i=1}^{n} u_i \cdot x_i + b$ от n переменных является приближением аффинным для булевой функции $f(x_1, \ldots, x_n)$, если их значения совпадают более, чем на 2^{n-1} значениях $(x_1, \ldots, x_n)$. Число таких $(x_1, \ldots, x_n) \in \{0; 1\}^n$, что $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ равно $2^{n-1} + \frac{(-1)^b}{2} \cdot \tilde{f}(u)$, где $u = (u_1, \ldots, u_n)$, а $\tilde{f}(u)$ — коэффициент Уолша—Адамара. См. также *преобразование Уолша—Адамара*.

Приближение аффинное наилучшее [best affine approximation, син. *аппроксимация аффинная наилучшая*] — *приближение аффинное* $g(x_1, \ldots, x_n) = \sum\limits_{i=1}^{n} u_i \cdot x_i + b$ для булевой функции $f(x_1, \ldots, x_n)$, для которого $(-1)^b \cdot \tilde{f}(u) = \max\limits_{v \in \{0,1\}^n \setminus \{\bar{0}\}} |\tilde{f}(v)|$. Здесь $\tilde{f}(v)$ — коэффициенты

Уолша–Адамара функции f. См. также *преобразование Уолша–Адамара*.

Примитив криптографический [cryptographic primitive] — функция (семейство функций), которая используется как составной элемент при построении *криптосистем* (*протоколов криптографических*) и обладает определенным криптографическим свойством. Примеры п. к.: *функция односторонняя*, *хеш-функция*, *генератор последовательностей псевдослучайных*, *семейство функций псевдослучайных*. Иногда п. к. называют такие объекты, как *подпись цифровая*, *деньги электронные*, *сертификат ключа* и т. п., если они используются при построении протокола криптографического.

Проблема повторной траты денег электронных [e-money double spending problem] — возможность неоднократного использования одних и тех же *денег электронных* нечестным покупателем. Возникает в *системах платежей электронных автономных*, так как в них *транзакция платежа* выполняется без участия банка. Для решения п. п. т. д. э. известны два способа. Первый — идентификация *нарушителя* post factum. Он основывается на специальной конструкции электронных денег, позволяющей банку при выполнении *транзакции депозита* обнаружить повторную трату и идентифицировать нарушителя. При этом честным клиентам банка гарантируется безусловная *неотслеживаемость* платежей. Второй способ предотвращает повторную трату электронных денег посредством *бумажников электронных*.

Проверка подписи [signature verification] — см. *алгоритм проверки подписи цифровой*.

Пространство подписей [signature space] — множество всех значений *подписи цифровой*, которые могут быть сгенерированы данной *схемой подписи цифровой*.

Противник [adversary, син. *нарушитель внешний*] — внешний по отношению к *участникам криптопротокола* (*системы криптографической*) субъект (или коалиция субъектов), наблюдающий за передаваемыми сообщениями, и, возможно, вмешивающийся в работу участников, путем перехвата, искажения (модификации), вставки (создания новых), повтора и перенаправления сообщений, блокирования передачи и т. п. с целью нарушения одной или нескольких *функций-сервисов безопасности*. Может образовывать коалицию с *нарушителем*.

Противник активный [active adversary] — *противник*, который вмешивается в ход выполнения *протокола криптографического* или работу *системы криптографической*. Как правило, полный анализ всех

результатов однократного выполнения криптографического протокола позволяет обнаружить присутствие п. а.

Противник пассивный [passive adversary, eavesdropper] — *противник*, который может получать некоторую информацию о выполнении *протокола криптографического* или работы *системы криптографической*, но не вмешивается в их работу. В случае протоколов полный анализ результатов неоднократного их выполнения не позволяет обнаружить присутствие п. п.

Протокол [protocol] — описание распределенного алгоритма, в процессе выполнения которого два *участника* (или более) последовательно выполняют определенные действия и обмениваются сообщениями. Последовательность *шагов протокола* группируется в *циклы* (*раунды*).

Протокол аутентификации абонентов [user authentication protocol] — см. *аутентификация абонента* (*пользователя*), *протокол идентификации*.

Протокол аутентификации сообщений [message authentication protocol] — *протокол криптографический*, предназначенный для обеспечения *целостности* сообщений, под которой понимается гарантируемая получателю возможность удостовериться, что сообщение поступило от заявленного отправителя и в неискаженном виде. В случае, когда *участники протокола* доверяют друг другу и защищаются от *противника*, п. а. с. строятся на основе *кодов аутентичности сообщений*. Если же участники друг другу не доверяют, то для аутентификации сообщений используется *схема подписи цифровой*.

Протокол голосования [election scheme, voting scheme, voting protocol] — *протокол криптографический прикладной*, позволяющий проводить процедуру голосования, в которой избирательные бюллетени существуют только в электронной форме. Является *протоколом криптографическим*, т. к. обеспечивает тайный характер голосования. Основное свойство п. г. — универсальная проверяемость, т. е. предоставление возможности всякому желающему, включая сторонних наблюдателей, в любой момент времени проверить правильность подсчета голосов.

Протокол групповой [group-oriented protocol] — *протокол криптографический*, в котором какой-либо алгоритм, требующий знания *ключа секретного*, является распределенным. Например, в *протоколе подписи групповой* подписывающий заменяется группой *участников* таким образом, что корректная подпись может быть сформирована только при участии всех членов группы.

Протокол двусторонний [two-party protocol] — *протокол* с двумя *участниками*.

Протокол доказательства знания [proof of knowledge protocol] — см. *доказательство знания*.

Протокол идентификации [identification protocol, син. *схема идентификации*] — протокол *аутентификации сторон*, участвующих во взаимодействии и не доверяющих друг другу. Различают п. и. с *аутентификацией односторонней* или *аутентификацией взаимной*. П. и., как правило, основаны на известной обеим сторонам информации (*пароли*, личные идентификационные номера, *ключи секретные* или *ключи открытые*) и реализуются с использованием техники «запрос-ответ» или *доказательства знания*. В дополнение к п. и. могут использоваться некоторые физические приборы, с помощью которых проводится идентификация (магнитная или интеллектуальная пластиковая карта, прибор, генерирующий меняющиеся со временем пароли), а также биометрические параметры.

Протокол идентификации взаимной [mutual identification protocol] — см. *аутентификация взаимная*, *протокол идентификации*.

Протокол идентификации односторонней [one-way authentication protocol] — см. *аутентификация односторонняя*, *протокол идентификации*.

Протокол интерактивный [interactive protocol] — *протокол*, выполняемый за два *цикла* (*раунда*) или более.

Протокол криптографический [cryptographic protocol, син. *криптопротокол*] — *протокол*, предназначенный для выполнения функций *системы криптографической*, в процессе выполнения которого *участники* используют *алгоритмы криптографические*.

Протокол криптографический квантовый [quantum cryptographic protocol] — *протокол криптографический*, использующий *канал связи квантовый*.

Протокол криптографический прикладной [application cryptographic protocol] — *протокол криптографический*, предназначенный для решения практических задач обеспечения *функций-сервисов безопасности* с помощью *систем криптографических*. Примеры: протокол конфиденциальной передачи сообщений, *схема подписи цифровой*, *система платежей электронных*, *протокол голосования*, *протокол подписания контракта* и др.

Протокол криптографический примитивный [primitive cryptographic protocol] — *протокол криптографический*, который не имеет самостоятельного прикладного значения, но используется как базовый

компонент при построении *протоколов криптографических прикладных*. Как правило, п. к. п. решает какую-либо одну абстрактную задачу. Примеры: *протокол обмена секретами*, *протокол привязки к биту*, *протокол подбрасывания монеты (по телефону)*.

Протокол (алгоритм) обмена ключами Диффи—Хеллмана [Diffie—Hellman algorithm] — один из первых протоколов *распределения ключей открытого*. Предназначен для формирования «общего секрета» (*ключа*, идентификационного номера и др.) сторонами, обменивающимися данными по открытому каналу с использованием *ключей открытых* (общедоступных) и *ключей секретных* (индивидуальных). Вместе с *алгоритмом шифрования RSA* положил начало развитию *шифрсистем асимметричных*.

Протокол обмена секретами [secret exchange protocol] — *протокол криптографический примитивный* с двумя *участниками*. Входные слова участников называются секретами. В протоколе обмен секретами организован таким образом, чтобы в случае его прерывания (по любой причине) знания участников о секретах друг друга были приблизительно одинаковыми.

Протокол подбрасывания монеты (по телефону) [coin flipping (by telephone) protocol] — *протокол криптографический примитивный*, позволяющий двум не доверяющим друг другу *участникам* сгенерировать общий случайный равновероятный бит. Главное свойство таких протоколов состоит в том, что если хотя бы один из участников является *участником честным*, то сгенерированный бит будет случайным, независимо от действий другого участника. Имеются обобщения на случай конечных битовых строк, а также на случай произвольного количества участников.

Протокол подписания контракта [contract signing protocol] — *протокол криптографический прикладной*, как правило, с двумя *участниками*, которые, обмениваясь сообщениями по *каналам связи*, должны подписать контракт, существующий только в электронной форме. Основное требование к *стойкости криптографической* п. п. к. таково: при любом прерывании выполнения протокола шансы каждого из участников получить контракт, подписанный другим, и при этом не подписаться самому, ничтожно малы. Поэтому п. п. к. должен включать в себя *протокол обмена секретами*. Имеются и другие требования к стойкости протокола, в частности, так называемая защита от злоупотреблений (abuse). Последняя означает, что если выполнение протокола было прервано и контракт остался неподписанным, то ни один из участников не сможет доказать третьим лицам (*арбитрам*), что другой участвовал

в выполнении протокола (а, следовательно, имел намерение подписать данный контракт).

Протокол подписи групповой [group signature protocol] — описание *алгоритма формирования подписи цифровой*, предполагающего одновременное участие заранее определенной группы *участников*. В случае отсутствия хотя бы одного *участника* из группы формирование подписи невозможно.

Протокол (схема) привязки к биту [bit commitment protocol (scheme)] — *протокол криптографический примитивный* с двумя *участниками* (отправителем и получателем), посредством которого отправитель передает получателю бит информации (битовое обязательство) таким образом, что выполняются следующие два условия: 1) после передачи бита получателю (так называемого этапа привязки) отправитель уже не может изменить его значение; 2) получатель не может самостоятельно определить значение бита и узнает его только после выполнения отправителем так называемого этапа раскрытия.

Протокол разделения секрета [secret sharing protocol] — *протокол криптографический*, реализующий *схему разделения секрета* в модели, где *участники* являются абонентами сети связи. В этой модели имеется дополнительный участник (дилер), которому известно значение секрета. Дилер генерирует *доли секрета* и рассылает их остальным участникам. Всякая правомочная коалиция участников может восстановить секрет, выполнив протокол восстановления секрета. П. р. с. могут найти применение в организации хранения конфиденциальной информации, например, *ключей криптосистемы*, а также как *протоколы криптографические примитивные*. См. также *структура доступа*.

Протокол разделения секрета проверяемого [verifiable secret sharing protocol] — *протокол разделения секрета* предназначенный для случая, когда *участники* не доверяют друг другу, в том числе и дилеру. Для защиты от нечестного дилера п. р. с. п. предоставляет каждому из остальных участников возможность проверить, что от дилера получена корректная *доля секрета*.

Протокол распределения ключей [key distribution protocol] — *протокол* получения пользователями *ключей*, необходимых для функционирования *системы криптографической*. Различают следующие типы п. р. к.: протоколы передачи (уже сгенерированных) ключей; протоколы совместной выработки общего ключа (*распределение ключей открытое*); *схемы распределения ключей предварительного*.

Протокол с арбитром [arbitrated protocol, син. *протокол с посредником*] — *протокол криптографический*, в котором для разрешения спо-

ров между *участниками* требуется *арбитраж*. П. с а. делятся на два класса. В пессимистических протоколах *арбитр* должен участвовать в каждом сеансе выполнения *протокола*. В оптимистических протоколах участие арбитра требуется только в случае возникновения конфликтов между участниками.

Протокол с посредником [arbitrated protocol] — см. *протокол с арбитром*.

Протокол с разглашением нулевым [zero-knowledge protocol] — см. *доказательство с разглашением нулевым*.

Профиль сложности линейной [linear complexity profile] — для последовательности $v_1, \ldots, v_n$ профиль сложности линейной — это последовательность $L_1, L_2, \ldots, L_n$, где L_i — *сложность линейная последовательности* $v_1, \ldots, v_i$.

Псевдоколлизия [pseudocollision] — для *хеш-функции* $h(k, x) = h_k(x)$, зависящей от *ключа* k, псевдоколлизией называют такую пару $(k_1, x_1), (k_2, x_2), (k_1, x_1) \neq (k_2, x_2)$, что $h(k_1, x_1) = h(k_2, x_2)$.

P

Радиус спектральный [spectral radius] — максимальный по множеству ненулевых значений аргумента модуль коэффициента Уолша—Адамара булевой функции. Через р. с. выражается *нелинейность функции булевой*. См. также *преобразование Уолша—Адамара*.

Развертывание ключа [key scheduling] — в *шифрсистемах поточных* — выработка *последовательности ключевой* по короткому *ключу*. В *шифрсистемах блочных* — алгоритм вычисления *ключей цикловых* (*раундовых*) по *ключу разовому*.

Разглашение нулевое [zero-knowledge property] — свойство *протокола доказательства знания*, обеспечивающее такое его выполнение, что никакая информация о доказываемом утверждении, кроме факта его истинности, не может быть получена нечестным проверяющим из переданных сообщений за время полиномиально зависящее от суммарной длины этих сообщений.

Разглашение нулевое относительно проверяющего честного [honest-verifier zero-knowledge] — ослабленный вариант *разглашения нулевого*, при котором требуется, чтобы протокол *доказательства интерактивного* не давал никакой дополнительной информации о доказываемом утверждении лишь честному проверяющему, т. е. выполняющему действия, предписанные *протоколом*. С криптографической точки зрения данное свойство защищает доказывающего не от нечестного прове-

ряющего, а от *противника*, который подслушивает сеанс выполнения протокола.

Разграничение доступа [access control] — см. *функция-сервис разграничения доступа, система разграничения доступа.*

Разделение секрета [secret sharing] — см. *схема разделения секрета, протокол разделения секрета.*

Разделение секрета проверяемое [verifiable secret sharing] — см. *протокол разделения секрета проверяемого.*

Распределение ключей квантовое [quantum key distribution] — процедура распределения *ключей секретных*, реализуемая с помощью *протоколов криптографических квантовых* и *каналов связи квантовых*.

Распределение ключей открытое [public key distribution] — *протокол* совместной выработки пользователями (общего) *ключа секретного* путем обмена сообщениями по открытому *каналу связи*. Протокол должен исключать возможность получения информации о ключе посторонними, а также любым *участником* до завершения им действий, предусмотренных протоколом.

Расстояние единственности [unicity distance] — в задаче нахождения неизвестного параметра *системы криптографической* (например, *ключа секретного*) по выходным данным *криптосистемы* (например, по начальному отрезку *текста шифрованного*) — минимальное количество выходных данных, с заданной вероятностью достаточное для однозначного определения искомого параметра.

Расстояние между функциями булевыми [function-to-function distance] — расстоянием между булевыми функциями от одинакового количества переменных называется величина равная *расстоянию Хемминга* между векторами значений этих функций.

Расстояние от функции булевой до класса функций [function-to-class distance] — расстояние от булевой функции f до класса функций K — это величина равная

$$\Delta(f;\, K) = \min_{g \in K} \Delta(f;\, g),$$

где $\Delta(f;\, g)$ — *расстояние между функциями булевыми* f, g.

Расстояние Хемминга [Hamming distance] — расстояние Хемминга между векторами $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n)$ есть количество номеров координат i, для которых $x_i \neq y_i$.

Расшифрование [decryption, deciphering] — процесс обратный к *зашифрованию*, реализуемый при известном значении *ключа*. См. *алгоритм расшифрования.*

Регистр сдвига [shift register] — регистром сдвига длины n над множеством X с функцией обратной связи f называют конечный автономный автомат с множеством состояний X^n. Находясь в состоянии $(x_1, \ldots, x_n)$, р. с. вырабатывает выходной символ x_1 и переходит в состояние $(x_2, \ldots, x_n, f(x_1, \ldots, x_n))$. Рассматриваются различные обобщения понятия р. с.: неавтономный, обобщенный, р. с. с иными функциями выхода и др. Р. с. как техническое устройство используется при реализации различных компонентов *систем криптографических*, например, *генераторов фильтрующих*, *генераторов комбинирующих*.

Регистр сдвига линейный [linear feedback shift register (LFSR)] — *регистр сдвига* длины n над кольцом R, у которого функция обратной связи $f(x_1, \ldots, x_n)$ линейна над R.

Регистр сдвига нелинейный [nonlinear feedback shift register] — *регистр сдвига* длины n над кольцом R, у которого функция обратной связи $f(x_1, \ldots, x_n)$ не линейна над R.

Режим выработки имитовставки [message authentication code mode] — см. *режим выработки кода аутентичности сообщения*.

Режим выработки кода аутентичности сообщения [message authentication code mode, син. *режим выработки имитовставки*] — *режим шифрования*, применяемый для выработки *кода аутентичности сообщения*.

Режим шифрования [encryption mode] — способ получения *алгоритма зашифрования*, исходя из *алгоритма зашифрования блочного базового*. Основными р. ш. являются: простая замена или электронная кодовая книга (ECB), сцепление блоков шифртекста (CBC), обратная связь по шифртексту (CFB), обратная связь по выходу (OFB). Выбор р. ш. имеет целью обеспечение определенных свойств *алгоритма шифрования* (ограничение распространения искажений, простота синхронизации и др.).

C

Свойство перемешивания [mixing property] — строго не формализуемое свойство *функции зашифрования*, выражающееся, в современном понимании, в существенном усложнении взаимосвязи статистических и аналитических характеристик элементов *текст шифрованного* по сравнению с подобными взаимосвязями элементов *текста открытого*. Термин «перемешивание» перенесен в *криптографию* К. Шенноном из теории вероятностей.

Свойство рассеивания [diffusion property] — строго не формализуемое свойство *функции зашифрования*, состоящее в том, что каждый знак *текста открытого* влияет на большое число знаков *текста шифрованного*. Термин введён К. Шенноном.

Свойство усложнения [confusion property] — строго не формализуемое свойство *функции зашифрования*, означающее сложную зависимость между *ключом* и *текстом шифрованным*. Термин введён К. Шенноном.

Семейство подстановок псевдослучайных [pseudorandom permutation family] — *семейство функций псевдослучайных*, в котором каждая функция является подстановкой.

Семейство подстановок с секретом [trapdoor permutation family] — семейство *функций с секретом*, в котором каждая функция является подстановкой.

Семейство функций псевдослучайных [pseudorandom function family] — семейство функций, обладающее следующим свойством. Функция, выбранная случайно равновероятно из семейства, алгоритмически неотличима от случайной функции. При этом каждая из функций, и выбранная из с. ф. п., и случайная функция, рассматривается как *ящик черный*, т. е. алгоритм может только получать значения функции на выбираемых им значениях аргумента.

Сертификат ключа [key certificate] — структура данных заранее определенного формата, включающая *ключ открытый*, идентификационную информацию владельца *ключа*, а также другую служебную информацию (время действия и предназначение ключа, тип используемых *алгоритмов криптографических*, и др.), заверенная *подписью цифровой* уполномоченного лица доверенного *центра сертификации* (*центра удостоверяющего*).

Синтез криптографический [cryptosynthesis, син. *криптосинтез*] — условно выделяемая часть *криптографии* (*криптологии*), связанная с разработкой *систем криптографических* (*протоколов криптографических*).

Синхропосылка [synchrosignal] — комбинация знаков, передаваемая по *каналу связи* и предназначенная для вхождения в связь аппаратуры шифрования или для синхронизации аппаратуры. См. также *вектор инициализации*.

Система идентификации [identification system] — *система криптографическая*, выполняющая *аутентификацию сторон* в процессе информационного взаимодействия. Математическая модель с. и. включает *протокол идентификации* и *систему ключевую*.

Система имитозащиты [integrity system] — *система криптографическая*, выполняющая *аутентификацию сообщений* и предназначенная для защиты от несанкционированного изменения информации или навязывания ложной информации. В частности, с. и. обеспечивает *целостность* информации. Математическая модель с. и. включает *алгоритм кодирования имитозащищающего* (это может быть *алгоритм шифрования*, *код аутентификации*, либо др. преобразование) и алгоритм принятия решения об истинности полученной информации, а также *систему ключевую*.

Система ключевая [key system] — состоит из *множества ключевого* (*криптосистемы*) и двух подсистем: *системы установки ключей* и *системы управления ключами*.

Система ключевая шифрсистемы асимметричной [key system of a public key cryptosystem] — *система ключевая*, основанная на использовании каждым *участником* пары, состоящей из *ключа открытого* и *ключа секретного*. Такие системы облегчают реализацию многих ключевых протоколов по сравнению с *шифрсистемами симметричными*. Вместе с тем, для обеспечения взаимного доверия между пользователями требуется дополнительная система, называемая *инфраструктурой ключей открытых*.

Система ключевая шифрсистемы симметричной [key system of a secret key cryptosystem] — *система ключевая*, основанная на использовании только *ключей секретных*, что исключает необходимость механизмов доверия, свойственных *шифрсистемам асимметричным*, но вместе с тем, затрудняет реализацию ряда протоколов *цикла жизненного ключей* (например, распределения ключей).

Система криптографическая [cryptographic system (cryptosystem), син. *криптосистема*] — система обеспечения безопасности информации криптографическими методами в части *конфиденциальности*, *целостности*, *аутентификации*, *невозможности отказа* и *неотслеживаемости*. В качестве подсистем может включать *системы шифрования*, *системы идентификации*, *системы имитозащиты*, *системы подписи цифровой* и др., а также *систему ключевую*, обеспечивающую работу остальных систем. В основе выбора и построения с. к. лежит условие обеспечения *стойкости криптографической*.

Система криптографическая квантовая [quantum cryptographic system] — *система криптографическая*, использующая *каналы связи квантовые*.

Система криптографическая пороговая [threshold cryptographic scheme] — *система криптографическая*, в которой *ключ сек-*

ретный распределен между n *участниками* так, что для функционирования системы необходима и достаточна совместная работа любых t участников, где $t < n$ — заданное число.

Система обмена данными электронная [electronic data interchange (EDI)] — автоматизированная технология осуществления сбора, классификации, хранения, поиска, обработки и передачи информации, основанная на едином представлении и структурировании данных. В настоящее время интегрируется с технологиями автоматизации делопроизводства и документооборота. Для защиты с. о. д. э. применяются *системы криптографические*, обеспечивающие *конфиденциальность*, *целостность*, *аутентификацию* и *невозможность отказа*.

Система перевода средств денежных электронная [electronic funds transfer (EFT)] — система автоматизации перевода финансовых средств с использованием *системы обмена данными электронной*. Собирает данные транзакций, сортирует и группирует их в соответствии с банком назначения и передает в общем формате в систему, занимающуюся проведением финансовых расчетов.

Система (протокол) платежей электронных [electronic cash system, e-cash system] — система осуществления транзакций и взаиморасчетов между сторонами в электронной (безбумажной) форме. Различают: *системы перевода средств денежных электронные* с использованием *систем обмена данными электронных* (межбанковские переводы), и системы, в которых используются дематериализованные денежные аналоги. Последние различаются по степени дематериализации: *деньги электронные*, *деньги виртуальные* и *деньги цифровые*. С. п. э. состоит из набора *протоколов*, из которых основными являются протоколы, реализующие *транзакцию снятия со счета*, *транзакцию платежа* и *транзакцию депозита*. Если для выполнения транзакции платежа необходимо участие банка-эмитента, осуществляющего выдачу в обращение дематериализованных денег, то с. п. э. называется *системой платежей электронных централизованной*, в противном случае — *системой платежей электронных автономной*.

Система платежей электронных автономная [off-line e-cash system] — *система платежей электронных*, в которой *транзакцию платежа* выполняют покупатель и продавец, без участия банка-эмитента. В такой системе требуется дополнительная *транзакция депозита*, с помощью которой продавец может положить полученные *деньги электронные* на свой счет в банке.

Система платежей электронных централизованная [on-line e-cash system] — *система платежей электронных*, в которой *тран-*

закция платежа выполняется с участием банка-эмитента *денег электронных*.

Система подписи цифровой [digital signature cryptosystem] — *система криптографическая*, выполняющая *аутентификацию источника данных* или *аутентификацию сообщения*. Предназначена для защиты от отказа субъектов от некоторых из ранее совершенных ими действий. Например, отправитель может отказаться от факта передачи сообщения, утверждая, что его создал сам получатель, а получатель может модифицировать, подменить или создать новое сообщение, а затем утверждать, что оно получено от отправителя. Математическая модель с. п. ц. включает *схему подписи цифровой* и *систему ключевую*, в качестве которой обычно выступает *инфраструктура ключей открытых*. Для разрешения споров необходима процедура *арбитража*, с помощью которой третья сторона — *арбитр* — разрешает споры о подлинности *подписи цифровой*.

Система разграничения доступа [access control mechanism] — оборудование или программное обеспечение, процедуры автоматизированной системы, процедуры администратора и их различные комбинации, которые обнаруживают, предотвращают несанкционированный доступ и разрешают законный доступ в автоматизированных системах.

Система управления ключами [key management system] — подсистема *системы ключевой*, определяющая порядок регистрации ключей, их использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых *ключей*. Целью управления ключами является нейтрализация таких *угроз*, как компрометация и несанкционированное использование ключей, например, использование ключа, срок действия которого истек.

Система уравнений с правыми частями искаженными [system of equations with perturbed right-hand side] — система уравнений, получающаяся из совместной системы уравнений при случайном искажении правых частей уравнений. Такие системы возникают, например, в *криптоанализе* при сочетании реальных данных с упрощенными моделями порождающих их устройств.

Система уравнений случайных [random system of equations] — система уравнений, которая кроме неизвестных содержит случайные величины или функции.

Система установки ключей [key establishment system] — подсистема *системы ключевой*, определяющая алгоритмы и процедуры генерации, распределения, передачи и проверки *ключей*.

Система шифрования [cryptosystem, cipher, син. *шифрсистема*] — *система криптографическая*, предназначенная для защиты информации от лиц, не имеющих права доступа к ней. Защита обеспечивается путем *зашифрования* информации. Математическая модель с. ш. включает способ кодирования исходной и выходной информации, *шифр* и *систему ключевую*. Основными требованиями, определяющими качество с. ш., являются: *стойкость криптографическая*, *имитостойкость*, *помехоустойчивость шифра* и др.

Скремблер [scrambler] — устройство, осуществляющее преобразование сигнала путём изменений соотношений между временем, амплитудой и частотой, не выходящих за пределы используемого диапазона.

Сложность алгоритма временна́я [time complexity] — функция, выражающая зависимость числа элементарных операций, производимых при работе алгоритма, от длины записи исходных данных. Обычно рассматривается с. а. в. в худшем случае, то есть максимальное значение сложности временной по всем исходным данным одинаковой длины. Рассматривается также с. а. в. в среднем, то есть среднее значение сложности временно́й при случайном выборе исходных данных одинаковой длины.

Сложность алгоритма емкостна́я [space complexity] — функция, выражающая зависимость числа ячеек памяти, используемых в работе алгоритма, от длины записи исходных данных. Обычно рассматривается с. а. е. в худшем случае, то есть максимальное значение емкостной сложности по всем исходным данным одинаковой длины. Рассматривается также с. а. е. в среднем, то есть среднее значение сложности емкостной при случайном выборе исходных данных одинаковой длины.

Сложность квадратичная последовательности [linear complexity] — для последовательности над кольцом R — наименьшая длина *регистра сдвига* над R с функцией обратной связи второй степени, порождающего эту последовательность.

Сложность (протокола) коммуникационная [communication complexity] — функция, выражающая зависимость максимального количества битов информации, пересылаемых в процессе выполнения распределенного алгоритма от длины записи исходных данных. С. к. — показатель эффективности реализации *протоколов криптографических*.

Сложность Лемпела—Зива последовательности [Lempel—Ziv complexity] — отношение объема словаря, построенного по последовательности символов алгоритмом сжатия Лемпела—Зива, к объему словаря, построенного по *последовательности случайной идеальной*. Поня-

тие с. Л.—З. п. находит применение, например, при построении *наборов тестов статистических*.

Сложность линейная последовательности [linear complexity] — для последовательности над кольцом R — наименьшая длина *регистра сдвига линейного* над R, порождающего эту последовательность.

Сложность последовательности 2-адическая [2-adic complexity] — под 2-адической сложностью бесконечной периодической двоичной последовательности v понимается величина $\log_2(\max(|p|, |q|)$, где p/q — несократимая дробь, у которой 2-адическое представление совпадает с последовательностью v.

Сложность последовательности по Колмогорову [Kolmogorov complexity] — под сложностью последовательности v по Колмогорову понимают наименьшую длину последовательности u, перерабатываемой некоторым алгоритмом (машиной Тьюринга) в последовательность v. Понятие предложено А. Н. Колмогоровым для алгоритмического определения понятий случайности и количества информации. Другие подходы к определению сложности и случайности разрабатывали Р. Соломонофф, П. Мартин-Леф и др. В *криптографии* алгоритмические подходы к определению случайности находят применение при построении и анализе свойств *генераторов последовательностей псевдослучайных криптографически сильных*. См. также *энтропия алгоритмическая*.

Сообщение открытое [plaintext, cleartext] — в широком смысле — данные, представленные в виде последовательности над конечным множеством (буквы, цифры и др. символы) или непрерывного сигнала (звуки, изображения и др.), подлежащие *зашифрованию*. В более узком смысле — аналогичные данные, обладающие доступным семантическим (смысловым) содержанием и предназначенные для хранения, преобразования или передачи.

Сообщение шифрованное [ciphertext] — сообщение, полученное в результате *зашифрования сообщения открытого*.

Способ шифрования [encryption method (cipher type)] — способ преобразования множества *сообщений открытых* в множество *сообщений шифрованных* и обратно. Основные известные с. ш. реализуются *шифром гаммирования*, *шифром замены простой* и *шифром перестановки*, а также их комбинациями.

Средства криптографические [cryptographic tools, cryptographic mechanisms] — в широком смысле — средства обеспечения безопасности информации, использующие *функции криптографические*. В узком смысле — средства, реализованные в виде документов, механических, электромеханических, электронных технических устройств или

программ, предназначенные для выполнения функций *системы криптографической*.

Средства криптографические аппаратные [cryptographic hardware (device, facility)] — *средства криптографические*, реализованные в виде специальных технических устройств. Реализуют одну или несколько *функций криптографических* или их частей.

Средства криптографические встраиваемые [build-in cryptographic mechanisms] — *средства криптографические*, внешние по отношению к операционной системе, но зависящие от нее. К ним относятся различные интерфейсы прикладного программирования.

Средства криптографические выше прикладного уровня [above the application layer cryptographic mechanisms] — *средства криптографические программные*, реализаванные таким образом, что все данные заранее преобразуются так, чтобы они могли быть переданы непосредственно с помощью существующего протокола прикладного уровня, и чтобы при этом были реализованы необходимые службы и обеспечивался необходимый уровень безопасности.

Средства криптографические наложенные [additional cryptographic mechanisms] — *средства криптографические*, не связанные с функционированием операционной системы.

Средства криптографические прикладного уровня [application layer cryptographic mechanisms] — *средства криптографические программные*, реализованные таким образом, что модули, выполняющие *функции криптографические*, расположены только на прикладном уровне и не требуют никаких модификаций для программных модулей и интерфейсов для более низких уровней. Это означает, что для обеспечения функций безопасности должны быть модифицированы как прикладные протоколы, так и сами прикладные программы, использующие эти протоколы.

Средства криптографические программные [software cryptographic mechanism] — программные средства, реализующие одну или несколько *функций-сервисов безопасности криптографических*. Различают с. к. п. с выполнением в контексте пользователя и на уровне ядра или системном уровне операционной системы. С. к. п. с выполнением в контексте пользователя, как правило, ориентированы на выполнение ограниченного множества *функций криптографических* и решают какую-либо одну конкретную задачу. Могут быть реализованы как в виде законченного программного продукта, интеграция которого заключается в обычной инсталляции данного продукта, так и в виде программных модулей, установка которых может требовать дополнительных проце-

дур встраивания их в программное обеспечение. С. к. п. с выполнением на уровне ядра или системном уровне ОС реализуются в виде системных функций, выполняемых на уровне ядра, либо на системном уровне (драйверы, динамические библиотеки). Для унификации реализации и использования функций криптографических различными приложениями в этом случае разрабатывается специальный *крипто API*.

Средства криптографические сетевого уровня [network layer cryptographic mechanism] — *средства криптографические программные*, реализованные таким образом, что модули, выполняющие *функции криптографические*, расположены только на сетевом уровне без каких бы то ни было модификаций для программных модулей и интерфейсов для уровня канала передачи данных и прикладного уровня.

Средства криптографические транспортного уровня [transport layer cryptographic mechanism] — *средства криптографические программные*, реализованные таким образом, что модули, выполняющие *функции криптографические*, расположены на транспортном уровне, который осуществляет контроль доставки информации и контроль ее *целостности*. Такая реализация имеет целью усиление безопасности сетевого программного интерфейса с помощью введения дополнительных возможностей, а также обеспечения возможности прикладным программам избирательно использовать эти дополнительные возможности.

Средства криптографические физического и канального уровня [physical and data layer cryptographic mechanism] — *средства криптографические аппаратные*, осуществляющие *шифрование* трафика (соединения) на физическом или канальном уровне, исполненные в виде *скремблеров*, шифрующих модемов, специализированных канальных адаптеров и т. п.

Средства криптографические штатные [cryptographic services] — *средства криптографические*, заложенные в функциональные возможности операционных систем.

Стандарт ISO 7498.2 [ISO 7498.2 standard] — международный стандарт под названием «Базовая эталонная модель взаимодействия открытых систем. Часть 2: Архитектура безопасности», утвержденный в 1989 г. Содержит впервые изложенную в наиболее полном виде концепцию *функций-сервисов безопасности*. В 1991 году этот стандарт был повторен в «рекомендации X.800: Архитектура безопасности взаимодействия открытых систем, для применений МККТТ». Содержит описание основных (базовых) функций-сервисов безопасности для случая взаимодействия двух систем, а также основных механизмов, обеспечивающих эти услуги, включая *средства криптографические*. Указано так-

же их желательное расположение в эталонной семиуровневой модели взаимодействия открытых систем. Для построения защищенных распределенных систем современные стандарты определяют и ряд других функций-сервисов безопасности, например, *туннелирование*, межсетевое экранирование и др.

Стандарт ISO/IEC 15408-99 [ISO/IEC 15408-99 standard, common criteria] — международный стандарт «Общие критерии оценки безопасности информационных технологий. Версия 2.0», определяющий порядок оценки компьютерных систем по требованиям безопасности при проведении сертификационных испытаний. В 2002 г. на его основе утверждены ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий», а также руководящий документ Гостехкомиссии «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». Определяет понятие профиля защиты, включающего цели защиты, обоснованные функциональные требования и требования адекватности. В соответствии с этим документом *система криптографическая* подлежит оценке по двум показателям: *системе управления ключами* и выполняемым *операциям криптографическим*. Их реализация должна соответствовать действующим стандартам. Оценке подлежат корректность реализации, полнота реализации всех режимов работы, форматов и протоколов взаимодействия, соответствие указанным в профиле целям, а также другие свойства, определяющие уровень гарантий конкретного продукта. Вместе с тем, в рамках данного подхода не подлежат оценке *стойкость криптографическая* и истинный уровень доверия к системе.

Стандарт подписи цифровой DSS [digital signature standard (DSS)] — стандарт *подписи цифровой* (США), принятый с 2000 г. Рекомендует для использования три *схемы подписи цифровой*: DSA — основана на вычислениях в мультипликативной группе конечного простого поля из семейства *схем подписи цифровой Эль Гамаля* (действует с 1994 г.); RSA — основана на вычислениях в кольце вычетов по составному модулю, ECDSA — основана на вычислениях в *группе точек кривой эллиптической*.

Стандарт подписи электронной цифровой ГОСТ Р 34.10-94 [GOST digital signature algorithm P 34.10-94] — первый российский стандарт *подписи цифровой*, действовавший с 1994 по 2002 г. Основан на вычислениях в мультипликативной группе конечного простого поля и принадлежит семейству *схем подписи цифровой Эль Гамаля*.

Стандарт подписи электронной цифровой ГОСТ Р 34.10-2001 [GOST digital signature algorithm P 34.10-2001] — российский стандарт *подписи цифровой*, действующий с июля 2002 г. Определяет *алгоритм формирования подписи цифровой* и *алгоритм проверки подписи цифровой*. Основан на вычислениях в *группе точек кривой эллиптической* над конечным простым полем и принадлежит семейству *схем подписи цифровой Эль Гамаля*.

Стандарт функции хеширования SHS [secure hash standard (SHS)] — стандарт США, определяющий алгоритмы вычисления значения *хеш-функции*: алгоритм SHA-1 (введен в действие в 1995 г.) и алгоритмы SHA-256, SHA-384, SHA-512 (введены в действие в 2002 г.).

Стандарт функции хеширования ГОСТ Р 34.11-94 [GOST hash function P 34.11-94] — российский стандарт *хеш-функции*, действующий с 1994 г. Определяет алгоритм вычисления значения хеш-функции.

Стандарт шифрования AES [advanced encryption standard (AES)] — стандарт *шифрования* данных США, предназначенный для использования в *шифрсистемах симметричных*. Построен на основе *алгоритма зашифрования блочного базового* с размером блока 128 бит и длиной ключа 128, 192 или 256 бит. Введен в действие в 2002 г.

Стандарт шифрования DES [data encryption standard (DES)] — стандарт *шифрования* данных США, предназначенный для использования в *шифрсистемах симметричных*. Был первым в мире открытым официальным стандартом шифрования, действовавшим с 1977 по 1997 г. Построен на основе *алгоритма зашифрования блочного базового* с размером блока 64 бит и длиной *ключа* 56 бит. Имеет 4 *режима шифрования* и 2 *режима выработки кода аутентичности сообщения*.

Стандарт шифрования ГОСТ 28147-89 [GOST 28147-89] — российский стандарт *шифрования*, предназначенный для использования в *шифрсистемах симметричных*. Построен на основе *алгоритма зашифрования блочного базового* с размером блока 64 бит. Длина ключа — 256 бит заполнения ключевого запоминающего устройства (КЗУ) и 512 бит заполнения узлов замены (УЗ). Имеет 4 *режима шифрования* и *режим выработки имитовставки*.

Стандарт шифрования с депонированием ключей EES [escrowed encryption standard (EES)] — стандарт *шифрования* с депонированием ключей, принятый в США в 1994 г. Основан на использовании *алгоритма зашифрования блочного* Skipjack с добавлением в начале *шифртекста* специального блока информации, называемого LEAF

(law enforcement access field), позволяющего в случае необходимости по ключевой информации, хранящейся у двух официально назначенных для этой цели сторон, восстановить *ключ*.

Степень (порядок) нелинейности функции булевой [Boolean function degree] — степень многочлена Жегалкина, задающего булеву функцию.

Степень функции алгебраическая [algebraic degree of a function] — для *функции дискретной* от n переменных над конечным полем P — минимальная степень многочлена от n переменных над полем P, представляющего данную функцию. Для булевых функций понятие *степени алгебраической* совпадает с понятием *степени нелинейности функции булевой*.

Стойкость доказуемая [provable security] — см. *стойкость криптографическая теоретическая*.

Стойкость криптографическая [cryptographic security] — фундаментальное понятие *криптографии* — свойство *криптосистемы* (*криптопротокола*), характеризующее её (его) способность противостоять *атакам противника* и/или *нарушителя*, как правило, имеющим целью получить *ключ секретный* или *сообщение открытое*. Развиваются два основных подхода к определению и оценке стойкости — *стойкость теоретическая* и *стойкость практическая*.

Стойкость (криптосистемы) практическая [practical security (of the cryptosystem)] — вычислительная сложность алгоритма (см. *сложность алгоритма временна́я, сложность алгоритма емкостная, сложность коммуникационная*), реализующего наилучшую в определенном смысле *атаку* на *криптосистему*. Чаще всего под с. п. понимают временну́ю сложность выполнения успешной атаки на криптосистему наиболее быстрым из известных алгоритмов при реальных предположениях о свойствах криптосистемы и ее применении, а также о вычислительных машинах, на которых она будет реализовываться. Такой подход, с учетом перспектив развития вычислительных машин, позволяет оценить время, в течение которого данная криптосистема будет обеспечивать защищенность информации. См. также *стойкость криптографическая*.

Стойкость примитива криптографического [security of a cryptographic primitive] — соответствие свойств *примитива криптографического* его предназначению. Например, стойкость *функции односторонней* предполагает отсутствие эффективных (полиномиальных) алгоритмов ее инвертирования, стойкость *хеш-функции криптографической* — отсутствие эффективных методов построения *коллизий* и т. п.

Стойкость (шифрсистемы) совершенная [perfect secrecy] — свойство *системы шифрования*, заключающееся в том, что *текст шифрованный* не содержит информации о *ключе* и *тексте открытом*, кроме, возможно, его длины. Например, таким свойством обладает шифрсистема *гаммирования*, если применяемая *гамма* является реализацией *последовательности случайной идеальной*.

Стойкость (криптосистемы) теоретическая [theoretical security] — *стойкость криптографическая*, определяемая в рамках некоторой математической модели. Основные подходы к определению с. т. в настоящее время — *стойкость теоретико-информационная* и *стойкость теоретико-сложностная*. Рассмотрение с. т. в рамках абстрактных математических моделей позволяет говорить о *стойкости доказуемой*.

Стойкость теоретико-информационная (шенноновская) [information-theoretic (Shannon) security] — вид *стойкости теоретической*, определяемый с точки зрения математической теории информации. С. т.-и. *криптосистемы* обычно характеризуется количеством информации (в смысле К. Шеннона) относительно неизвестного *противнику* и/или *нарушителю* элемента криптосистемы, содержащимся в перехваченном *тексте шифрованном* или других доступных данных и вычисленным в рамках той или иной вероятностной модели. Говорят также, что с. т.-и. криптосистемы характеризует ее способность противостоять *атакам* со стороны противника и/или нарушителя, располагающего неограниченными вычислительными ресурсами.

Стойкость теоретико-сложностная [complexity-based security] — вид *стойкости теоретической*, определяемый с точки зрения математической теории сложности алгоритмов. С. т.-с. *криптосистемы* означает ее способность противостоять *атакам* со стороны *противника* и/или *нарушителя*, располагающего ограниченными вычислительными ресурсами. Ограниченность ресурсов при этом обычно понимается в том смысле, что противник может использовать только алгоритмы, для которых *сложность алгоритма временная* (*емкостная*, *коммуникационная*) удовлетворяет заданным ограничениям (например, полиномиальные алгоритмы). Как правило, с. т.-с. основывается на каком-либо *предположении криптографическом*.

Структура доступа [access structure] — в *схеме разделения секрета* — разбиение семейства всех подмножеств конечного множества *участников* S на два подсемейства. Множества из первого семейства называются правомочными коалициями, а множества из второго — неправомочными коалициями.

Структура статистическая функции булевой [statistic structure of Boolean function] — для булевой функции f от n переменных — набор из 2^n чисел $\Delta_a^f = 2^{n-1} - \|f(x) + (a, x)\|$, $a \in \{0, 1\}^n$. Числа Δ_a^f называются коэффициентами структуры статистической.

Структура функции линейная [linear structure of function] — для булевой функции $f\colon \{0, 1\}^n \to \{0, 1\}$ — множество таких ненулевых векторов $\alpha \in \{0, 1\}^n$, что $f(x) + f(x + \alpha) \equiv \text{const}$. Если множество таких векторов не пусто, то говорят, что функция f обладает линейной структурой.

Схема идентификации [identification scheme] — см. *протокол идентификации*.

Схема подписи цифровой [digital signature scheme] — состоит из двух алгоритмов, *алгоритма формирования подписи цифровой* и *алгоритма проверки подписи цифровой*. Надежность с. п. ц. определяется сложностью решения следующих трех задач для лица, не являющегося владельцем *ключа секретного*: *подделки подписи цифровой*, то есть вычисления значения подписи под заданным документом; создания подписанного сообщения, то есть нахождения хотя бы одного сообщения с правильным значением подписи (*подделка подписи цифровой экзистенциальная*); подмены сообщения, то есть подбора двух различных сообщений с одинаковыми значениями подписи.

Схема подписи цифровой вслепую [blind signature scheme] — *схема подписи цифровой*, в которой *алгоритм формирования подписи цифровой* выполняется вслепую в том смысле, что этот алгоритм применяется к специально сформированному сообщению, из которого без знания секретного ключа нельзя получить никакой информации о том сообщении, которое будет извлечено из него вместе с корректной подписью получателем. Используется в *системах платежей электронных* как средство обеспечения *неотслеживаемости*.

Схема подписи цифровой вслепую справедливая [fair blind signature scheme] — *схема подписи цифровой вслепую*, в которой *неотслеживаемость* получателей подписей может быть, при определенных условиях, отозвана. В *системах платежей электронных* такие схемы используются для предотвращения так называемых «идеальных» преступлений (безусловная *неотслеживаемость* электронных платежных средств обеспечивает преступникам возможность безопасного получения выкупа или отмывания денег).

Схема подписи цифровой групповой [group signature scheme] — *схема подписи цифровой*, в которой правом вычисления значения подписи обладают только члены определенной группы *участников*, каж-

дый из которых обладает своим *ключом секретным*. Проверка *подписи цифровой* осуществляется с помощью единственного *ключа открытого*. Подписавший сообщение член группы остается анонимным. Его анонимность может быть нарушена только в случае необходимости разрешения спорной ситуации.

Схема подписи цифровой конфиденциальной [undeniable signature scheme] — *схема подписи цифровой*, в которой процедура проверки подписи предусматривает участие подписавшего. Поэтому факт подписания того или иного сообщения остается конфиденциальным и может быть установлен только в том случае, если подписывающий дает на это согласие. В с. п. ц. к. *алгоритм проверки подписи цифровой* замещается парой *протоколов*, с помощью которых подписавший *доказывает* с *разглашением нулевым*, что подпись корректна, либо, напротив, некорректна. Как и в других схемах подписи цифровой, споры о подлинности подписей решаются с помощью процедуры *арбитража*.

Схема подписи цифровой с доказуемостью подделки [fail-stop signature scheme] — *схема подписи цифровой*, позволяющая в случае обнаружения *подделки подписи* в вероятностью близкой к единице доказать этот факт третьим лицам. Первоначально появилась как одноразовая, то есть её использование прекращалось после проведения доказательства подделки, но в дальнейшем была модифицирована для случая многоразового использования.

Схема подписи цифровой Эль Гамаля [El Gamal digital signature scheme] — *схема подписи цифровой*, основанная на *задаче логарифмирования дискретного*. В более широком смысле говорят о семействе схем подписи цифровой Эль Гамаля, к которому относят саму схему Эль Гамаля, схему Шнорра, схему стандарта DSA (США), ГОСТ Р.34.10 и др.

Схема (n, t)-пороговая [(n, t)-threshold scheme] — см. *схема разделения секрета пороговая*.

Схема разделения секрета [secret sharing scheme] — состоит их трех объектов: *структуры доступа* и двух протоколов, называемых протоколом разделения секрета и протоколом восстановления секрета. Исходной информацией протокола разделения секрета служит секрет s, а выходом — набор *долей секрета* $s_1, \ldots, s_n$. Доля s_i передается i-му участнику. Всякая правомочная коалиция может однозначно восстановить секрет s с помощью долей своих частников, используя алгоритм восстановления секрета, а совокупность долей секрета, полученных любой неправомочной коалицией, не позволяет получить секрет s. В некоторых с. р. с. вместо алгоритма необходим *протокол разделения секрета*.

Схема разделения секрета идеальная [ideal secret sharing scheme] — *схема разделения секрета*, в которой число битов, содержащихся в каждой *доле секрета*, равно числу битов, содержащихся в самом секрете.

Схема разделения секрета пороговая [threshold secret sharing scheme, (n, t)-threshold scheme, син. *схема* (n, t)*-пороговая*] — *схема разделения секрета* с n участниками для *структуры доступа*, в которой правомочными являются все коалиции, содержащие не менее t *участников* для некоторого t, а все коалиции с меньшим числом частников — неправомочны.

Схема разделения секрета совершенная [perfect secret sharing scheme] — *схема разделения секрета*, в которой *доли секрета* любой неправломочной коалиции не позволяет получить никакой информации о значении секрета. Такие схемы называют совершенными, чтобы отличить их от тех схем разделения секрета, в которых неправомочные коалиции могут получить частичную информацию о секрете. См. также *структура доступа*.

Схема распределения ключей предварительного [preliminary key distribution scheme] — *схема разделения секрета*, применяемая в сети связи для уменьшения объема хранимой информации о *ключах*. Суть с. р. к. п. состоит в том, что предварительно распределяются не ключи, а сгенерированные в *центре распределения ключей* секретные данные меньшего объема, по которым каждый пользователь самостоятельно вычисляет по оговорённому алгоритму необходимый для связи ключ. С. р. к. п. должна быть устойчивой относительно компрометации части ключей, в том числе, вследствие обмана или сговора некоторых пользователей, и гибкой, то есть быстро восстанавливаться как после частичной компрометации, так и после подключения новых пользователей.

Схема Фейстеля (Файштеля) [Feistel scheme, син. *преобразование Фейстеля*] — способ построения *цикла* (*раунда*) *шифрования* в *алгоритмах шифрования итеративных* (блочных) на основе *регистра сдвига нелинейного* длины 2 с функцией обратной связи, зависящей от *ключа циклового* (*раундового*). Схема названа по имени одного из разработчиков и запатентована в США в 1974 г.

Т

Таблица ортогональная [orthogonal array] — матрица размеров $(\lambda \cdot v^t) \times k$, составленная из v различных элементов и такая, что в любых её t столбцах, $2 \leqslant t \leqslant k$, $\lambda \geqslant 1$, каждый из v^t возможных векторов длины t встречается как строка ровно λ раз.

Таблица ортогональная простая [simple orthogonal array] — *таблица ортогональная*, в которой все строки попарно различны.

Текст открытый [plaintext] — *сообщение открытое*, представленное в виде последовательности над конечным алфавитом.

Текст шифрованный (шифртекст) [ciphertext] — текст, полученный в результате *зашифрования текста открытого*.

Теория аутентификации Симмонса [Simmons authentication theory] — теория *протоколов аутентификации сообщений* стойких безусловно для *систем имитозащиты*, разработанная Г. Симмонсом, аналог теории К. Шеннона систем (безусловно стойких) секретной связи. Основу теории аутентификации составляют модель *кода аутентификации*, определение атак — *имитация* и *подмена*, и нижние границы длин *ключей* в *протоколах аутентификации сообщений* стойких безусловно.

Тест автокорреляции [autocorrelation test] — критерий проверки качества *последовательности псевдослучайной*, основанный на сравнении выборочной *функции автокорреляционной последовательности* с распределением этой функции для *последовательности случайной идеальной*. См. также *постулаты Голомба*.

Тест бита следующего (предсказатель) [next bit test (predictor)] — критерий проверки качества двоичной *последовательности псевдослучайной*, основанный на оценке качества наилучшего прогноза бита по значениям всех предыдущих битов. Для *последовательности случайной идеальной* вероятность совпадения бита с любым его прогнозом равна $1/2$.

Тест профиля сложности линейной [linear complexity profile test] — критерий проверки качества *последовательности псевдослучайной*, основанный на вычислении *сложности линейной* ее отрезков с помощью алгоритма Берлекемпа—Мэсси и на сравнении выборочного распределения полученных значений с их распределением для *последовательности случайной идеальной*.

Тест серий [run test] — критерий проверки качества *последовательности псевдослучайной*, основанный на сравнении суммарного числа серий из нулей и серий из единиц (в случае двоичной последовательно-

сти) с распределением этого числа для *последовательности случайной идеальной*.

Тест универсальный Маурера [Maurer universal test] — критерий проверки качества *последовательности псевдослучайной*, основанный на вычислении сумм логарифмов от длин промежутков между повторными появлениями *мультиграмм* заданной длины и сравнении этой суммы с ее распределением для *последовательности случайной идеальной*. Универсальность теста состоит в том, что при неограниченном увеличении длин мультиграмм последовательности он обнаруживает отличие любой неидеальной стационарной случайной последовательности от идеальной.

Тест частот цепочек [serial test] — критерий проверки качества *последовательности псевдослучайной*, основанный на разбиении ее на цепочки заданной длины и сравнении эмпирических частот появления разных цепочек с их распределением для *последовательности случайной идеальной*.

Тест частотный [frequency test] — критерий проверки качества *последовательности псевдослучайной*, основанный на вычислении частот появлений знаков в отрезках последовательности и сравнении этих частот с их распределением для *последовательности случайной идеальной*.

Транзакция (протокол) депозита [deposit transaction (protocol)] — *протокол криптографический*, компонент *системы платежей электронных автономной*. В т. д. два *участника* — продавец и банк. Продавец посылает банку *монеты электронные* для депозита. Банк проверяет подлинность *денег электронных* и, после решения *проблемы повторной траты денег электронных* методом идентификации нарушителя, post factum выполняет надлежащую процедуру.

Транзакция (протокол) платежа [payment transaction (protocol)] — *протокол криптографический*, компонент *системы платежей электронных*. В случае *системы платежей электронных централизованной* в т. п. три *участника* — покупатель, продавец и банк. Покупатель передает *деньги электронные* продавцу, который, в свою очередь, пересылает их в банк. Последний проверяет подлинность денег электронных, а также выясняет, не были ли они уже потрачены ранее. Если все корректно, банк кладет деньги электронные на счет продавца и уведомляет его об этом. В *системах платежей электронных автономных* в т. п. два участника — покупатель и продавец. Продавец может проверить только подлинность полученных денег электронных, которые он в дальнейшем в любой момент времени может положить на свой счет

с помощью *транзакции депозита*. Поскольку банк не участвует в т. п., существует угроза повторной траты денег электронных.

Транзакция (про́токол) снятия со счета [withdrawal transaction (protocol)] — *протокол криптографический*, компонент *системы платежей электронных*. В т. с. со с. два *участника* — банк и покупатель, являющийся клиентом этого банка. Покупатель передает банку запрос на снятие со счета определенной суммы, и банк выдает эту сумму *деньгами электронными*. Для защиты денег электронных от подделки банк, как правило, использует *схему подписи цифровой*. *Неотслеживаемость* платежей, осуществляемых деньгами электронными, обычно осуществляется за счет применения *схемы подписи цифровой вслепую*.

Туннелирование [tunnelling] — процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. Т., как и экранирование, можно рассматривать как самостоятельную *функцию-сервис безопасности*. Его суть состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт». Данный сервис может применяться для обеспечения *конфиденциальности* и *целостности* всей передаваемой порции, включая служебные поля. Т. может применяться как на сетевом, так и на прикладном уровнях. Комбинация т. и *шифрования* позволяет реализовать закрытые виртуальные частные сети.

У

Угроза [threat] — потенциальная опасность нарушения одного или нескольких свойств *системы криптографической* (*протокола криптографического*), например, *конфиденциальности*, *целостности*, *аутентификации*, *невозможности отказа*, *неотслеживаемости*.

Угроза активная [active threat] — *угроза*, которая может быть реализована путем намеренного несанкционированного вмешательства в работу *криптосистемы* (*протокола криптографического*).

Усложнение последовательности линейной рекуррентной [linear recurrent sequence confusion] — преобразование *последовательности линейной рекуррентной* с целью усложнения ее аналитического строения. Одним из распространенных способов у. п. л. р. является ее преобразование с помощью *генератора фильтрующего*.

Устройство криптографическое [cryptographic device] — *средство криптографическое аппаратное*, выполненное в виде отдельного устройства.

Участник (протокола) [party] — субъект, участвующий в той или иной форме в выполнении *протокола*.

Участник нечестный [dishonest party] — см. *нарушитель*.

Участник честный [honest party] — *участник протокола криптографического*, владеющий всей необходимой информацией, в т. ч., если требуется, *ключами секретными*, и выполняющий действия в соответствии с протоколом.

Ф

Формирование подписи цифровой [generation digital signature] — см. *алгоритм формирования подписи цифровой*.

Функции-сервисы безопасности криптографические [cryptographic service] — *функции-сервисы безопасности*, обеспечиваемые *средствами криптографическими*. К ним относятся: *конфиденциальность*, *аутентификация*, обеспечение *целостности*, *невозможность отказа* от ранее совершенных действий и др.

Функция автокорреляционная последовательности [autocorrelation function of sequence] — для двоичной последовательности $u(0), \ldots, u(n-1)$ функция автокорреляционная задается равенством

$$C_u(d) = \frac{1}{n} \cdot \sum_{i=0}^{n-1} (-1)^{u(i)+u(i+d \pmod n)}, \quad d \in \{1, \ldots, n-1\}.$$

Функция автокорреляционная функции булевой [autocorrelation function of Boolean function] — функция автокорреляционная $C_f(u)\colon \{0;1\}^n \to Z$ булевой функций f от n переменных определяется равенством $C_f(u) = \frac{1}{2^n} \cdot \sum\limits_{x \in \{0;1\}^n} (-1)^{f(x)+f(x+u)}$, то есть эта функция является *функцией кросс-корреляции* между f и f.

Функция без запретов [interdiction free function] — *функция дискретная*, не имеющая *запретов функции*.

Функция дискретная [discrete function] — функция, отображающая конечное множество X в конечное множество Y. Наиболее важными классами ф. д. являются булевы (двоичные) функции и k-значные функции. Булевы функции отображают n-ю декартову степень множества $\{0, 1\}$ в множество $\{0, 1\}$, а k-значные функции отображают n-ю декартову степень множества $\{0, 1, \ldots, k-1\}$ в множество $\{0, 1, \ldots, k-1\}$, $k > 2$. При этом число n равно количеству переменных ф. д.

Функция зашифрования [encryption function] — функция зашифрования описывает процесс *зашифрования* и осуществляет зависящее от *ключа* отображение последовательностей *блоков текста* (*сообщения*) *открытого* в последовательности *блоков текста* (*сообщения*) *шифрованного*. Доопределяется на множество всех текстов (сообщений) открытых и реализуется *алгоритмом зашифрования*.

Функция корреляции взаимной [cross-correlation function] — см. *функция кросс-корреляции*.

Функция корреляционно-иммунная [correlation immune function] — функция, являющаяся *корреляционно-иммунной порядка* k для некоторого k.

Функция корреляционно-иммунная порядка k [correlation immune function of order k] — *функция дискретная* $f\colon X^n \to X$, $|X| < \infty$, для которой случайные величины $f(x_1, \ldots, x_n)$ и $(x_{i_1}, \ldots, x_{i_k})$ независимы для любого подмножества $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$, если $(x_1, \ldots, x_n)$ — случайный вектор, имеющий равномерное распределение на X^n. Если f — булева функция, то корреляционная иммунность порядка k эквивалентна равенству нулю коэффициентов Уолша—Адамара $\tilde{f}(\beta)$ для всех ненулевых векторов β веса не выше k. См. также *преобразование Уолша—Адамара*.

Функция криптографическая [cryptographic function] — функция, необходимая для реализации *системы криптографической*. К таким функциям относятся: генерация *ключей*, генерация *последовательностей псевдослучайных*, *функция шифрования*, вычисление и проверка значений *кода аутентичности сообщения* и *подписи цифровой*, вычисление значения *хеш-функции* и др.

Функция кросс-корреляции [cross-correlation function, син. *функция корреляции взаимной*] — функция кросс-корреляции $C_{f,g}(t)$: $\{0,1\}^n \to Z$ между булевыми функциями f и g от n переменных задается равенством

$$C_{f,g}(t) = \frac{1}{2^n} \cdot \sum_{x \in \{0,1\}^n} (-1)^{f(x)+g(x+t)}.$$

Функция невырожденная [nondegenerate function] — функция, существенно зависящая от всех своих переменных.

Функция негомоморфная совершенно [perfectly nonhomomorphic function] — *функция дискретная* $f\colon X \to Y$, для которой при каждом ненулевом $a \in X$ функция $f(x+a) - f(x)$ является *сбалансированной*. Понятие ф. н. с. обобщает понятие *функции совершенно нелинейной* на случай недвоичных функций.

Функция нелинейности максимальной [maximal nonlinearity function] — булева функция f от n переменных, для которой *нелинейность функции булевой* f достигает своего максимального возможного значения. Если n четно, то множество всех ф. м. совпадает с множеством *функций совершенно нелинейных*. В тоже время, ф. м., в отличие от функций совершенно нелинейных, существуют и в случае, когда n нечетно.

Функция однонаправленная [one-way function] — см. *функция односторонняя*.

Функция односторонняя [one-way function, син. *функция однонаправленная*] — отображение множества всех слов конечной длины n над конечным алфавитом, для которого существует такое $\gamma < \infty$, что образ любого слова длины n можно вычислить за $O(n^\gamma)$ операций, но ни для какого $\beta < \infty$ не существует алгоритма, вычисляющего для любого слова длины n его прообраз за $O(n^\beta)$ операций Понятие ф. о. используется, в основном, при конкретизации определения *стойкости криптографической шифрсистем асимметричных*. Вопрос о существовании ф. о. является открытым. Доказательство односторонности какой-либо функции означало бы доказательство гипотезы $\mathrm{NP} \neq \mathrm{P}$ в теории сложности алгоритмов. Различают ф. о. сильные, ф. о. слабые, функции дистрибутивно односторонние, подлинные и др. Иногда ф. о. называют эффективно вычислимую функцию, для которой не известен эффективный алгоритм обращения.

Функция равновероятная [balanced function] — см. *функция сбалансированная*.

Функция расшифрования [decryption function] — функция, описывающая процесс *расшифрования* и осуществляющая отображение, обратное к *функции зашифрования*. Доопределяется на множество всех текстов (сообщений) шифрованных и реализуется *алгоритмом расшифрования*.

Функция с запретами [function with interdictions] — *функция дискретная*, для которой существует *запрет функции*. Выходная последовательность *генератора фильтрующего*, построенного с помощью ф. с з., является *последовательностью псевдослучайной*, в которой отсутствуют некоторые *мультиграммы* символов, поэтому она может быть отбракована *набором тестов статистических*.

Функция с секретом [trapdoor function] — *функция дискретная*, зависящая от параметра (секрета, описания секрета). Знание параметра позволяет эффективно (с полиномиальной сложностью) вычислять и инвертировать данную функцию. Если параметр неизвестен, то

не существует эффективного алгоритма инвертирования функции. Семейство ф. с с. обладает свойствами *функции односторонней*. Применение ф. с с. предполагает построение соответствующего *генератора функций с секретом*, т. е. эффективного алгоритма, порождающего пары (функция, секрет). Например, см. *шифрсистема асимметричная*.

Функция сбалансированная [balanced function, син. *функция равновероятная*] — *отображение сбалансированное*, у которого значение параметра m равно 1.

Функция сбалансированная по выходу [output balanced function] — *функция дискретная* $f\colon X^n \to X^m$, для которой каждый элемент $y \in X^m$ имеет одно и то же число прообразов.

Функция сжатия [compression function] — функция, отображающая входные данные, состоящие из текущего *хеш-значения* и очередного блока хешируемого сообщения, в новое хеш-значение. Используется в интерактивных конструкциях *хеш-функций*, позволяющих хешировать сообщения произвольной длины.

Функция со входом сбалансированным [input balanced function] — *функция дискретная* $f\colon X^n \to X^m$, у которой аргумент $x = (x_1, \ldots, x_n)$ рассматривается как случайный вектор с взаимно независимыми и равномерно распределенными на X координатами.

Функция совершенно нелинейная [perfect nonlinear function] — булева функция f от n переменных, для которой при любом ненулевом векторе $\alpha \in \{0; 1\}^n$ сумма $f(x+\alpha)+f(x)$ является *функцией сбалансированной*. Ф. с. н. существуют только в том случае, когда n четно.

Функция усложнения [combining function] — функция, используемая для увеличения аналитической сложности промежуточных последовательностей, например, в *генераторах фильтрующих* и *генераторах комбинирующих шифрсистем поточных* или реализуемая s-блоками в *шифрсистемах блочных*. Должна обладать, в частности, *свойством рассеивания* и/или *свойством усложнения* и/или *свойством перемешивания*.

Функция фильтрующая [filtering function] — функция, используемая для усложнения *последовательности псевдослучайной*, вырабатываемой *регистром сдвига линейным*, при построении *последовательности управляющей*. См. также *генератор фильтрующий*.

Функция шифрования [encryption function] — термин, объединяющий понятия *функции зашифрования* и *функции расшифрования*.

Функция эластичная [resilient function] — *функция k-эластичная* при некотором k.

Функция k-эластичная [k-resilient function] — *функция дискретная, являющаяся функцией корреляционно-иммунной порядка k и функцией сбалансированной по выходу.*

Функция эластичная линейная [linear resilient function] — *функция эластичная* $f\colon GF(q)^n \to GF^m(q)$, у которой все m координатных функций являются линейными.

Функция-сервис аутентификации источника данных [data origin authentication service] — *функция-сервис безопасности*, обеспечивающая возможность проверки того, что полученные данные действительно созданы конкретным источником. Данная функция не обеспечивает защиты от повторного навязывания или модификации данных.

Функция-сервис аутентификации сторон [peer entity authentication service] — *функция-сервис безопасности*, обеспечивающая возможность проверки того, что одна из сторон информационного взаимодействия действительно является той, за которую она себя выдает. Применяется с целью защиты от атаки типа *имитация* и от *атаки на протокол с передачей повторной.*

Функция-сервис безопасности [security services] — защитная функция, выполняемая подсистемой безопасности и определяемая ее целевым назначением. В соответствии со *стандартом ISO 7498.2* выделено пять классов ф.-с. б. для архитектуры безопасности эталонной модели взаимодействия: *аутентификация сторон и аутентификация источника данных*, *разграничение доступа*, *конфиденциальность*, *целостность* и *невозможность отказа* от факта отправления или получения сообщения.

Функция-сервис конфиденциальности данных [data confidentiality service] — *функция-сервис безопасности*, обеспечивающая невозможность несанкционированного получения доступа к данным или раскрытия данных.

Функция-сервис обеспечения невозможности отказа [non-repudiation service] — *функция-сервис безопасности*, обеспечивающая *невозможность отказа* одной из сторон от факта участия в информационном обмене (полностью или в какой либо его части).

Функция-сервис обеспечения невозможности отказа с доказательством источника [non-repudiation service with proof of origin] — *функция-сервис безопасности*, обеспечивающая *невозможность отказа* отправителя от факта отправления сообщения.

Функция-сервис обеспечения невозможности отказа с доказательством получения [non-repudiation service with proof of deliv-

ery] — *функция-сервис безопасности*, обеспечивающая *невозможность отказа* получателя от факта получения сообщения.

Функция-сервис обеспечения целостности соединения без восстановления [connection integrity service without recovery] — *функция-сервис безопасности*, обеспечивающая возможность проверки того, что все данные, передаваемые при установленном соединении, не подверглись модификации, без восстановления этих данных.

Функция-сервис обеспечения целостности соединения с восстановлением [connection integrity service with recovery] — *функция-сервис безопасности*, обеспечивающая возможность проверки того, что все данные, передаваемые при установленном соединении, не подверглись модификации, с восстановлением этих данных.

Функция-сервис разграничения доступа [access control service] — *функция-сервис безопасности*, обеспечивающая невозможность несанкционированного использования ресурсов системы. Данный термин понимается в самом широком смысле. На практике решение о предоставлении доступа основывается на *аутентификации сторон*. См. *система разграничения доступа*.

Функция-сервис целостности данных [data integrity service] — *функция-сервис безопасности*, обеспечивающая возможность проверки того, что защищаемая информация не подверглась несанкционированной модификации или разрушению.

X

Хеш-значение [hash-code, hash-result, hash-value, hash, imprint, digital fingerprint, message digest] — значение *хеш-функции* для данного аргумента.

Хеш-функция [hash function] — функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно фиксированной длины.

Хеш-функция криптографическая [cryptographic hash function] — *хеш-функция*, сочетающая в себе свойства *хеш-функции односторонней*, *хеш-функции с прообразами вторыми трудно обнаружимыми* и *хеш-функции с коллизиями трудно обнаружимыми*. Особо выделяют *хеш-функции криптографические, задаваемые ключом*, имеющие другое содержание.

Хеш-функция криптографическая, задаваемая ключом [cryptographic hash function with key] — *хеш-функция криптографическая*, реализуемая *алгоритмом кодирования имитозащищающего*, или

кодом аутентификации, и предназначенная для обеспечения невозможности для *противника* и/или *нарушителя* создавать новые или модифицировать передаваемые (или хранимые) сообщения.

Хеш-функция односторонняя [one-way hash function (OWHF)] — *хеш-функция*, для которой задача поиска прообразов заданных значений является вычислительно трудной.

Хеш-функция с коллизиями трудно обнаружимыми [collision-intractable hash function] — *хеш-функция*, для которой задача поиска *коллизий* является вычислительно трудной.

Хеш-функция с прообразами вторыми трудно обнаружимыми [second preimage resistant hash function] — *хеш-функция*, для которой задача поиска *коллизий прообраза второго* является вычислительно трудной.

Ц

Целостность [integrity] — отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью. Необходимым условием соблюдения ц. является защищённость сообщения от преднамеренной или случайной несанкционированной модификации или уничтожения.

Целостность выделенных полей [selective field integrity] — обеспечение возможности проверки того, что выделенные поля передаваемых данных не подверглись несанкционированной модификации или уничтожению.

Центр доверия [trusted entity, trusted authority, authority. trusted third party] — особый *участник протокола криптографического*, которому доверяют все остальные его участники, введенный в протокол для усиления его безопасности. Различают следующие виды ц. д.: *центр регистрации*, *центр распределения ключей*, *центр сертификации*, *центр установки меток временных*, центр нотаризации и т. д.

Центр распределения ключей [key distribution center] — *центр доверия*, распределяющий среди *участников* (*протокола*) *ключи секретные* в *шифрсистемах симметричных* или *шифрсистемах асимметричных*.

Центр регистрации [registration center] — *центр доверия*, который работает вместе с *центром сертификации*. выполняя роль местного автономного центра хранения реестра *сертификатов ключей*. Основные функции ц. р. — регистрация пользователей в системе и присвоение им уникальных идентификаторов, оптимизация управления реестром сер-

тификатов при большом числе запросов, позволяющая масштабировать систему управления сертификатами для большого числа пользователей на большой территории, одновременно сдвигая процесс подтверждения ближе к пользователям.

Центр сертификации (ключей открытых) [certification center] — *центр доверия*, обеспечивающий аутентичность *ключей открытых* путем придания им *сертификатов ключей*, заверенных *подписью цифровой*.

Центр удостоверяющий [certification authority] — в соответствии с Федеральным законом Российской Федерации от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи» — юридическое лицо, выполняющее следующие функции: изготовление *сертификатов ключей открытых* подписей цифровых; создание ключей *подписей цифровых* по обращению участников сети с гарантией сохранения в тайне *ключа секретного* подписи; приостановление и возобновление действия сертификатов ключей подписей, а также аннулирование их; ведение реестра сертификатов ключей подписей, обеспечение его актуальности и возможности свободного доступа к нему участников информационных систем; проверка уникальности ключей открытых подписей цифровых в реестре сертификатов ключей подписей и архиве ц. у.; выдача сертификатов ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии; осуществление по обращениям пользователей сертификатов ключей подписей подтверждения подлинности подписи цифровой в электронном документе в отношении выданных им сертификатов ключей подписей.

Центр установки меток (временных) [timestamping authority] — *центр доверия* или процесс, который связывает документ со временем его создания или последнего изменения для защиты от *атак*, в которых *противник* и/или *нарушитель* изменяет дату в недействительном *сертификате ключа* на то время, когда он был действителен.

Цикл (раунд) (протокола криптографического) [round, pass (of cryptographic protocol)] — в *протоколах криптографических* с двумя *участниками* — временной интервал, в котором активен только один из участников. Другое название — проход (pass) протокола. Цикл (раунд) завершается формированием и отсылкой сообщения с последующим переходом активного участника в состояние ожидания и передачей активности другому участнику. В протоколах с тремя и более участниками в синхронном случае цикл — период времени между двумя точками синхронизации. К очередной точке синхронизации каждый участ-

ник должен отослать все сообщения, которые ему предписано передать другим участникам в текущем ц. В *протоколах доказательства интерактивного* циклом (раундом) часто называют комбинацию из трех шагов: заявка, запрос, ответ. В асинхронном случае понятие цикла (раунда) условно.

Цикл жизненный ключей [key lifetime] — последовательность стадий, которые проходят *ключи* от момента генерации до момента уничтожения. Включает такие основные стадии, как: генерация, регистрация ключей (и пользователей), инициализация, период действия, хранение, смена, архивирование, уничтожение и восстановление.

Цикл (раунд) шифрования [round] — один шаг (из ряда однородных шагов) в *алгоритме шифрования итеративном*. Реализуется, как правило, с помощью относительно простых преобразований, обладающих определенными криптографическими свойствами.

Ш

Шаг (протокола) [step (of a protocol), protocol action] — конкретное законченное действие, выполняемое *участником* (*протокола*) во время одного *цикла* (*раунда*) протокола, например, вычисление значения некоторой функции, проверка правильности *сертификата ключа*, генерация случайного числа, отправка сообщения, и т. п.

Ширина покрытия группы [group cover width] — наименьшее k, для которого конечная группа G с системой образующих M представима в виде $G = M^{n_1} \cup \ldots \cup M^{n_k}$ при некоторых натуральных $n_1, \ldots, n_k$.

Шифр [cipher] — семейство обратимых отображений множества последовательностей *блоков текстов* (*сообщений*) *открытых* в множество последовательностей *блоков текстов* (*сообщений*) *шифрованных* и обратно, задаваемых *функцией шифрования*. Каждое из отображений определяется некоторым параметром, называемым *ключом*, и описывается некоторым *алгоритмом шифрования*, реализующим один из *режимов шифрования*. Математическая модель ш. включает *алгоритм зашифрования*, *алгоритм расшифрования*, определение режима шифрования, а также модель множества *текстов открытых*. В зависимости от способа представления текстов открытых (сообщений) различают блочные, поточные и другие ш. Основными требованиями, определяющими качество ш., являются: *стойкость криптографическая*, *имитостойкость*, *помехоустойчивость шифра* и др.

Шифр гаммирования [keystream cipher] — *шифр*, в котором *функция зашифрования* осуществляет *гаммирование*.

Шифр замены простой [substitution cipher] — *шифр*, в котором *функция зашифрования* состоит в замене *блоков текста* (*сообщения*) открытого *блоками текста* (*сообщения*) шифрованного в соответствии с *ключом*, представляющим собой подстановку на множестве блоков текста. См. также *ключ коммутаторный*.

Шифр перестановки [permutation cipher] — *шифр*, в котором *текст* (*сообщение*) *шифрованный* получается из *текста* (*сообщения*) *открытого* перестановкой *блоков текста* (сообщения) открытого.

Шифр совершенный [perfect cipher] — *шифр*, при использовании которого *текст шифрованный* не дает *противнику*, не знающему *ключа секретного*, никакой информации о *тексте открытом*, т. е. условное распределение на множестве текстов открытых при заданном тексте шифрованном совпадает с безусловным распределением на множестве текстов открытых.

Шифрование [encryption, enciphering] — термин объединяющий термины *зашифрование* и *расшифрование*.

Шифрование аппаратное [hardware encryption] — *шифрование*, выполняемое с применением *средств криптографических аппаратных*.

Шифрование программное [software encryption] — *шифрование*, выполняемое только с применением *средств криптографических программных*.

Шифрование сеанса [session encryption] — способ реализации сеанса связи между двумя сторонами, при котором все передаваемые в процессе его выполнения сообщения шифруются на специально сгенерированном для данного сеанса *ключе сеансовом*.

Шифрсистема [cryptosystem, cipher] — см. *система шифрования*.

Шифрсистема асимметричная [public-key cryptosystem, asymmetric cryptosystem, син. *шифрсистема с ключом открытым*] — *система шифрования*, в которой асимметричным образом используются ключи двух видов — *ключи открытые* и *ключи секретные*. Ключ открытый *участника протокола* задает процесс *зашифрования* направляемых в его адрес сообщений и является общедоступным. Ключ секретный участника протокола задает процесс *расшифрования* направляемых в его адрес сообщений и хранится им в тайне. *Стойкость криптографическая* ш. а. определяется трудоемкостью, с которой *противник* и/или *нарушитель* может вычислить ключ секретный, исходя из знания ключа открытого и другой дополнительной информации о шифрсистеме.

Шифрсистема блочная [block ciphering system] — *система шифрования*, в которой *функция зашифрования* реализуется *алгоритмом зашифрования блочным*.

Шифрсистема поточная [stream ciphering system] — *система шифрования*, в которой *функция зашифрования* реализуется *алгоритмом зашифрования поточным*.

Шифрсистема с ключом открытым [public-key cryptosystem] — См. *шифрсистема асимметричная*.

Шифрсистема с ключом секретным [private-key cryptosystem] — см. *шифрсистема симметричная*.

Шифрсистема симметричная [secret key cryptosystem, symmetric cryptosystem, син. *шифрсистема с ключом секретным*] — *система шифрования*, в которой симметричным образом используются секретные *ключи зашифрования* и *ключи расшифрования*. В ш. с. ключи зашифрования и расшифрования в большинстве случаев совпадают, а в остальных случаях один легко определяется по другому. *Стойкость криптографическая* ш. с. определяется трудоемкостью, с которой *противник* и/или *нарушитель* может вычислить любой из секретных ключей, и оценивается при общепринятом допущении, что противнику и/или нарушителю известны все элементы шифрсистемы, за исключением ключа секретного (*правило Керкгоффса*).

Шифрсистема RSA [RSA cryptosystem] — *шифрсистема асимметричная*, реализующая *алгоритм шифрования RSA*.

Шифртекст [ciphertext] — текст, полученный в результате *зашифрования текста открытого*.

Э

Энтропия [entropy] — теоретико-информационная характеристика распределения случайной величины. Энтропия (по К. Шеннону) дискретной случайной величины S с распределением $(p_1, \ldots, p_n, \ldots)$ равна $H(S) = -\sum\limits_i p_i \log(p_i)$.

Энтропия алгоритмическая [algorithmic entropy, kolmogorov complexity entropy] — введенная А. Н. Колмогоровым мера количества информации, необходимого для описания конечного объекта. Под э. а. двоичного слова понимают сложность этого слова относительно оптимального способа его описания. (См. *сложность последовательности по Колмогорову*). Понятие алгоритмической энтропии связано с понятием *энтропии* случайной величины (по К. Шеннону).

Шифр гаммирования [keystream cipher] — *шифр*, в котором *функция зашифрования* осуществляет *гаммирование*.

Шифр замены простой [substitution cipher] — *шифр*, в котором *функция зашифрования* состоит в замене *блоков текста* (*сообщения*) открытого *блоками текста* (*сообщения*) шифрованного в соответствии с *ключом*, представляющим собой подстановку на множестве блоков текста. См. также *ключ коммутаторный*.

Шифр перестановки [permutation cipher] — *шифр*, в котором *текст* (*сообщение*) *шифрованный* получается из *текста* (*сообщения*) *открытого* перестановкой *блоков текста* (сообщения) открытого.

Шифр совершенный [perfect cipher] — *шифр*, при использовании которого *текст шифрованный* не дает *противнику*, не знающему *ключа секретного*, никакой информации о *тексте открытом*, т. е. условное распределение на множестве текстов открытых при заданном тексте шифрованном совпадает с безусловным распределением на множестве текстов открытых.

Шифрование [encryption, enciphering] — термин объединяющий термины *зашифрование* и *расшифрование*.

Шифрование аппаратное [hardware encryption] — *шифрование*, выполняемое с применением *средств криптографических аппаратных*.

Шифрование программное [software encryption] — *шифрование*, выполняемое только с применением *средств криптографических программных*.

Шифрование сеанса [session encryption] — способ реализации сеанса связи между двумя сторонами, при котором все передаваемые в процессе его выполнения сообщения шифруются на специально сгенерированном для данного сеанса *ключе сеансовом*.

Шифрсистема [cryptosystem, cipher] — см. *система шифрования*.

Шифрсистема асимметричная [public-key cryptosystem, asymmetric cryptosystem, син. *шифрсистема с ключом открытым*] — *система шифрования*, в которой асимметричным образом используются ключи двух видов — *ключи открытые* и *ключи секретные*. Ключ открытый *участника протокола* задает процесс *зашифрования* направляемых в его адрес сообщений и является общедоступным. Ключ секретный участника протокола задает процесс *расшифрования* направляемых в его адрес сообщений и хранится им в тайне. *Стойкость криптографическая* ш. а. определяется трудоемкостью, с которой *противник* и/или *нарушитель* может вычислить ключ секретный, исходя из знания ключа открытого и другой дополнительной информации о шифрсистеме.

Шифрсистема блочная [block ciphering system] — *система шифрования*, в которой *функция зашифрования* реализуется *алгоритмом зашифрования блочным*.

Шифрсистема поточная [stream ciphering system] — *система шифрования*, в которой *функция зашифрования* реализуется *алгоритмом зашифрования поточным*.

Шифрсистема с ключом открытым [public-key cryptosystem] — См. *шифрсистема асимметричная*.

Шифрсистема с ключом секретным [private-key cryptosystem] — см. *шифрсистема симметричная*.

Шифрсистема симметричная [secret key cryptosystem, symmetric cryptosystem, син. *шифрсистема с ключом секретным*] — *система шифрования*, в которой симметричным образом используются секретные *ключи зашифрования* и *ключи расшифрования*. В ш. с. ключи зашифрования и расшифрования в большинстве случаев совпадают, а в остальных случаях один легко определяется по другому. *Стойкость криптографическая* ш. с. определяется трудоемкостью, с которой *противник* и/или *нарушитель* может вычислить любой из секретных ключей, и оценивается при общепринятом допущении, что противнику и/или нарушителю известны все элементы шифрсистемы, за исключением ключа секретного (*правило Керкгоффса*).

Шифрсистема RSA [RSA cryptosystem] — *шифрсистема асимметричная*, реализующая *алгоритм шифрования RSA*.

Шифртекст [ciphertext] — текст, полученный в результате *зашифрования текста открытого*.

Э

Энтропия [entropy] — теоретико-информационная характеристика распределения случайной величины. Энтропия (по К. Шеннону) дискретной случайной величины S с распределением $(p_1, \ldots, p_n, \ldots)$ равна $H(S) = -\sum\limits_i p_i \log(p_i)$.

Энтропия алгоритмическая [algorithmic entropy, kolmogorov complexity entropy] — введенная А. Н. Колмогоровым мера количества информации, необходимого для описания конечного объекта. Под э. а. двоичного слова понимают сложность этого слова относительно оптимального способа его описания. (См. *сложность последовательности по Колмогорову*). Понятие алгоритмической энтропии связано с понятием *энтропии* случайной величины (по К. Шеннону).

Я

Ящик черный [black-box] — конечный автомат, у которого известны только входной и выходной алфавиты и доступны для наблюдения выходные последовательности при произвольных входных последовательностях. Если дополнительно известна оценка числа состояний автомата, то говорят о ящике черном относительном.