А. Г. Коробейников, Ю.А.Гатчин

Математические основы криптологии

Учебное пособие

Санкт-Петербург 2004

УДК 511
Коробейников А. Г, Ю.А.Гатчин. Математические основы криптологии. Учебное пособие. СПб: СПб ГУ ИТМО, 2004. – 106 с, илл.

В данной книге представлен материал, необходимый для введения в теорию криптографичесих алгоритмов, математическим фундаментом которых является прикладная теория чисел. Это в первую очередь теория групп, теория колец и теория полей. Рассмотрены криптосистемы с секретным ключом (симметричные или классические), а также криптосистемы с открытым ключом (асимметричные). Кроме того, представлены основные положения криптографического протокола "электронная подпись". В каждом разделе приведены примеры на соответствующие темы.

Книга предназначена в первую очередь для студентов, обучающихся по специальности 075400 “Комплексная защита объектов информатизации”, но может быть интересна широкому кругу специалистов.

Илл. – 6, список литературы – 17 наим.

ВВЕДЕНИЕ

Долгое время наука криптография была засекречена, т.к. применялась, в основном, для защиты государственных и военных секретов. Термин "криптология" даже нельзя было произносить тем, кто профессионально работал в этой области, не говоря уже о каких бы то ни было открытых публикациях на эту тему. В открытых организациях, как учебных, так и научно-исследовательских, никто криптологией официально не занимался. Слово "криптология" впервые появилось у нас в переводной статье Дж. Л. Месси "Введение в современную криптологию" в тематическом выпуске ТИИЭР, т.76, № 5 за 1988 год. Освещающая классические вопросы криптологии, она может служить хорошим введением в предмет.

В настоящее время, методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц и организаций. Дело здесь совсем не обязательно в секретах, а в том, что сейчас очень большой обмен информацией происходит в цифровом виде через открытые каналы связи. К этой информации возможно применение угроз недружественного ознакомления, накопления, подмены, фальсификации и т.д. Наиболее надежные методы защиты от таких угроз дает именно криптография.

Математические методы, используемые в криптографии, невозможно успешно освоить без знания таких алгебраических структур, как группы, кольца и поля. Поэтому знание и умение работать с этими объектами является необходимым условием для подготовки специалистов в области защиты информации.

В силу присущей методам криптографии специфики, большой интерес представляет множество целых чисел и различные алгебраические структуры на его базе. Поэтому основное внимание будет уделено работе с целыми числами.

Математическая криптография возникла как наука о шифровании информации, т.е. как наука о криптосистемах. Большое влияние на развитие криптографии оказали появившиеся в середине двадцатого века работы американского математика Клода Шеннона. В классической шенноновской модели системы секретной связи имеют место два полностью доверяющих друг-другу участника, которым необходимо передавать между собой информацию, не предназначенную для третьих лиц. Такая информация называется конфиденциальной или секретной. Отсюда возникает задача обеспечения конфиденциальности, т.е. защита секретной информации от противника. Эта задача, по крайней мере исторически, – первая задача криптографии. Она традиционно решается с помощью криптосистем.

При обмене информацией между участниками часто возникает ситуация, когда информация не является конфиденциальной, но важен факт поступления сообщений в неискаженном виде, т.е. наличие гарантии, что

никто не сумеет подделать сообщение. Такая гарантия называется обеспечением целостности информации и составляет вторую задачу криптографии.

Для предотвращения угрозы контроля за источниками информации (откуда пересылаются сообщения) необходима система контроля за доступом к ресурсам, которая должна удовлетворять двум, казалось бы, взаимно исключающим требованиям. Во – первых, всякий желающий должен иметь возможность обратиться к этой системе анонимно, а во – вторых, при этом все же доказать свое право на доступ к ресурсам. Примером могут служить бумажные купюры. Если ресурсом является некоторый товар, то наличие у покупателя достаточного количества купюр является доказательством его права на доступ к ресурсу. С другой стороны, хотя каждая бумажная купюра и имеет уникальный номер, отслеживать купюры по номерам практически невозможно, т.е. нельзя определить, кто ее использовал и в каких платежах. Аналог этого свойства в криптографии называется неотслеживаемостью. Обеспечение неотслеживаемости – третья задача криптографии.

Если задача обеспечения конфиденциальности решается с помощью криптосистем, то для обеспечения целостности и неотслеживаемости разрабатываются криптографические протоколы.

В первой части кратко рассмотрена история криптографии и её основные понятия. Приведены основные классические шифры, такие как, шифр Цезаря, маршрутная транспозиция, таблица Виженера, одноразовый блокнот и т.д.

Во второй части введены базовые определения и понятия теории множеств, такие как "отображение" и "бинарные отношения", представлена основная теорема арифметики, наибольший общий делитель и т.д..

В третьей части определены и рассмотрены основные алгебраические структуры используемые в криптографии. Это такие множества как группы, кольца, поля. Определены понятия гомоморфизмов, изоморфизмов и автоморфизмов. Введено кольцо классов вычетов. Определены правила отображений из одного кольца в другое. Рассмотрены поля Галуа.

В четвертой части изучаются основные свойства диофантова уравнения и методы его решения.

В пятой части представлены основные положения шифрования с секретным ключом. Рассмотрены подстановки, перестановки, блочные и потоковые шифры, система Виженера и т.д. т.п.

В шестой части рассмотрены основные положения асимметричного шифрования. Рассмотрены криптосистемы на базе алгоритмов Диффи-Хелмана, Эль-Гамаля, RSA, эллиптических кривых и т.д. и т.п.

В седьмой части рассмотрены основные положения криптографического протоколов аутентификации и "электронной подписи".

В восьмой части кратко рассмотрено использование криптографических алгоритмов для защиты программного обеспечения. Дан анализ их применения в некоторых программных продуктах.

Каждая часть сопровождается соответствующими примерами.

1. КЛАССИЧЕСКИЕ ШИФРЫ И ОСНОВНЫЕ ПОНЯТИЯ

1.1. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ТЕРМИНОЛОГИЯ

Проблемами защиты информации путем ее преобразования занимается *криптология* (kryptos - тайный, logos - наука). Криптология разделяется на два направления - *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов криптоанализа - исследование возможности расшифровывания информации без знания ключей.

В этой книге основное внимание будет уделено криптографическим методам.

Современная криптография включает в себя четыре основных направления:

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами.

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей *шифрованию* и *дешифрованию,* будут рассматриваться *тексты*, построенные на некотором *алфавите*. Под этими терминами понимается следующее.

Алфавит - конечное множество используемых для кодирования информации знаков.

Текст - упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных информационных системах (ИС) можно привести следующие:

- алфавит Z_{33} - 32 буквы русского алфавита и пробел;
- алфавит Z_{44} – 43 буквы русского алфавита, знаки препинания и пробела;
- алфавит Z_{256} – символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит – $Z_2 = \{0,1\}$;
- восьмеричный алфавит – $Z_8 = \{0,1,2,3,4,5,6,7\}$;
- шестнадцатеричный алфавит – $Z_{16} = \{0,1,2,3,4,5,6,7,8,9,10,11, 12,13, 14, 5\}$;
- и т.д.и т.п.

Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом (называемый также криптограммой) (рис.1).

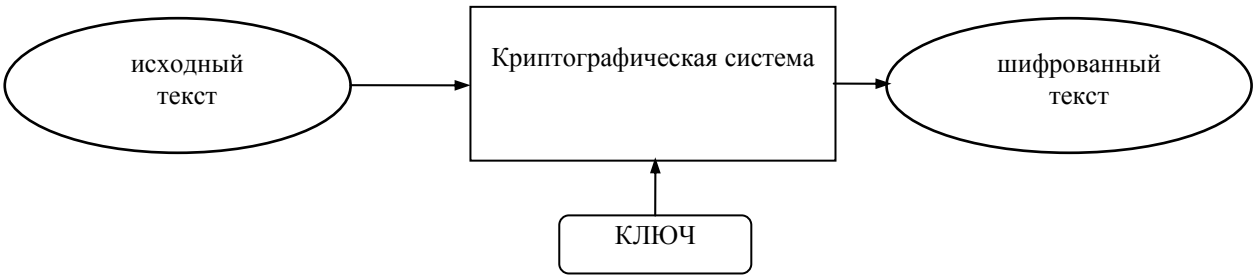

Рис.1. Процесс шифрования данных

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный (рис.2).

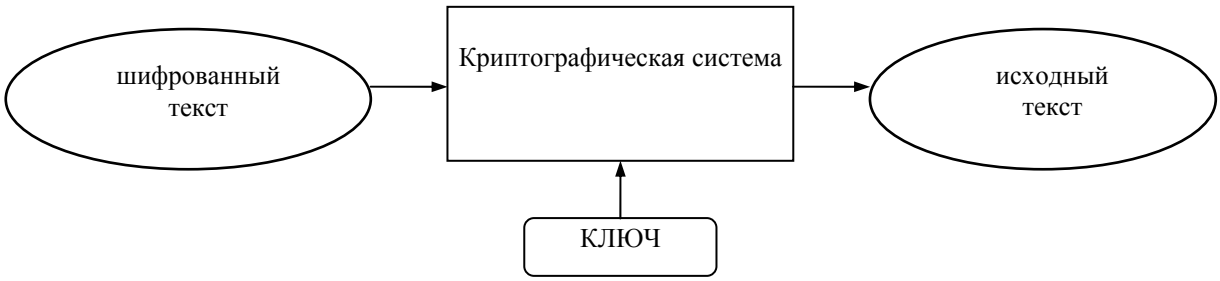

Рис.2. Процесс дешифрования данных

Ключ - информация, необходимая для шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство **T** преобразований открытого текста. Члены этого семейства индексируются, или обозначаются каким-нибудь символом, например ***k***. Параметр ***k*** является ключом. Пространство ключей ***K*** - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита. Цель криптографической системы заключается в том, чтобы зашифровать осмысленный исходный текст, получив в результате совершенно бессмысленный на взгляд шифрованный текст. Получатель, которому он предназначен, должен быть способен расшифровать эту шифрограмму, восстановив, таким образом, соответствующий ей открытый текст. При этом противник (называемый также криптоаналитиком) должен быть неспособен раскрыть исходный текст. Существует важное отличие между дешифрованием и раскрытием криптосистемы. Раскрытием криптосистемы назы-

вается результат работы криптоаналитика, приводящий к возможности эффективного раскрытия любого, зашифрованного с помощью данной криптосистемы, открытого текста. Степень неспособности криптосистемы к раскрытию называется ее *стойкостью* (*криптостойкостью*), или другими словами криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Таким образом, преобразование $\mathbf{T}_k$ определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Существуют несколько способов, в соответствии с которыми могут классифицироваться криптографические системы. Например, существует такая классификация:

- криптосистемы ограниченного использования;
- криптосистемы общего использования;
- криптосистемы с секретным ключом;
- криптосистемы с открытым ключом.

Криптографическая система называется криптосистемой *ограниченного использования*, если ее стойкость основывается на сохранении в секрете самого характера алгоритмов шифрования и дешифрования. Простейшим историческим примером такой системы можно считать шифр Цезаря, который будет рассмотрен далее. Криптосистемы ограниченного использования обычно разрабатываются любителями и почти всегда являются детской забавой для опытного криптоаналитика-профессионала. Гораздо важнее то, что такие системы вообще не используются для конфиденциальной связи в современной ситуации, когда должна обеспечиваться работа большого числа абонентов.

Криптографическая система называется криптосистемой *общего использования*, если ее стойкость основывается не на секретности алгоритмов шифрования и дешифрования, а на секретности ее ключа. Ключ должен легко вырабатываться конкретными пользователями при помощи их собственных ключей таким образом, чтобы даже разработчик криптосистемы не мог раскрыть ее, не имея доступа к тому ключу, который в ней в действительности использовался. Для некоторых применений (главным образом в военных, дипломатических и разведывательных ведомствах) для разработчика общей криптосистемы нет никаких причин для того, чтобы открытым образом описывать характер ее алгоритмов. Сохраняя эту информацию в тайне, можно обеспечить даже некоторую дополнительную безопасность. Однако, решающим обстоятельством, позволяющим полагаться на такую секретность, это не является, поскольку ничего нельзя сказать о том, когда она может быть скомпрометирована. По этой

причине, исследования надежности таких систем всегда должны проводиться в предположении, что потенциальному противнику о криптосистеме известно все, за исключением реально используемого секретного ключа. А если на самом деле противник такими знаниями не обладает, то это даже лучше. Для других типов применений, подобных, например, большим финансовым комплексам, в действительности лучше раскрывать, как работают их криптосистемы. В противном случае пользователи всегда будут предполагать возможность существования некоего секретного метода раскрытия такой криптосистемы.

Одним из требований обеспечения стойкости общей криптографической системы является огромное количество возможных ключей, не позволяющее провести исчерпывающий поиск (при котором осуществляется попытка систематического дешифровывания заданной криптограммы, используя при этом каждый из возможных ключей до тех пор, пока не получится некий осмысленный открытый текст). Однако необходимо знать, что большое число ключей само по себе стойкости криптосистемы не обеспечивает.

Общая криптографическая система называется *криптосистемой с секретным ключом*, если в ней любые две стороны, перед тем, как связаться друг с другом, должны заранее договориться между собой об использовании в дальнейшем некоторой секретной части информации, которая и называется *секретным ключом*. Такой механизм секретного распределения ключей мог эффективно работать в прошлом, то есть в ситуации, когда криптография использовалась небольшим числом пользователей. В настоящее время, когда криптография стала общедоступной, было бы неразумно организовывать такую сеть, в которой каждой паре потенциальных пользователей заранее предоставлялся бы их совместный секретный ключ, потому что тогда число таких ключей возрастало бы лавинообразно с увеличением числа пользователей.

В 1976 году Уитфрид Диффи (Diffie) и Мартин Хеллман (Hellman) заложили основы для преодоления этой трудности, предложив понятие криптографии с *открытым ключом*. Сходное понятие было независимо открыто Ральфом Мерклем (Merkle). Вскоре последовала его первая практическая реализация, предложенная Рональдом Ривестом (Rivest), Эди Шамиром (Shamir) и Леонардом Адлеманом (Adleman). Секретная связь по незащищенным каналам связи между двумя совершенно незнакомыми друг с другом сторонами наконец-то стала возможна.

Основное наблюдение, которое, собственно, и привело к криптографии с открытым ключом, заключалось в следующем – тот, кто зашифровывает сообщение, не обязательно должен быть способен его расшифровывать. В таких системах каждый пользователь выбирает свой собственный секретный ключ, на основании которого получает пару алгоритмов. Затем он делает один из них доступным каждому из возможных пользователей, объявляя этот алгоритм своим открытым алгоритмом

шифрования, в то время как другой, соответствующий первому и являющийся его личным алгоритмом дешифрования, хранит в строгом секрете.

Само собой разумеется, что такие системы могут быть стойкими, только если по свойствам общедоступного алгоритма шифрования невозможно "вычислить" или подобрать соответствующий ему алгоритм дешифрования.

Термины *распределение ключей* и *управление ключами* относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

1.2. ИЗ ИСТОРИИ КРИПТОГРАФИИ

Потребность шифровать и передавать шифрованные сообщения возникла очень давно. Так, еще в V-IV вв. до н. э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли *скиталами*. Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полосу папируса, наматывали ее на свою скиталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки отправляли адресату. Так как буквы на ней разбросаны в беспорядке, то прочитать написанное можно только при помощи соответствующей скиталы, намотав на нее без пропусков полосу папируса.

Аристотелю принадлежит способ дешифрования этого шифра. Надо изготовить длинный конус и, начиная с основания, обертывать его лентой с шифрованным сообщением, постепенно сдвигая ее к вершине. В какой-то момент начнут просматриваться куски сообщения. Так можно определить диаметр скиталы.

Были и другие способы защиты информации, разработанные в античные времена. Напрмер, древнегреческий полководец Эней Тактика в IV веке до н.э. предложил устройство, названное впоследствии "диском Энея". Принцип его таков. На диске диаметром 10-15 см и толщиной 1-2 см высверливались отверстия по числу букв алфавита. В центре диска помещалась "катушка" с намотанной на ней ниткой достаточной длины. При зашифровании нитка "вытягивалась" с катушки и последовательно протягивалась через отверстия, в соответствии с буквами шифруемого текста. Диск и являлся посланием. Получатель послания последовательно

вытягивал нитку из отверстий, что позволяло ему получать передаваемое сообщение, но в обратном порядке следования букв. При перехвате диска недоброжелатель имел возможность прочитать сообщение тем же образом, что и получатель. Но Эней предусмотрел возможность легкого уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть "катушку" с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий диска.

Сам термин “шифр” арабского происхождения. В начале XV в. арабы опубликовали энциклопедию “Шауба Аль-Аща”, в которой есть специальный раздел о шифрах. В этой энциклопедии указан способ раскрытия шифра простой замены. Он основан на различной частоте повторяемости букв в тексте. В этом разделе есть перечень букв в порядке их повторяемости на основе изучения текста Корана. Заметим, что в русском тексте чаще всего встречается буква “О”, затем буква “Е” и на третьем месте стоят буквы “И” и “А”. Более точно: на 1000 букв русского текста в среднем приходится 90 букв “О”, 72 буквы “Е” или “Ё”, 60 букв “И” и “А” и т.д.

В Древней Греции идея Энея была использована при создании и других оригинальных шифров замены. Например, в одном из вариантов вместо диска использовалась линейка с числом отверстий, равных количеству букв алфавита. Каждое отверстие обозначалось своей буквой; буквы по отверстиям располагались в произвольном порядке. К линейке была прикреплена катушка с намотанной на нее ниткой. Рядом с катушкой имелась прорезь. При шифровании нить протягивалась через прорезь, а затем через отверстие, соответствующее первой букве шифруемого текста, при этом на нити завязывался узелок в месте прохождения ее через отверстие; затем нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и т.д. После окончания шифрования нить извлекалась и передавалась получателю сообщения. Тот, имея идентичную линейку, протягивал нить через прорезь до отверстий, определяемых узлами, и восстанавливал исходный текст по буквам отверстий.

Это устройство получило название "линейка Энея". Шифр, реализуемый линейкой Энея, является одним из примеров шифра замены: буквы заменяются на расстояния между узелками с учетом прохождения через прорезь. Ключом шифра являлся порядок расположения букв по отверстиям в линейке. Противник, завладевший нитью (даже имея линейку, но без нанесенных на ней букв), не сможет прочитать сообщение.

Аналогичное "линейке Энея" "узелковое письмо" получило распространение у индейцев Центральной Америки. Свои сообщения они также передавали в виде нитки, на которой завязывались разноцветные узелки, определявшие содержание сообщения.

Заметным вкладом Энея в криптографию является предложенный им так называемый книжный шифр, описанный в сочинении "Об обороне укрепленных мест". Эней предложил прокалывать малозаметные дырки в книге или в другом документе над буквами (или под ними) секретного со-

общения. Интересно отметить, что в первой мировой войне германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые симпатическими чернилами на буквы газетного текста. Книжный шифр в современном его виде имеет несколько иной вид. Суть этого шифра состоит в замене букв на номер строки и номер этой буквы в строке и заранее оговоренной странице некоторой книги. Ключом такого шифра является книга и используемая страница в ней. Этот шифр оказался "долгожителем" и применялся даже во времена второй мировой войны.

В Древней Греции (II в. до н. э.) был также известен шифр, называемый *квадрат Полибия*. Это устройство представляло собой квадрат 5 х 5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку этого квадрата записывалась одна буква. (В греческом варианте одна клетка оставалась пустой, в латинском – в одну клетку помещали две буквы ***i*** и ***j***.) В результате каждой букве отвечала пара чисел и шифрованное сообщение превращалось в последовательность пар чисел.

Пример 1. 13 34 22 24 44 34 15 42 22 34 43 45 32

Это сообщение записано при использовании латинского варианта квадрата Полибия, в котором буквы расположены в алфавитном порядке.
("Cogito, ergo sum" – лат, "Я мыслю, следовательно существую"). ♦

Интересно отметить, что в несколько измененном виде шифр Полибия дошел до наших дней и получил своеобразное название "тюремный шифр". Для его использования нужно только знать естественный порядок расположения букв алфавита (как в указанном выше примере для английского языка). Стороны квадрата обозначаются не буквами (ABCDE), а числами (12345). Число 3, например, передается путем тройного стука. При передаче буквы сначала "отстукивается число, соответствующее строке, в которой находится буква, а затем номер соответствующего столбца. Например, буква "F" передается двойным стуком (вторая строка) и затем одинарным (первый столбец).

С применением этого шифра связаны некоторые исторические казусы. Так, декабристы, посаженные в тюрьму после неудавшегося восстания, не смогли установить связь с находившимся в "одиночке" князем Одоевским. Оказалось, что этот князь (хорошо образованный по тем временам) не помнил естественный порядок расположения букв в русском и французском алфавитах (другими языками он не владел). Декабристы для русского алфавита использовали прямоугольник размера 5х6 (5 строк и 6 столбцов) и редуцированный до 30 букв алфавит.

Тюремный шифр", строго говоря, не шифр, а способ перекодировки сообщения с целью его приведения к виду, удобному для передачи по каналу связи (через стенку). Дело в том, что в таблице использовался естественный порядок расположения букв алфавита. Отметим, что при произвольном расположении букв в квадрате возникает одно затруднение: либо нужно помнить отправителю и получателю сообщения заданный произвольный порядок следования букв в таблице (ключ шифра), что во-

обще говоря затруднительно, либо иметь при себе запись этих букв. Во втором случае появляется опасность ознакомления с ключом посторонних лиц.

В 1 в. н.э. Ю. Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на третью:

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

Пример 2. Донесение Ю. Цезаря Сенату об одержанной им победе над Понтийским царем выглядело так:

YHQL YLGL YLFL("Veni, vidi, vici" – лат. "Пришел, увидел, победил") .♦

Император Август (1 в. н. э.) в своей переписке заменял первую букву на вторую, вторую – на третью и т. д. Последнюю – на первую:

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

Пример 3. Любимое изречение императора Августа выглядело так:

GFTUJOB MFOUF ("Festina lente" – лат. "Торопись медленно") .♦

Квадрат Полибия, шифр Цезаря входят в класс шифров, называемых *подстановка* или *простая замена*, т.е. это шифры, в которых каждой букве алфавита соответствует буква, цифра, символ или какая-нибудь их комбинация.

В известных рассказах “Пляшущие человечки” Конан Дойля и “Золотой жук” Эдгара По используемые шифры относятся к указанному классу шифров. В другом классе шифров – *перестановка* – буквы сообщения каким-нибудь способом переставляются между собой. К этому классу принадлежит шифр скитала.

Неудобство шифров типа подстановка (простая замена) в случае использования стандартного алфавита очевидно. Таблица частот встречаемости букв алфавита позволяет определить одни или несколько символов, а этого иногда достаточно для дешифрования всего сообщения (“Пляшущие человечки” Конан Дойля или “Золотой жук” Эдгара По). Поэтому обычно пользуются разными приемами, чтобы затруднить дешифрование. Для этой цели используют *многобуквенную систему шифрования* – систему, в которой одному символу отвечают одна или несколько комбинаций двух и более символов. Другой прием – использование нескольких алфавитов. В этом случае для каждого символа употребляют тот или иной алфавит в зависимости от ключа, который связан каким-нибудь способом с самим символом или с его порядком в передаваемом сообщении.

1.3. МАРШРУТНАЯ ТРАНСПОЗИЦИЯ

К классу перестановка относится шифр *маршрутная транспозиция* и его вариант *постолбцовая транспозиция*. В каждом из них в данный прямоугольник [$n \times m$] сообщение вписывается заранее обусловленным способом, а столбцы нумеруются или обычным порядком следования, или в порядке следования букв ключа – буквенного ключевого слова.

Пример 4. Зашифруем фразу “Дела давно минувших дней, преданья старины глубокой”, используя для этого два прямоугольника 6×8. В первом прямоугольнике столбцы нумеруются в обычном порядке следования – слева направо, а во втором – в порядке следования букв слова “Пушкин”. Используя расположение букв этого ключа в алфавите, получим набор чисел [4 5 6 2 1 3]:

1	2	3	4	5	6
д	е	л	а	д	а
в	н	о	м	и	н
у	в	ш	и	х	д
н	е	й	п	р	е
д	а	н	ь	я	с
т	а	р	и	н	ы
г	л	у	б	о	к
о	й	а	б	в	г

4	5	6	2	1	3
д	е	л	а	д	а
в	н	о	м	и	н
у	в	ш	и	х	д
н	е	й	п	р	е
д	а	н	ь	я	с
т	а	р	и	н	ы
г	л	у	б	о	к
о	й	а	б	в	г

В первом случае получим шифрованный текст, если будем выписывать буквы очередного столбца в порядке следования столбцов (прямом или обратном), во втором, – если будем выписывать буквы столбца в порядке следования букв ключа. Таким образом, будем иметь:

1) двундтго енвеаалй лошйнруа амипьибб дихрянов андесыкг;

2) дихрянов амипьибб андесыкг двундтго енвеаалй лошйнруа. ♦

1.4. ТАБЛИЦА ВИЖЕНЕРА

В процессе шифрования (и дешифрования) иногда используется *таблица Виженера*, которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу букв в алфавите. Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом. Выбирается слово – лозунг и подписывается с повторением над буквами сообщения.

Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном.

Пример 5. Таблица 1, составлена из 31 буквы русского алфавита (без букв Ё и Ъ).

таблица 1

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю

Выбираем лозунг – математика. Находим столбец, отвечающий букве "м" лозунга, а затем строку, соответствующую букве "к". На пересечении выделенных столбца и строки находим букву "ц". Так продолжая дальше, получаем весь шифрованный текст.

м а т е м а т и к а м а т е м а т и к а м а т е м а

к р и п т о г р а ф и я с е р ь е з н а я н а у к а

ц р ь ф я о х ш к ф ф я д к э ь ч п ч а л н т ш ц а ♦

К сообщению можно применять несколько систем шифрования.

1.5. МОДИФИЦИРОВАННЫЙ ШИФР ЦЕЗАРЯ

Аббат Тритемеус – автор первой печатной книги о тайнописи (1518г.) – предложил несколько шифров и среди них шифр, который можно считать усовершенствованием шифра Цезаря. Этот шифр устроен так. Все буквы алфавита нумеруются по порядку (от 1 до 31 в русском варианте). Затем выбирают какое-нибудь слово, называемое "ключом", и подписывают под сообщением с повторением.

Чтобы получить шифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 31, то из нее вычитают 31. В результате получают последо-

вательность чисел от 1 до 31. Вновь заменяя числа этой последовательности соответствующими буквами, получают шифрованный текст. Разбиваем этот текст на группы одной длины, получают шифрованное сообщение.

Пример 6. Выбираем ключевое слово "Пособие". Составляем сообщение "сессия начинается в конце семестра"

с е с с и я н а ч и н а е т с я в к о н ц е с е м е с т р а
п о с о б и е п о с о б и е п о с о б и е п о с о б и е п о

Шифруем, разбиваем текст на группы длины 6, и получаем шифрованное сообщение:

в ф д а и и у р з ь э в о ш в о ф щ р ц э х б ч ы з ь ш б п ♦

Чтобы получить шифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 33, то из нее вычитают 33. В результате получают последовательность чисел от 1 до 33. Вновь заменяя числа этой последовательности соответствующими буквами, получают шифрованный текст. Разбивал этот текст на группы одной длины (например, по 5*),* получают шифрованное сообщение.

Если под ключом шифра понимать однобуквенное слово “В” (в русском варианте), то мы получим шифр Цезаря.

Пример 7. Для сообщения из примера 6, получим:

ф и ф ф л в р г ь л р г и х ф в в н т р щ и ф и п и ф х у г ♦

1.6. ОДНОРАЗОВЫЙ БЛОКНОТ

Почти все используемые на практике шифры характеризуются как условно надежные, поскольку они могут быть раскрыты в принципе при наличии неограниченных вычислительных возможностей. Абсолютно надежные шифры нельзя разрушить даже при наличии неограниченных вычислительных возможностей. Доказательство существования и единственности абсолютно надежного шифра получил К.Шеннон с помощью разработанного им теоретико-информационного метода исследования шифров. Таким образом, единственный абсолютно надежный шифр, который используется на практике, это так называемый *одноразовый блокнот*, в основе которого лежит та же идея, что и шифре Цезаря. Рассмотрим его основную идею.

Занумеровав все символы расширенного алфавита Z_{44} числами от 0 до 43, можно рассматривать любой передавамый текст, как последовательность $\{a_n\}$ чисел множества $\mathbf{A}=\{\mathbf{0,1,2,\ldots,43}\}$. Имея случайную последовательность $\{c_n\}$ из чисел множества **A** той же длины что и передаваемый текст (ключ), складываем по модулю[1] 44 число a_n передаваемого текста с соответствующим числом c_n ключа

$$a_n+c_n \equiv b_n (\mathbf{mod}\ 44),\ 0 \le b_n \le 43,$$

[1] Операции сложения и вычитания по модулю будут определены в главе 3

получим последовательность $\{b_n\}$ знаков шифрованного текста.

Чтобы получить передаваемый текст, можно воспользоваться тем же ключом:

$$a_n \equiv b_n - c_n (\mathbf{mod}\ 44),\ 0 \le a_n \le 43.$$

У двух абонентов, находящихся в секретной переписке, имеются два одинаковых блокнота, составленных из отрывных страниц, на каждой из которых напечатана таблица со случайными числами или буквами, т.е. случайная последовательность чисел из множества **A**. Таблица имеет только две копии: одна используется отправителем, другая – получателем. Отправитель свой текст шифрует указанным выше способом при помощи первой страницы блокнота. Зашифровав сообщение и отправив его второму абоненту, он уничтожает использованную страницу. Получатель шифрованного текста расшифровывает его и также уничтожает использованный лист блокнота. Нетрудно видеть, что одноразовый шифр нераскрываем в принципе, так как символ в тексте может быть заменен любым другим символом и этот выбор совершенно случаен.

2. МНОЖЕСТВА И ОТОБРАЖЕНИЯ

2.1. МНОЖЕСТВА

Математическое понятие *множество* является одним из центральных во всей математике. Оно определяется в зависимости от задач. Примером может служить группа аксиом, известная как система NGB (по имени авторов – Джона фон Нейман, Поля Бернайса, Курта Геделя). Главная идея, положенная в основу NGB, заключается в различении понятий множества и класса. Все объекты NGB являются классами. Класс соответствует нашему интуитивному пониманию совокупности. Множеством являются те классы, которые являются элементами других классов. Классы, не являющиеся множествами, называются *собственными классами*.

Существует другая группа аксиом – система ZF (по имени авторов – Эрнста Цермело и Абрахама Френкеля). Это теория *построимых множеств*, т.е. множество строится из некоторых простых элементов, с помощью таких операций, как пересечение, объединение, дополнение и т.д.

Мы будем понимать под множеством любую совокупность объектов, называемых *элементами* множества. Множества с конечным числом различных элементов могут быть описаны путем явного перечисления всех элементов. Обычно эти элементы заключаются в фигурные скобки. Например, {16,32,64} – множество степеней двойки, заключенных между 10 и 100. Множество обозначается прописной буквой какого-либо алфавита, а его элементы – строчными буквами того же или другого алфавита. Для некоторых особо важных множеств приняты стандартные обозначения, которых следует придерживаться. Так, буквами **N, Z, Q, R** обозначают соответственно множество натуральных чисел, множество целых чисел, множество рациональных чисел и множество вещественных чисел. При заданном множестве **S** *включение* $\mathbf{a}\in\mathbf{S}$ указывает на то, что **a** – элемент множества. В противном случае записывают $\mathbf{a}\notin\mathbf{S}$. Говорят, что **S** – *подмножество* **T** или $\mathbf{S}\subset\mathbf{T}$ (**S** содержится в **T**), когда имеет место импликация:

$$\mathbf{x}\in\mathbf{S},\ \forall\mathbf{x} \Rightarrow \mathbf{x}\in\mathbf{T}.$$

Два множества совпадают (или равны), если у них одни и те же элементы. Символически это записывается в виде:

$$\mathbf{S}=\mathbf{T} \Leftrightarrow \mathbf{S}\subset\mathbf{T} \text{ и } \mathbf{T}\subset\mathbf{S}.$$

Пустое множество $\varnothing$, т.е. множество, не содержащее ни одного элемента, по определению входит в число подмножеств любого множества.

Под *пересечением* двух множеств **S** и **T** понимают множество

$$\mathbf{S}\cap\mathbf{T}=\{\mathbf{x}|\ \mathbf{x}\in\mathbf{S} \text{ и } \mathbf{x}\in\mathbf{T}\},$$

а под их объединением – множество

$$\mathbf{S}\cup\mathbf{T}=\{\mathbf{x}|\ \mathbf{x}\in\mathbf{S} \text{ или } \mathbf{x}\in\mathbf{T}\}.$$

Пусть **X** и **Y** – произвольные множества. Пару (x,y) элементов $\mathbf{x\in X,\ y\in Y}$, взятых в данном порядке, называют *упорядоченной парой*, считая при этом, что $(x_1,y_1)=(x_2,y_2)$ тогда и только тогда, когда $x_1=x_2$, $y_1=y_2$. *Декартовым произведением* двух множеств **X** и **Y** называется множество всех упорядоченных пар (x,y):

$$\mathbf{X\times Y=\{(x,y)|x\in X,\ y\in Y\}}.$$

Пример 8. Пусть, **R** – множество всех вещественных чисел. Тогда декартов квадрат $\mathbf{R^2=R\times R}$ есть просто множество всех декартовых координат на плоскости относительно заданных координатных осей. ♦

Аналогично можно ввести декартово произведение трех, четырех и т.д. множеств. При $\mathbf{X_1=X_2=X_3=\ldots=X_k=X}$ сокращенно пишут $\mathbf{X^k}$ и говорят о k-й декартовой степени множества **X**. Элементами $\mathbf{X^k}$ являются последовательности, или строки $(x_1,x_2,\ldots x_k)$ длины k.

2.2. ОТОБРАЖЕНИЯ

Понятие *отображения* или *функции* также является одним из центральных в математике. При заданных **X** и **Y** отображение **f** с *областью определения* **X** и *областью значений* **Y** сопоставляет каждому элементу $\mathbf{x\in X}$ элемент $\mathbf{f(x)\in Y}$. Символически отображение записывается в виде $\mathbf{f:X\to Y}$. *Образом* при отображении **f** называется множество всех элементов вида **f(x)**:

$$\mathrm{Im}\ \mathbf{f=\{f(x)|x\in X\}=f(X)\subset Y}.$$

Множество

$$\mathbf{f^{-1}(y)=\{x\in X|f(x)=y\}}$$

называется *прообразом* элемента $\mathbf{y\in Y}$.

Отображение $\mathbf{f:X\to Y}$ называется *сюръективным,* или *отображением на*, когда Im $\mathbf{f=Y}$.

Отображение $\mathbf{f:X\to Y}$ называется *инъективным,* когда из $\mathbf{x\neq x'}$ следует $\mathbf{f(x)\neq f(x')}$.

Отображение $\mathbf{f:X\to Y}$ называется *биективным,* или взаимно однозначным, если оно одновременно сюръективно и инъективно.

Равенство **f=g** двух отображений означает по определению, что их соответствующие области совпадают.

Пример 9. Пусть $\mathbf{R_+}$ – множество положительных вещественных чисел. Тогда отображения $\mathbf{f:R\to R}$, $\mathbf{g:R\to R_+}$, $\mathbf{h:R_+\to R_+}$, определенные одним и тем же правилом $\mathbf{x\to x^2}$, все различны: **f** – ни сюръективно, ни инъективно, **g** – сюръективно, но не инъективно, а отображение **h** – биективно. Таким образом, задание области определения и области значений – важная часть определения отображения. ♦

Единичным или *тождественным* отображением $\mathbf{e_X:X\to X}$ называется отображение, переводящее каждый элемент $\mathbf{x\in X}$ в себя.

Отображение $\mathbf{f^{-1}}$ является обратным к **f**, если $\mathbf{f(x)=y \Leftrightarrow f^{-1}(y)=x}$.

Пример 10. Найти обратное отображение $\mathbf{f^{-1}}$ для $\mathbf{f(x)}=\frac{1}{\sqrt{x-5}}$**.** Обратное отображение удовлетворяет условию $\mathbf{f(f^{-1}(x))=f^{-1}(f(x))=e_X=x}$. Следовательно, $\frac{1}{\sqrt{f^{-1}(x)-5}}=x$. $\Rightarrow 1=\mathbf{f^{-1}(x)}\cdot\mathbf{x^2}-5\mathbf{x^2}$; $\Rightarrow \mathbf{f^{-1}(x)}=1/\mathbf{x^2}+5$.

Проверка.$\mathbf{f(f^{-1}(x))=f}(1/\mathbf{x^2}+5)=\frac{1}{\sqrt{1/x^2+5-5}}=\mathbf{x=f^{-1}(f(x))=f^{-1}}(\frac{1}{\sqrt{x-5}})=\frac{1}{\frac{1}{x-5}}+5$ ♦

2.3. БИНАРНЫЕ ОТНОШЕНИЯ

Для любых двух множеств **X** и **Y** всякое подмножество $\mathbf{O\subset X\times Y}$ называется *бинарным отношением* между **X** и **Y** (или просто на **X**, если **X=Y**).

Бинарное отношение ~ на **X** называется отношением эквивалентности, если для всех **x**, $\mathbf{x_1}$, $\mathbf{x_2\in X}$ выполнены условия:

i. $\mathbf{x\sim x}$ (рефлексивность);
ii. $\mathbf{x\sim x_1 \Rightarrow x_1\sim x}$ (симметричность);
iii. $\mathbf{x\sim x_1}$, $\mathbf{x_1\sim x_2 \Rightarrow x_2\sim x}$ (транзитивность).

Подмножество

$$\mathbf{H=\{x'\in X|x'\sim x\}\subset X}$$

всех элементов, эквивалентных данному **x**, называется классом эквивалентности, содержащим **x**.

Так как $\mathbf{x\sim x}$ (условие i), то $\mathbf{x'\in H}$. Любой элемент $\mathbf{x'\in H}$ называется *представителем класса* **H**.

Справедливо следующая теорема.

Теорема 1. Множество классов эквивалентности по отношению ~ является разбиением множества **X** в том смысле, что **X** является объединением непересекающихся подмножеств.

Доказательство. В самом деле, так как $\mathbf{x\in H}$, то $\mathbf{X=\cup H_i}$. Далее, класс **H** однозначно определяется любым своим представителем, т.е. $\mathbf{H_i=H_j \Leftrightarrow\ x_i\sim x_j}$. В одну сторону: $\mathbf{x_i\sim x_j}$ и $\mathbf{x\in H_i \Rightarrow x\sim x_i \Rightarrow x\sim x_j \Rightarrow x\in H_j \Rightarrow H_i\subset H_j}$. Но $\mathbf{x_i\sim x_j \Rightarrow x_j\sim x_i}$ (условие ii). Поэтому выполнено и обратное включение $\mathbf{H_j\subset H_i}$. Значит $\mathbf{H_j=H_i}$. В другую сторону: так как $\mathbf{x\in H,}$ то $\mathbf{H_i=H \Rightarrow x\in H_i \Rightarrow x\sim x_i}$.

Если теперь $\mathbf{H_j\cap H_i\neq\varnothing}$ и $\mathbf{x\in H_j\cap H_i}$, то $\mathbf{x\sim x_i}$ и $\mathbf{x\sim x_j}$, откуда в силу транзитивности (условие iii) имеем $\mathbf{x_i\sim x_j}$ и $\mathbf{H_j=H_i}$. Значит, различные классы не пересекаются. Теорема доказана. ♦

Пример 11. Пусть $\mathbf{V=R^2}$ – вещественная плоскость с прямоугольной системой координат. Тогда, взяв за свойство ~ принадлежность

точек **P**, **P'**$\in$**V** одной горизонтальной прямой, получим отношение эквивалентности с классами – горизонтальными прямыми (рис. 3).

Гиперболы Γ_p (рис. 4) вида $xy=p>0$ определяют отношение эквивалентности в области $V_+ \subset V$ точек $P(x,y)$ с координатами $x>0$, $y>0$.

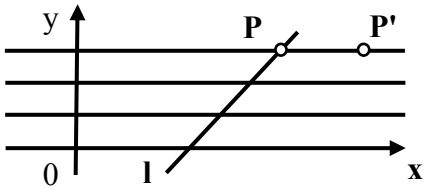

Рис. 3.

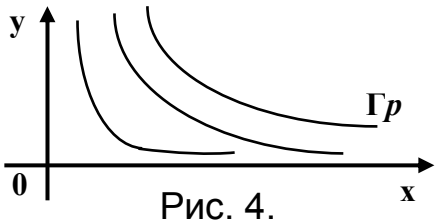

Рис. 4.

2.4. ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

Целое число s называется *делителем* (или *множителем*) целого числа n, если $n=st$ для некоторого $t\in\mathbf{Z}$. В свою очередь n называется *кратным* s. Делимость n на s обозначается символом |. Делимость – транзитивное свойство (смотри 2.3, свойство iii) на $\mathbf{Z}$. Целое число p, делители которого исчерпываются числами $\pm p$, ± 1 (*несобственные делители*), называется *простым*. Обычно в качестве простых берутся положительные простые числа > 1.

Фундаментальную роль простых чисел вскрывает так называемая основная теорема арифметики.

Теорема 2. Каждое положительное целое число $n\neq 1$ может быть записано в виде произведения простых чисел: $n=p_1p_2p_3\ldots p_S$. Эта запись единственна с точностью до порядка сомножителей.(Без доказательства)♦

Собрав вместе одинаковые простые множители и изменив обозначения, получим запись n в виде: $n=p_1^{1}p_2^{2}p_3^{3}\ldots p_S^{S}$.

Теорема 3 (Евклида) гласит, что множество

$$\mathbf{P}=\{2,3,5,11,13,\ldots\}$$

всех простых чисел бесконечно. Действительно, если бы существовало бы лишь конечное число простых чисел, например $p_1p_2\ldots p_k$, то по основной теореме число $c=p_1p_2\ldots p_k+1$ делилось бы по крайней мере на одно из p_i. Без ограничения общности считаем $c=p_1c'$. Тогда $p_1(c'-p_2\ldots p_k)=1$, а это невозможно, поскольку делителями единицы в $\mathbf{Z}$ являются лишь ± 1, что и требовалось доказать. ♦

2.5. АЛГОРИТМ ДЕЛЕНИЯ В Z

При заданных $a,b\in\mathbf{Z}$, $b>0$, всегда найдутся $q,r\in\mathbf{Z}$ такие, что

$$a=bq+r,\quad 0\leq r<b$$

(если считать лишь $b\neq 0$, то будет выполнено неравенство $0\leq r<|b|$).

В самом деле, множество $\mathbf{S}=\{a-bs|s\in\mathbf{Z},a-bs\geq 0\}$, очевидно, не пусто (например, $a-b(-a^2)\geq 0$). Стало быть, **S** содержит наименьший элемент. Обозначим его $r=a-bq$. По условию $r\geq 0$. Предположив $r\geq b$, мы получили бы элемент $r-b=a-b(q+1)\in\mathbf{S}$, меньший, чем r. Это противоречие устраняется лишь при $r<b$.

Проведенное несложное рассуждение дает алгоритм для нахождения частного b и остатка r за конечное число шагов.

Алгоритм деления в $\mathbf{Z}$ можно также использовать для определения *наибольшего общего делителя* (НОД), известного из школьного курса математики. Именно, при заданных целых числах n, m, одновременно не равных нулю, положим

$$\mathbf{J}=\{nu+mv|u,v\in\mathbf{Z}\}.$$

Выберем в **J** наименьший положительный элемент $d=nu_0+mv_0$. Используя алгоритм деления, запишем $n=dq+r$, $0\leq r<d$. Ввиду выбора d включение

$$r=n-dq=n-(nu_0+mv_0)q=n(1-u_0q)+m(-v_0q)\in\mathbf{J}$$

влечет равенство $r=0$. Стало быть, $d|n$. Аналогично доказывается, что $d|m$.

Пусть теперь d' – любой делитель чисел n и m. Тогда

$$d'|n,\ d'|m\ \Rightarrow d'|nu_0,\ d'|mv_0\ \Rightarrow d'|(nu_0+mv_0)\ \Rightarrow d'|d.$$

Итак, d обладает всеми свойствами НОД, и поэтому $d=$НОД(n,m). Мы пришли к следующему утверждению.

Наибольший общий делитель двух целых чисел n,m, не равных одновременно нулю, всегда записывается в виде

$$\text{НОД}(n,m)=nu+mv;\ u,v\in\mathbf{Z}.$$

В частности, целые числа n,m взаимно просты тогда и только тогда, когда $nu+mv=1$ при некоторых $u,v\in\mathbf{Z}$.

Для доказательства этого утверждения нужно взять любой положительный элемент из множества **J**, а затем уменьшать его при помощи алгоритма деления до тех пор, пока не получится наименьший элемент, который и будет наибольшим общим делителем.

В дальнейшем нам понадобится так называемая *функция Эйлера* ($\varphi:\mathbf{N}\to\mathbf{N}$). Она определяется следующим образом. Если натуральное число n делится в точности на k различных простых чисел $p_1,p_2,\ldots p_k$, то количество чисел, меньших n и взаимно простых с n, равно

$$\varphi(n)=n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k).$$

Пример 12. $p_1=3$; $p_2=5$; $p_3=7$; $p_4=11$; $n=p_1p_2p_3,p_4,=1155$;

$\varphi(n)=1155(1-1/3)(1-1/5)(1-1/7)(1-1/11)=480$. ♦

3. МНОЖЕСТВА С АЛГЕБРАИЧЕСКИМИ ОПЕРАЦИЯМИ

3.1. БИНАРНЫЕ ОПЕРАЦИИ

Пусть **X** – произвольное множество. *Бинарной алгебраической операцией* (или *законом композиции*) на **X** называется произвольное (но фиксированное) отображение $\tau: X\times X\to X$ декартова квадрата $X^2=X\times X$ в **X**. Таким образом, любой упорядоченной паре (a,b) элементов $a,b\in X$ ставится в соответствие определенный элемент $\tau(a,b)$ того же множества **X**. Иногда вместо $\tau(a,b)$ пишут $a\tau b$, а еще чаще бинарную операцию на **X** обозначают каким-нибудь специальным символом: $*$, $\bullet$, $\cdot$ или $+$.

На **X** может быть задано, вообще говоря, много различных операций. Желая выделить одну из них, используют скобки $(X, *)$ и говорят, что операция $*$ определяет на **X** *алгебраическую структуру* или что $(X, *)$ – *алгебраическая система*.

Пример 13. В множестве **Z** целых чисел, помимо естественных операций $+$, $\cdot$ (сложения и умножения), легко указать получающиеся при помощи $+$ (или $-$) и $\cdot$ "производные" операции: $n\bullet m=n+m-nm$, $n*m=-n-m$ и т.д. Мы приходим к различным алгебраическим структурам $(Z,+),(Z,-)$, $(Z, \bullet)$ и $(Z, *)$. ♦

Наряду с бинарными алгебраическими операциями не лишены интереса гораздно более общие n-арные операции (унарные при $n=1$, тернарные при $n=3$ и т.д.), равно как и их комбинации. Связанные с ними алгебраические структуры составляют специальную теорию универсальных алгебр.

В направлении конструирования разных бинарных операций на множестве **X** также, очевидно, открывается неограниченный простор фантазии. Но задача изучения произвольных алгебраических структур слишком обща, чтобы она представляла реальную ценность. По этой причине ее рассматривают при различных естественных ограничениях.

3.2. ПОЛУГРУППЫ И МОНОИДЫ

Бинарная операция $*$ на множестве **X** называется *ассоциативной*, если $(a*b)*c=a*(b*c)$ всех $a,b,c\in X$. Она также называется *коммутативной*, если $a*b=b*a$. Те же названия присваиваются и соответствующей алгебраической структуре $(X,*)$. Требования ассоциативности и коммутативности независимы. В самом деле, операция $*$ на **Z**, заданная правилом $n*m=-n-m$, очевидно, коммутативна. Но $(1*2)*3=(-1-2)*3=-(-1-2)-3=0 \neq 1*(2*3)= 1*(-2-3)=-1-(-5)=4$. Так что условие ассоциативности не выполняется.

Элемент $e \in \mathbf{X}$ называется *единичным* (или *нейтральным*) относительно рассматриваемой бинарной операции $*$, если $e*x=x*e$ для всех $x \in \mathbf{X}$. Если e' – еще один единичный элемент, то, как следует из определения, $e'=e'*e=e*e'=e$. Следовательно, в алгебраической структуре $(\mathbf{X},*)$ может существовать не более одного единичного элемента.

Множество $\mathbf{X}$ с заданной на нем бинарной ассоциативной операций называется *полугруппой*. Полугруппу с единичным (нейтральным) элементом принято называть *моноидом*.

Элемент a моноида $(\mathbf{M},\cdot,e)$ называется *обратимым*, если найдется элемент $b \in \mathbf{M}$, для которого $a \cdot b = b \cdot a = e$ (понятно, что элемент b тоже обратим). Если еще и $a \cdot b' = e = b' \cdot a$, то $b' = e \cdot b' = (b \cdot a) \cdot b' = b \cdot (a \cdot b') = b \cdot e = b$. Это дает основание говорить просто об *обратном элементе* a^{-1} к (обратимому) элементу $a \in \mathbf{M}: a \cdot a^{-1} = e = a^{-1} \cdot a$. Разумеется, $(a^{-1})^{-1} = a$.

Пример 14. Пусть Ω – произвольное множество, $\mathbf{M}(\Omega)$ – множество всех отображений Ω в себя. Тогда $(\mathbf{M}(\Omega),\bullet,e_\Omega)$ – моноид, где $\bullet$ – естественная композиция отображений, а e_Ω – тождественное отображение. ♦

Пример 15. Пусть $\mathbf{M_n}(\mathbf{R})$ – множество квадратных матриц n×n с вещественными коэффициентами. Тогда $(\mathbf{M_n}(\mathbf{R}),*,\mathbf{E})$ – моноид, где $*$ – операция умножения матриц, $\mathbf{E}$ – единичная матрица n×n. ♦

Пример 16. Пусть $n\mathbf{Z}=\{nm \mid m \in \mathbf{Z}\}$ – множество целых чисел, делящихся на n. Тогда $(n\mathbf{Z},+,0)$ – коммутативный моноид, а $(n\mathbf{Z},\cdot)$ – коммутативная полугруппа без единицы ($n > 1$). ♦

3.3. ГРУППЫ. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Моноид $\mathbf{G}$, все элементы которого обратимы, называется *группой*. Другими словами, предполагается выполнение следующих аксиом:

($\mathbf{G}1$) на множестве $\mathbf{G}$ определена бинарная операция $*$;

($\mathbf{G}2$) операция $*$ ассоциативна: $(x*y)*z=x*(y*z)$ для всех $x,y,z \in \mathbf{G}$;

($\mathbf{G}3$) $\mathbf{G}$ обладает нейтральным (единичным) элементом e: $e*x=x*e$ для всех $x \in \mathbf{G}$;

($\mathbf{G}4$) для каждого элемента $x \in \mathbf{G}$ существует обратный $x^{-1}: x^{-1}*x = x*x^{-1}=e$.

Для обозначения числа элементов в группе $\mathbf{G}$ (точнее, мощности группы) используются равноправные символы Card$\mathbf{G}$, $|\mathbf{G}|$ и $(\mathbf{G}:e)$.

Пример 17. $\mathbf{GL}(n,\mathbf{R})$ – множество квадратных матриц n×n с вещественными коэффициентами с ненулевым определителем. Тогда $\mathbf{GL}(n,\mathbf{R})$ – группа по операции умножения матриц. Эта группа носит специальное название - полная линейная группа *степени* n над $\mathbf{R}$. ♦

Пример 18. Используя рациональные числа вместо вещественных, мы приходим к полной линейной группе $\mathbf{GL}(n,\mathbf{Q})$ степени n над $\mathbf{Q}$. ♦

Подмножество $\mathbf{H}\subset\mathbf{G}$ называется подгруппой **G**, если $\boldsymbol{e}\in\mathbf{H}$; $\boldsymbol{h}_1,\boldsymbol{h}_2\in\mathbf{H}\Rightarrow\boldsymbol{h}_1\boldsymbol{h}_2\in\mathbf{H}$ и $\boldsymbol{h}\in\mathbf{H}\Rightarrow\boldsymbol{h}^{-1}\in\mathbf{H}$. Подгруппа $\mathbf{H}\subset\mathbf{G}$ – собственная, если $\mathbf{H}\neq\boldsymbol{e}$ и $\mathbf{H}\neq\mathbf{G}$.

Пример 19. Рассмотрим в группе **GL**(n,**R**) подмножество **SL**(n,**R**) матриц с определителем, равным 1, т.е.:

$$\mathbf{SL}(\boldsymbol{n},\mathbf{R})=\{\mathbf{A}\in\mathbf{GL}(\boldsymbol{n},\mathbf{R})|\det\mathbf{A}=1\}.$$

Очевидно, что $\mathbf{E}\in\mathbf{SL}(\boldsymbol{n},\mathbf{R})$. Кроме того, $\det\mathbf{A}=1$, $\det\mathbf{B}=1\Rightarrow\det\mathbf{AB}=1$ и $\det\mathbf{A}^{-1}=1$. Поэтому $\mathbf{SL}(\boldsymbol{n},\mathbf{R})$ – подгруппа в $\mathbf{GL}(\boldsymbol{n},\mathbf{R})$. Она носит название *специальной линейной группы степени* $\boldsymbol{n}$ над **R**. Ее называют еще *унимодулярной*. ♦

Пример 20. Подгруппа $\mathbf{SL}(\boldsymbol{n},\mathbf{R})$ содержит подгруппу $\mathbf{SL}(\boldsymbol{n},\mathbf{Q})$, которая, в свою очередь, содержит интересную подгруппу $\mathbf{SL}(\boldsymbol{n},\mathbf{Z})$ целочисленных матриц с единичным определителем. ♦

Пример 21. Положим в примерах 17 и 18 $\boldsymbol{n}=1$. Тогда мы приходим к мультипликативным группам $\mathbf{R}^*=\mathbf{R}\backslash\{0\}=\mathbf{GL}(1,\mathbf{R})$ и $\mathbf{Q}^*=\mathbf{Q}\backslash\{0\}=\mathbf{GL}(1,\mathbf{Q})$ вещественных и рациональных чисел. Эти группы бесконечны. ♦

Пример 22. Так как в $(\mathbf{Z},*,1)$ обратимыми элементами являются только –1 и 1, то $\mathbf{GL}(1,\mathbf{Z})=\{\pm1\}$. ♦

Пример 23. $\mathbf{SL}(1,\mathbf{R})=\mathbf{SL}(1,\mathbf{Q})=\mathbf{SL}(1,\mathbf{Z})=1$. Но уже при $\boldsymbol{n}=2$ группа $\mathbf{SL}(2,\mathbf{Z})$ бесконечна. Ей принадлежат, в частности, все матрицы

$$\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & 0\\ m & 1\end{pmatrix},\begin{pmatrix}m & m-1\\ 1 & 1\end{pmatrix},\ \boldsymbol{m}\in\mathbf{Z}.\ \blacklozenge$$

3.3.1 Симметрическая и знакопеременная группы

Пусть $\boldsymbol{\Omega}$ – конечное множество из $\boldsymbol{n}$ элементов. Поскольку природа этих элементов для нас несущественна, удобно считать, что $\boldsymbol{\Omega}=\{1,2,\ldots\boldsymbol{n}\}$. Группа $\mathbf{S}(\boldsymbol{\Omega})$ всех взаимно однозначных отображений $\boldsymbol{\Omega}\to\boldsymbol{\Omega}$ называется *симметрической группой степени* $\boldsymbol{n}$ (иначе: *симметрической группой на* $\boldsymbol{n}$ *символах* или *на* $\boldsymbol{n}$ *точках*) и чаще обозначается через $\mathbf{S}_\mathbf{n}$. Ее элементы, обычно обозначаемые строчными буквами греческого алфавита, называются *перестановками* (или *подстановками*).

В развернутой и наглядной форме перестановку σ: $\boldsymbol{i}\to\sigma(\boldsymbol{i})$, $\boldsymbol{i}=1,2,\ldots n$, изображают двухрядным символом

$$\sigma=\begin{pmatrix}1 & 2 & . & . & . & n\\ i_1 & i_2 & . & . & . & i_n\end{pmatrix},$$

полностью указывая все образы:

$$\begin{array}{rl} & 1\ 2\ \ldots\ \boldsymbol{n}\\ \sigma: & \downarrow\downarrow\quad\ \downarrow\\ & \boldsymbol{i}_1\ \boldsymbol{i}_2\ \ldots\ \boldsymbol{i}_\mathrm{n}\end{array}$$

где $\boldsymbol{i}_\mathrm{k}=\sigma(\mathrm{k})$, $\mathrm{k}=1,2,\ldots\boldsymbol{n}$, – переставленные символы $1,2,\ldots\boldsymbol{n}$. Как всегда, $\boldsymbol{e}$ – единичная перестановка $\boldsymbol{e}(\boldsymbol{i})=\boldsymbol{i}$ для любых $\boldsymbol{i}$. Ее обычно не показывают.

Более коротко перестановки будем записывать в виде $\sigma=(i_1 i_2 \ldots i_n)$.

Перестановки $\sigma,\tau\in S_n$ перемножаются в соответствии с общим правилом композиции отображений: $(\sigma\tau)(i)=\sigma(\tau(i))$.

Пример 24. Пусть

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\4&6&1&5&3&2\end{pmatrix},\ \tau=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}.$$

Тогда

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\4&6&1&5&3&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\2&3&5&1&6&4\end{pmatrix}.$$

В то же время

$$\tau\sigma=\begin{pmatrix}1&2&3&4&5&6\\4&6&1&5&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\3&1&6&2&4&5\end{pmatrix}.$$

т.е. $\sigma\tau\neq\tau\sigma$. ♦

Найдем порядок группы S_n. Перестановкой σ символ 1 можно перевести в любой $\sigma(1)$, для чего существует ровно n различных возможностей. Но, зафиксировав $\sigma(1)$, мы можем брать в качестве $\sigma(2)$ лишь один из оставшихся n-1 символов, в качестве $\sigma(3)$ – соответственно n-2 символа, и т.д. Всего имеется $\sigma(1),\sigma(2),\ldots\sigma(n)$ возможностей выбора, а стало быть, и всех различных перестановок получается $n\cdot(n-1)\ldots2\cdot1=n!$. Таким образом,

$$\mathrm{Card}S_n=|S_n|=(S_n:e)=n!$$

Разложим теперь перестановки из S_n в произведения более простых перестановок. Идея разложения поясняется на перестановках из примера 24. Перестановку σ можно записать разными способами:

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\4&6&1&5&3&2\end{pmatrix}=\begin{pmatrix}1&4&5&3&2&6\\4&5&3&1&6&2\end{pmatrix}.$$

Нетрудно заметить, что по существу σ оказалась разложенной на две части:

$$\sigma=\left[\begin{pmatrix}1&4&5&3\\4&5&3&1\end{pmatrix}u\begin{pmatrix}2&6\\6&2\end{pmatrix}\right].$$

Первые четыре места содержат сведения, как σ воздействует на числа 1, 3, 4 и 5, а вторые два мета хранят информацию о воздействии σ на цифры 2 и 6. Более коротко это записывается так:

σ=(1 4 5 3)(2 6); τ=(1 6)(2 5)(3 4); $\sigma\tau$=(1 2 3 5 6 4); $\alpha=\tau\sigma$=(1 3 6 5 4 2).

Перестановка α=(1 3 6 5 4 2), или, что то же самое, α=(3 6 5 4 2 1) =(6 5 4 2 1 3)=(5 4 2 1 3 6)=(4 2 1 3 6 5)=(2 1 3 6 5 4) носит название цикла длины 6, а перестановка σ=(1 4 5 3)(2 6) – есть произведение двух независимых (непересекающихся) циклов длины 4 и 2.

Правило возведения цикла в степень k проиллюстрируем на цикле $\mathbf{C}$=(1 2 3 4 5). Имеем $\mathbf{C}^2$=(1 3 5 2 4), $\mathbf{C}^3$=(1 4 2 5 3), $\mathbf{C}^4$=(1 5 4 3 2), $\mathbf{C}^5$=(1)(2)(3)(4)(5), $\mathbf{C}^6$=(1 2 3 4 5) и т.д. и т.п.

Нетрудно заметить, что при возведении цикла в степень 2, i – ый элемент переходит в элемент, находящийся от него на втором месте справа, при возведении цикла в степень 3, i – ый элемент переходит в элемент, находящийся от него на третьем месте справа, и т.д. и т.п. Отсюда становится понятным правило возведения цикла в степень k. Надо каждый элемент заменить на элемент, стоящий на k – ом месте справа.

Исходя из рассмотренного примера, можно сказать, что верно следующее утверждение: если k – длина цикла $\mathbf{C}$, то $\mathbf{C}^k=\mathbf{C}^{2k}=\ldots=e$ – единичное преобразование.

Пример 25. Пусть σ=(1 4 5 3)(2 6). Тогда σ^2=(1 5)(3 4), σ^3=(1 3 5 4)(2 6), $\sigma^4=e$. ♦

Цикл длины 2 называется *транспозицией*.

Любая транспозиция имеет вид $\tau=(j\ i)$ и оставляет на месте все символы, отличные от j, i.

Для транспозиций справедлива следующая теорема.

Теорема 4. Любая перестановка $\tau\in\mathbf{S_n}$ является произведением транспозиций.

Доказательство. В самом деле, любой цикл можно записать в виде транспозиций следующим образом:

$(1\ 2\ \ldots\ l\text{-}1\ l)=(1\ l)(1\ l\text{-}1)\ldots(1\ 3)(1\ 2)$

что и является доказательством. ♦

Пример 26. Пусть σ=(1 4 5 3)(2 6). Разложим σ в произведение транспозиций. Имеем σ=(1 4 5 3)(2 6)=(1 4)(1 5)(1 3)(2 6)=(3 1)(3 4)(3 5)(2 6) = (4 5)(4 3)(4 1)(2 6) и т.д. и т.п. ♦

Но надо отметить, что ни о какой единственности записи перестановки через транспозиции не может быть и речи. Транспозиции, вообще говоря, не коммутируют, а их число не является инвариантом перестановки.

Пример 27. В $\mathbf{S_4}$ имеем:

(1 2 3)=(1 3)(1 2)=(2 3)(1 3)=(1 3)(2 4)(1 2)(1 4). ♦

Впрочем, неединственность разложения видна из равенства $\sigma\tau^2=\sigma$ для любых транспозиций σ и τ. Тем не менее, один инвариант разложения перестановки через транспозиции все-таки существует. Чтобы обнаружить его по возможности естественным способом, рассмотрим действие $\mathbf{S_n}$ на функциях.

Пусть $\sigma\in\mathbf{S_n}$ и $f(\mathbf{X_1},\ldots\mathbf{X_n})$ – функция от любых n аргументов. Полагаем:

$$(\sigma\circ f)=f\left(X_{\sigma^{-1}(1)},\ldots X_{\sigma^{-1}(n)}\right).$$

Говорят, что функция $g=\sigma\circ f$ *получается действием* σ на f.

Пример 28. Пусть $\sigma=(1\ 2\ 3)$ и $f(X_1,X_2,X_3)=X_1+2X_2^2+3X_3^3$. Тогда $g=\sigma\circ f=X_3+2X_1^2+3X_2^3$. ♦

Говорят, что функция f называется *кососимметрической*, если $\sigma\circ f=-f$ для любой транспозиции $\sigma\in S_n$, т.е.

$$f(X_1,X_2,\ldots X_j,\ldots X_i,\ldots)=-(X_1,X_2,\ldots X_i\ldots X_j\ldots).$$

Лемма 1. Пусть α, β – любые перестановки из S_n. Тогда

$$(\alpha\beta)\circ f=\alpha\circ(\beta\circ f).$$

Доказательство. В соответствии с определением $g=\sigma\circ f$ имеем:

$$(\alpha\beta)\circ f(X_1,\ldots X_n)=f\left(X_{(\alpha\beta)^{-1}(1)},\ldots X_{(\alpha\beta)^{-1}(n)}\right)=$$

$$f\left(X_{(\beta^{-1}\alpha^{-1})(1)},\ldots X_{(\beta^{-1}\alpha^{-1})(n)}\right)=f\left(X_{(\beta^{-1}(\alpha^{-1}(1)))},\ldots X_{(\beta^{-1}(\alpha^{-1}(n)))}\right)=$$

$$\beta\circ f\left(X_{(\alpha)^{-1}(1)},\ldots X_{(\alpha)^{-1}(n)}\right)=\alpha\circ(\beta\circ f(X_1,\ldots X_n))$$

что и требовалось доказать. ♦

Справедлива следующая теорема.

Теорема 5. Пусть π – перестановка из S_n, $\pi=\tau_1\tau_2\ldots\tau_k$ – какое-нибудь разложение π в произведение транспозиций. Тогда число

$$\varepsilon_\pi=(-1)^k,$$

называемое *четностью* π(иначе *сигнатурой* или *знаком* π) полностью определяется перестановкой π и не зависит от способа разложения, т.е. четность целого числа k для данной перестановки π всегда одна и та же. Кроме того, $\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$ для всех $\alpha,\beta\in S_n$.

Доказательство. Возьмем произвольную кососимметрическую функцию f от n аргументов $X_1,\ldots X_n$. По лемме действие π на f сводится к последовательному применению транспозиций τ_k, $\tau_{k-1},\ldots\tau_1$, т.е. к k – кратному умножению f на –1:

$$\pi\circ f=(\tau_1\tau_2\ldots\tau_{k-1})\circ(\tau_k\circ f)=-(\tau_1\tau_2\ldots\tau_{k-1})\circ f=\ldots=(-1)^k f=\varepsilon_\pi f.$$

Так как левая часть этого соотношения зависит от π, но не от какого-либо его разложения, то и отображение $\varepsilon:\pi\to\varepsilon_\pi$, заданное правилом $\varepsilon_\pi=(-1)^k$, должно полностью определятся перестановкой π при условии, конечно, что f – не тождественно равная нулю функция. Но мы знаем, что существуют кососимметрические функции, не равные нулю, например, определитель Вандермонда $\Delta_n(X_1,\ldots X_n)$ порядка n.

Применение к такой функции f перестановки $\alpha\beta$ по правилу, изложенному в лемме, дает:

$$\varepsilon_{\alpha\beta}f=(\alpha\beta)\circ f=\alpha\circ(\beta\circ f)=\alpha\circ(\varepsilon_\beta f)=\varepsilon_\beta(\alpha\circ f)=\varepsilon_\beta(\varepsilon_\alpha f)=(\varepsilon_\alpha\varepsilon_\beta)f,$$

откуда и следует соотношение $\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$. Теорема доказана. ♦

Перестановка $\beta\in S_n$ называется *четной*, если $\varepsilon_\beta=1$, и *нечетной*, если $\varepsilon_\beta=-1$.

Из определения четной и нечетной перестановки следует, что все транспозиции – нечетные перестановки. В связи с этим справедливо следующее

Утверждение. Все четные перестановки степени n образуют подгруппу $\mathbf{A_n} \in \mathbf{S_n}$ порядка $n!/2$ (она называется знакопеременной группой степени n).

Доказательство. Пусть ε_α, ε_β, $\varepsilon_{\alpha\beta}$, $\varepsilon_\pi, \varepsilon_{\pi^{-1}} \in \mathbf{A_n}$. Тогда, так как $\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$, то $\varepsilon_{\alpha\beta}=1$, ввиду того, что $\varepsilon_\alpha=\varepsilon_\beta=1$. Кроме того, и $\varepsilon_{\pi^{-1}}=\varepsilon_\pi$, поскольку $\varepsilon_{\pi^{-1}}\varepsilon_\pi=\varepsilon_e=1=\varepsilon_\pi\varepsilon_\pi$. Так как $\mathbf{A_n}$ – подмножество в $\mathbf{S_n}$, то все аксиомы группы выполнены.

Запишем $\mathbf{S_n}$ в виде $\mathbf{A_n} \cup \underline{\mathbf{A_n}}$, где $\underline{\mathbf{A_n}}$ – множество всех нечетных перестановок степени n. Отображение $\mathbf{S_n}$ в себя, определенное правилом

$$\rho_{(12)}: \pi \to (12)\pi,$$

биективно. (Оно инъективно: $(12)\alpha=(12)\beta \Rightarrow \alpha=\beta$. Далее можно просто заметить, что $(\rho_{(12)})^2$ – единичное отображение). Так как $\varepsilon_{(12)\pi}=\varepsilon_{(12)}\varepsilon_\pi=-\varepsilon_\pi$, то $\rho_{(12)}\mathbf{A_n}=\underline{\mathbf{A_n}}$, $\rho_{(12)}\underline{\mathbf{A_n}}=\mathbf{A_n}$. Значит, число четных перестановок в $\mathbf{S_n}$ совпадает с числом нечетных перестановок. Отсюда $|\mathbf{A_n}|=0.5|\mathbf{S_n}|=n!/2$. Утверждение доказано. ♦

Отметим, что рассмотренный в 1.1. шифр “Скиталла” состоит в преобразовании открытого текста в шифрованный путем определенной перестановки букв открытого текста, т.е. используется группа $\mathbf{S_n}$.

3.4. МОРФИЗМЫ ГРУПП

3.4.1 Изоморфизмы

Известно, что три вращения φ_0, φ_1, φ_2 против часовой стрелки на углы 0°, 120°, 240° переводят правильный треугольник P_3 в себя. Но имеются еще три *осевых преобразования симметрии* (*отражения*) ψ_1, ψ_2, ψ_3 с указанными на рис. 5 осями симметрии 1—1', 2—2', 3—3'. Всем шести

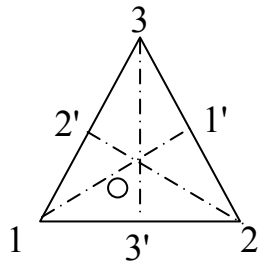

Рис. 5.

преобразованиям симметрии соответствуют перестановки на множестве вершин треугольника. Получаем: $\varphi_0 \sim e, \varphi_1 \sim (123), \varphi_2 \sim (132), \psi_1, \sim (23), \psi_2 \sim (13), \psi_3 \sim (12)$. Так как других перестановок степени 3 нет, то можно утверж-

дать, что группа D_3 всех преобразований симметрии правильного треугольника обнаруживает большое сходство с симметрической группой $\mathbf{S_3}$. Отсюда следует, что нам необходимо каким-то образом сравнивать группы. Для этого вводится понятие изоморфизма. Дадим его определение: две группы **G** и **G'** с операциями $*$ и $\circ$ называются *изоморфными*, если существует отображение $\mathbf{f:G\to G'}$ такое, что:

(i) $\mathbf{f}(a*b)=\mathbf{f}(a)\circ\mathbf{f}(b)$ для всех $a,b\in\mathbf{G}$;

(ii) **f** – биективно.

Факт изоморфизма групп обозначается символически $\cong$.

Отметим простейшие свойства изоморфизма.

1. Единица переходит в единицу. Действительно, если e – единица группы **G**, то $e*a=a*e=a$, и значит $\mathbf{f}(e)\circ\mathbf{f}(a)=\mathbf{f}(a)\circ\mathbf{f}(e)=\mathbf{f}(a)$, откуда следует, что $\mathbf{f}(e)=e'$ – единица группы **G'**. В этом рассуждении использованы, хотя и частично, оба свойства **f**. Для (i) это очевидно, а свойство (ii) обеспечивает сюръективность **f**, так что элементами $\mathbf{f}(g)$ исчерпывается вся группа **G'**.
2. $\mathbf{f}(a^{-1})=\mathbf{f}(a)^{-1}$. В самом деле, согласно (i), $\mathbf{f}(a)\circ\mathbf{f}(a^{-1})=\mathbf{f}(a*a^{-1})=\mathbf{f}(e)=e'$ – единица группы **G'**, откуда $\mathbf{f}(a)^{-1}=\mathbf{f}(a)^{-1}\circ e'=\mathbf{f}(a)^{-1}\circ(\mathbf{f}(a)\circ\mathbf{f}(a^{-1}))=(\mathbf{f}(a)^{-1}\circ\mathbf{f}(a))\circ\mathbf{f}(a^{-1})=e'\circ\mathbf{f}(a^{-1})=\mathbf{f}(a^{-1})$.
3. Обратное отображение $\mathbf{f^{-1}:G\to G'}$ (существующее в силу свойства (ii)) тоже является изоморфизмом. Для этого надо убедиться лишь в справедливости свойства (i) для $\mathbf{f^{-1}}$. Пусть $a',b'\in\mathbf{G'}$. Тогда ввиду биективности **f** имеем $a'=\mathbf{f}(a)$, $b'=\mathbf{f}(b)$ для каких-то $a,b\in\mathbf{G}$. Поскольку **f** – изоморфизм, $a'\circ b'=\mathbf{f}(a)\circ\mathbf{f}(b)=\mathbf{f}(a*b)$. Отсюда имеем $a*b=\mathbf{f^{-1}}(a'\circ b')$, а так как, в свою очередь, $a=\mathbf{f^{-1}}(a')$, $b=\mathbf{f^{-1}}(b')$, то $\mathbf{f^{-1}}(a'\circ b')=\mathbf{f^{-1}}(a')*\mathbf{f^{-1}}(b')$.

Пример 29. В качестве изоморфного отображения **f** мультипликативной группы $(R_+,*,1)$ положительных чисел на аддитивную группу $(R,+,0)$ всех вещественных чисел может служить $\mathbf{f=ln}$. Известное свойство логарифма $\mathbf{ln}\ ab=\mathbf{ln}\ a+\mathbf{ln}\ b$ как раз моделирует свойство (i) в определении изоморфизма. Обратным к **f** служит отображение $x\to e^x$. ♦

Рассмотрим теперь теорему, иллюстрирующую роль изоморфизма в теории групп.

Теорема 6 (Кэли). Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы $\mathbf{S_n}$.

Доказательство. Пусть **G** – конечная группа, $n=|\mathbf{G}|$. Можно считать, что $\mathbf{S_n}$ – группа всех биективных отображений множества **G** на себя, так как природа элементов, представляемых элементами из $\mathbf{S_n}$, несущественна.

Для любого элемента $a\in\mathbf{G}$ рассмотрим отображение $\mathbf{L_a:G\to G}$, определенное формулой:

$$\mathbf{L_a}(g)=ag.$$

Если $e=g_1$, то $g_1,g_2,\ldots g_n$ – все элементы группы **G**. Тогда $ag_1,\ldots ag_n$ – те же элементы, но расположенные в каком-то другом порядке. Это и понятно, поскольку

$$ag_i = ag_k \Rightarrow a^{-1}(ag_i)=a^{-1}(ag_k)\Rightarrow(a^{-1}a)g_i=(a^{-1}a)g_k\Rightarrow g_i=g_k.$$

Значит, $\mathbf{L}_a$ – биективное отображение (перестановка), обратным к которому будет $\mathbf{L}_a^{-1}=L_{a^{-1}}$. Единичным отображением является $\mathbf{L}_e$.

Используя вновь ассоциативность умножения в **G**, получаем $\mathbf{L}_{ab}(g)=(ab)g=a(bg)=\mathbf{L}_a(\mathbf{L}_b(g))$, т.е. $\mathbf{L}_{ab}=\mathbf{L}_a\circ\mathbf{L}_b$.

Итак, множество $\mathbf{L}_e, L_{g_2},\ldots L_{g_n}$ образует подгруппу, скажем **H**, в группе **S**(**G**) всех биективных отображений множества **G** на себя, т.е. в $\mathbf{S}_n$. Мы имеем включение $\mathbf{H}\subset\mathbf{S}_n$ и имеем соответствие $\mathbf{L}:a\to\mathbf{L}_a\in\mathbf{H}$, обладающее по вышесказанному всеми свойствами изоморфизма. ♦.

Теорема Кэли, несмотря на свою простоту, имеет важное значение в теории групп. Она выделяет некий универсальный объект (семейство $\{\mathbf{S}_n|n=1,2,\ldots\}$ симметрических групп) – вместилище всех вообще конечных групп, рассматриваемых с точностью до изоморфизма. Фраза "с точностью до изоморфизма" отражает сущность не только теории групп, стремящейся объединить в один класс все изоморфные группы, но математики в целом, которая без таких обобщений была бы лишена смысла.

Положив **G=G'** в определении изоморфизма, мы получим изоморфное отображение $\varphi:\mathbf{G}\to\mathbf{G}$ группы **G** на себя. Оно называется *автоморфизмом* группы **G**.

Пример 30. Единичное отображение $e_g:g\to g$ – автоморфизм. ♦

Но, как правило, **G** обладает и нетривиальными автоморфизмами. Свойство 3 изоморфных отображений показывает, что отображение, обратное к автоморфизму, тоже будет автоморфизмом. Если, далее, φ,ψ – автоморфизмы группы **G**, то $(\varphi\circ\psi)(ab)=\varphi(\psi(ab))=\varphi(\psi(a)\psi(b))=(\varphi\circ\psi)(a)*(\varphi\circ\psi)(b)$ для любых $a,b\in\mathbf{G}$. Стало быть множество Aut(**G**) всех автоморфизмов группы **G** образует группу – подгруппу группы всех биективных **S**(**G**) отображений $\mathbf{G}\to\mathbf{G}$.

Пример 31. Посмотрим, как можно изменить операцию на группе, не меняя, в смысле изоморфизма, самой группы. Пусть **G** – произвольная группа, t – ее какой-то фиксированный элемент. Введем на множестве **G** новую операцию:

$$(g, h)\to g*h=gth.$$

Непосредственная проверка показывает, что $(g_1*g_2)*g_3=g_1*(g_2*g_3)$, т.е. операция $*$ ассоциативна. Кроме того, $g*t^{-1}=t^{-1}*g=g$ и $g*(t^{-1}g^{-1}t^{-1}) = (t^{-1}g^{-1}t^{-1})*g=t^{-1}$, а это значит, что $\{\mathbf{G},*\}$ – группа с единичным элементом $e_*=t^{-1}$. Элементом обратным к g_* в $\{\mathbf{G},*\}$, служит $g_*^{-1}=t^{-1}g^{-1}t^{-1}$. Отображение $f:g\to gt^{-1}$ устанавливает изоморфизм групп $\{\mathbf{G},\bullet\}$ и $\{\mathbf{G},*\}$, т.е. $f(gh)=f(g)*f(h)$. ♦

3.4.2. Гомоморфизмы

В группе автоморфизмов Aut(**G**) группы **G** содержится одна особая подгруппа. Она обозначается Inn(**G**) и называется *группой внутренних автоморфизмов*. Ее элементами являются отображения $\boldsymbol{I_a}:\boldsymbol{g}\to\boldsymbol{aga^{-1}}$. Небольшое упражнение показывает, что $\boldsymbol{I_a}$ действительно удовлетворяет свойствам, требуемым от автоморфизмов, причем $I_a^{-1} = I_{a^{-1}}$, $\boldsymbol{I_e}$ – единичный автоморфизм, $\boldsymbol{I_a}\circ\boldsymbol{I_b}=\boldsymbol{I_{ab}}$ (потому что $(\boldsymbol{I_a}\circ\boldsymbol{I_b})(\boldsymbol{g})=\boldsymbol{I_a}((\boldsymbol{I_b})(\boldsymbol{g}))=\boldsymbol{I_a}(\boldsymbol{bgb^{-1}})=\boldsymbol{abgb^{-1}a^{-1}}=\boldsymbol{abg}(\boldsymbol{b^{-1}a^{-1}})=\boldsymbol{abg}(\boldsymbol{ab})^{-1}=\boldsymbol{I_{ab}}(\boldsymbol{g})$. Последнее соотношение показывает, что отображение $\boldsymbol{f}:\mathbf{G}\to\mathrm{Inn}(\mathbf{G})$ группы **G** на группу Inn(**G**) ее внутренних автоморфизмов, определенное формулой $\boldsymbol{f}(\boldsymbol{a})=\boldsymbol{I_a}$, $\boldsymbol{a}\in\mathbf{G}$, обладает свойством (i) изоморфного отображения: $\boldsymbol{f}(\boldsymbol{a})\circ\boldsymbol{f}(\boldsymbol{b})=\boldsymbol{f}(\boldsymbol{ab})$. однако свойство (ii) при этом не обязано выполняться. Если, например, **G** – абелева группа, то $\boldsymbol{aga^{-1}}=\boldsymbol{g}$ для всех $\boldsymbol{a}\in\mathbf{G}$, так что $\boldsymbol{I_a}=\boldsymbol{I_e}$, и вся группа Inn(**G**) состоит из одного единичного элемента $\boldsymbol{I_e}$. Это обстоятельство делает естественным следующее определение:

Отображение $\boldsymbol{f}:\mathbf{G}\to\mathbf{G'}$ группы (**G**, ∗) в (**G'**,∘) называется *гомоморфизмом*, если $\boldsymbol{f}(\boldsymbol{a}*\boldsymbol{b})=\boldsymbol{f}(\boldsymbol{a})\circ\boldsymbol{f}(\boldsymbol{b})$, для любых $\boldsymbol{a},\boldsymbol{b}\in\mathbf{G}$ (другими словами, в определении изоморфизма опущено свойство (ii)).

Ядром гомоморфизма $\boldsymbol{f}$ называется множество

$\mathrm{Ker}\,\boldsymbol{f} = \{\boldsymbol{g}\in\mathbf{G} \mid \boldsymbol{f}(\boldsymbol{g}) = \boldsymbol{e'}$– единица группы $\mathbf{G'}\}$.

Гомоморфное отображение группы в себя называется еще ее *эндоморфизмом*.

В определении гомоморфизма от $\boldsymbol{f}$ не требуется не только биективности, но и сюръективности, что, впрочем, не очень существенно, поскольку всегда можно ограничиться рассмотрением образа $\mathrm{Im}\,\boldsymbol{f}\subset\mathbf{G'}$, являющегося, очевидно, подгруппой в **G'**. Главное отличие гомоморфизма $\boldsymbol{f}$ от изоморфизма заключается в наличии нетривиального ядра $\mathrm{Ker}\,\boldsymbol{f}$, являющегося мерой неинъективности $\boldsymbol{f}$. Если же $\mathrm{Ker}\,\boldsymbol{f} = \{\boldsymbol{e}\}$, то $\boldsymbol{f}:\mathbf{G}\to\mathrm{Im}\,\boldsymbol{f}$ – изоморфизм. Заметим, что $\boldsymbol{f}(\boldsymbol{a}) = \boldsymbol{e'}$, $\boldsymbol{f}(\boldsymbol{b}) = \boldsymbol{e'}$,$\Rightarrow\boldsymbol{f}(\boldsymbol{a}*\boldsymbol{b}) =\boldsymbol{f}(\boldsymbol{a})\circ\boldsymbol{f}(\boldsymbol{b}) = \boldsymbol{e'}\circ\boldsymbol{e'}= \boldsymbol{e'}$ и $\boldsymbol{f}(\boldsymbol{a^{-1}})=\boldsymbol{f}(\boldsymbol{a})^{-1}= (\boldsymbol{e})^{-1}=\boldsymbol{e'}$. Поэтому ядро $\mathrm{Ker}\,\boldsymbol{f}$ – подгруппа в **G**.

Пусть $\mathbf{H}=\mathrm{Ker}\,\boldsymbol{f}\subset\mathbf{G}$. Тогда (опуская знаки ∗ и ∘) $\boldsymbol{f}(\boldsymbol{ghg^{-1}}) = \boldsymbol{f}(\boldsymbol{g})\boldsymbol{f}(\boldsymbol{h})\boldsymbol{f}(\boldsymbol{g^{-1}}) =\boldsymbol{f}(\boldsymbol{g})\boldsymbol{e'}\boldsymbol{f}(\boldsymbol{g^{-1}})=\boldsymbol{e'}$, $\forall\boldsymbol{h}\in\mathbf{H}$, $\boldsymbol{g}\in\mathbf{G}$, т.е. $\boldsymbol{ghg^{-1}}\in\mathbf{H}$ и, значит, $\boldsymbol{g}\mathbf{H}\boldsymbol{g^{-1}}\subset\mathbf{H}$. Заменив здесь $\boldsymbol{g}$ на $\boldsymbol{g^{-1}}$, получим $\boldsymbol{g^{-1}}\mathbf{H}\boldsymbol{g}\subset\mathbf{H}$, откуда $\mathbf{H}\subset\boldsymbol{g}\mathbf{H}\boldsymbol{g^{-1}}$. Стало быть, $\mathbf{H}=\boldsymbol{g}\mathbf{H}\boldsymbol{g^{-1}}$, $\forall\boldsymbol{g}\in\mathbf{G}$. Подгруппы, обладающие этим свойством, называются *нормальными*. Еще их называют *инвариантными подгруппами* или *нормальными делителями*. Итак, нами доказана

Теорема 7. Ядра гомоморфизмов всегда являются нормальными подгруппами. ♦

Значение этого факта мы оценим в должной мере позднее. Заметим пока, что далеко не всякая подгруппа нормальна в **G**.

Пример 32. Отображение f:$\mathbf{R}\to\mathbf{T}=\mathbf{SO}(2)$ аддитивной группы вещественных чисел на группу $\mathbf{T}$ вращений плоскости с неподвижной точкой 0, задаваемое формулой $f(\lambda)=\Phi_\lambda$ (Φ_λ – вращение против часовой стрелки на угол $2\pi\lambda$), гомоморфно. Так как $\Phi_\lambda\circ\Phi_\mu=\Phi_{\lambda+\mu}$, а вращение на угол, целочисленно кратный 2π, совпадает с единичным вращением (на нулевой угол), то $\mathrm{Ker}\, f=\{2\pi n \mid n\in\mathbf{Z}\}$. Говорят также, что f – гомоморфизм $\mathbf{R}$ на окружность $\mathbf{S}^1$ единичного радиуса, поскольку имеется взаимно однозначное соответствие между Φ_λ и точкой на $\mathbf{S}^1$ с полярными координатами $(1,2\pi\lambda)$, $0\le\lambda<1$. ♦

Пример 33. Полная линейная группа $\mathbf{GL}(n,\mathbf{R})$ вещественных матриц $\mathbf{A}$ (т.е. матриц с коэффициентами в $\mathbf{R}$) с не равным нулю определителем $\det\mathbf{A}$ гомоморфно отображается на мультипликативную группу $\mathbf{R}^*$ отличных от нуля вещественных чисел, если положить $f=\det$. Условие гомоморфизма $f(\mathbf{AB})=f(\mathbf{A})f(\mathbf{B})$ выполнено. Здесь $\mathbf{SL}(n,\mathbf{R})=\mathrm{Ker}\, f$. ♦

Пример 34. Группа $\mathrm{Aut}(\mathbf{G})$ и даже отдельный неединичный элемент $\varphi\in\mathrm{Aut}(\mathbf{G})$ могут служить источником важных сведений о группе $\mathbf{G}$. Вот яркий пример такого рода. Пусть $\mathbf{G}$ – конечная группа, на которой действует автоморфизм порядка 2 ($\varphi^2=\varphi_e=1$) без неподвижных точек:

$$a\ne e \Rightarrow \varphi(a)\ne a.$$

Предположим, что $\varphi(a)a^{-1}=\varphi(b)b^{-1}$ для каких-то $a,b\in\mathbf{G}$. Тогда после умножения этого равенства на слева на $\varphi(b)^{-1}$ и справа на a получим $\varphi(b)^{-1}\varphi(a)=b^{-1}a$, т.е. $\varphi(b^{-1}a)=b^{-1}a$, откуда $b^{-1}a=e$ и $b^{-1}=a$. Итак, $\varphi(a)a^{-1}$ пробегает вместе с a все элементы группы $\mathbf{G}$, или, что равносильно, любой элемент $g\in\mathbf{G}$ записывается в виде $g=\varphi(a)a^{-1}$. Но в таком случае $\varphi(g)=\varphi(\varphi(a))\varphi(a^{-1})=\varphi^2(a)\varphi(a^{-1})=a\varphi(a)^{-1}=(\varphi(a)a^{-1})^{-1}=g^{-1}$. Итак, φ совпадает с отображением $g\to g^{-1}$. Зная это, получаем $ab=\varphi(a^{-1})\varphi(b^{-1})=\varphi(a^{-1}b^{-1})=(a^{-1}b^{-1})^{-1}=ba$, т.е. группа $\mathbf{G}$ оказывается абелевой. Кроме того, $(\mathbf{G}:e)$ – нечетное число, ибо $\mathbf{G}$ состоит из e и непересекающихся пар элементов g_i: $g_i^{-1}=\varphi(g_i)$. ♦

3.5. КОЛЬЦА. ОПРЕДЕЛЕНИЕ И ОБЩИЕ СВОЙСТВА

Алгебраические структуры $(\mathbf{Z},+)$, $(\mathbf{Z},\bullet)$ выступали у нас в качестве самых первых примеров моноидов, причем на $(\mathbf{Z},+)$ мы смотрели позднее как на аддитивную абелеву группу. В повседневной жизни, однако, эти структуры чаще всего объединяются, и получается то, что в математике называется кольцом. Важный элемент элементарной арифметики заключен в дистрибутивном (или сочетательном) законе $(a+b)c=ac+bc$, кажущимся тривиальным только в силу приобретенной привычки. Попытавшись, например, объединить алгебраические структуры $(\mathbf{Z},+)$, $(\mathbf{Z},\circ)$, где $n\circ m=n+m+nm$, мы уже не заметим столь хорошей согласованности между двумя бинарными операциями. А сейчас дадим определение кольца.

Пусть **K** – непустое множество, на котором заданы две бинарные алгебраические операции + (сложение) и × (умножение), удовлетворяющие следующим условиям:

К1 (**K**,+) – коммутативная (*абелева*) группа;

К2 (**K**,×) – полугруппа;

К3 операции сложения и умножения связаны дистрибутивными законами (другими словами, умножение дистрибутивно по сложению):

$$(a+b)\times c=a\times c+b\times c,\ c\times(a+b)=c\times a+c\times b,\quad a,b,c\in\mathbf{K}.$$

Тогда (**K**,+,×) называется *кольцом*.

Структура (**K**,+) называется *аддитивной группой кольца*, а (**K**,×) – его *мультипликативной полугруппой*. Если (**K**,×) – моноид, то говорят, что (**K**,+,×) – *кольцо с единицей*.

Подмножество **L** кольца **K** называется *подкольцом*, если

$$x, y\in\mathbf{L}\Rightarrow x+y\in\mathbf{L}\text{ и }x\times y\in\mathbf{L},$$

т.е. если **L** – подгруппа аддитивной группы и подполугруппа мультипликативной полугруппы кольца.

Кольцо называется *коммутативным*, если $x\times y=y\times x$ для всех $x,y\in\mathbf{K}$ (в отличие от групп, коммутативное кольцо не принято называть абелевым).

Пример 35. (**Z**,+,•) – кольцо целых чисел с обычными операциями сложения и умножения. Множество $m\mathbf{Z}$ целых чисел, делящихся на m, будет в **Z** подкольцом (без единицы при $m > 1$). Аналогично кольцами с единицей являются **Q** и **R**, причем естественные включения $\mathbf{Z}\subset\mathbf{Q}\subset\mathbf{R}$ определяют цепочки подколец кольца **R**. ♦

Пример 36. Свойства операций сложения и умножения в $\mathbf{M_n(R)}$ показывают, что $\mathbf{M_n(R)}$ – кольцо, называемое *кольцом квадратных матриц порядка* n *над* **R**. ♦

Пример 37. Можно рассматривать кольцо квадратных матриц $\mathbf{M_n(K)}$ над произвольным коммутативным кольцом **K**, поскольку при сложении и умножении двух матриц $\mathbf{A},\mathbf{B}\in\mathbf{M_n(K)}$ будет снова получаться матрица с коэффициентами из **K**. Все это прямо вытекает из формальных действий с матрицами. ♦

Пример 38. Пусть **X** – произвольное множество, **K** – произвольное кольцо, $\mathbf{K^X}=\{\mathbf{X}\to\mathbf{K}\}$ – множество всех функций $\mathbf{f:X}\to\mathbf{K}$, рассматриваемое вместе с двумя бинарными операциями – *поточечной суммой* $f+g$ и *поточечным произведением* fg, определяемыми следующим образом:

$$(f+g)(x)=f(x)\oplus g(x),$$
$$(fg)(x)=f(x)\otimes g(x).$$

(⊕ и ⊗ – операции сложения и умножения в **K**).

Без труда проверяется, что $\mathbf{K^X}$ удовлетворяет всем аксиомам кольца. Так, ввиду дистрибутивности операций в **K**, имеем

$$[f(x)\oplus g(x)]\otimes h(x)=f(x)\otimes h(x)\oplus g(x)\otimes h(x)$$

для любых $f,g,h \in \mathbf{K}^{\mathbf{X}}$ и любого $x \in \mathbf{X}$, а это по определению поточечных операций дает $(f+g)h=fh+gh$. Справедливость второго дистрибутивного закона устанавливается аналогично.

Если 0,1 – нулевой и единичный элементы в **K**, то $\mathbf{0_X}: x \to 0$ и $\mathbf{1_X}: x \to 1$ – постоянные функции, играющие роль нуля и единицы в $\mathbf{K}^{\mathbf{X}}$. В случае коммутативности **K** кольцо функций $\mathbf{K}^{\mathbf{X}}$ также коммутативно. ♦

Пример 39. Кольцо $\mathbf{K}^{\mathbf{X}}$ содержит разнообразные подкольца, определяемые специальными свойствами функций. Пусть **X**=[0,1] – замкнутый интервал в **R** и **K**=**R**. Тогда кольцо $\mathbf{R}^{[0,1]}$ всех вещественных функций, определенных на [0,1], содержит в качестве подколец кольцо $\mathbf{R}_{\text{огр}}^{[0,1]}$ всех ограниченных функций, кольцо $\mathbf{R}_{\text{непр}}^{[0,1]}$ всех непрерывных функций, кольцо $\mathbf{R}_{\text{диф}}^{[0,1]}$ всех непрерывно дифференцируемых функций и т.д., поскольку все отмеченные свойства сохраняются при сложении (вычитании) и умножении функций. ♦

Пример 40. Каждому $a \in \mathbf{R}$ отвечает *постоянная функция* $a_{\mathbf{X}}: x \to a$ и отображение вложения $a \to a_{\mathbf{X}}$ позволяет рассматривать **R** как подкольцо в $\mathbf{R}^{\mathbf{X}}$, т.е. почти каждому естественному классу функций соответствует свое подкольцо в $\mathbf{R}^{\mathbf{X}}$. ♦

Многие свойства колец являются переформулировками соответствующих свойств групп и вообще – множеств с одной ассоциативной операцией. Например, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ для всех неотрицательных целых m, n и всех $a \in \mathbf{K}$. Другие свойства, более специфические для колец и вытекающие прямо из аксиом кольца, моделируют, по существу, свойства **Z**. Отметим некоторые из них.

1. $a0=0a=0$ для всех $a \in \mathbf{K}$. Действительно, $a+0=a \Rightarrow a(a+0)=aa \Rightarrow a^2+a0=a^2 \Rightarrow a^2+a0=a^2+0 \Rightarrow a0=0$ (аналогично $0a=0$).
2. Предположим, что 0=1. Тогда получаем, что $a=a1=a0=0$ для всех $a \in \mathbf{K}$, т.е. **K** состоит только из нуля. Стало быть, в нетривиальном кольце **K** всегда $0 \neq 1$.
3. $(-a)b=a(-b)=-(ab)$. Действительно, $0 = a0 = a(b-b)=ab+a(-b) \Rightarrow a(-b) = -(ab)$. ♦

Аналогично моделируются и некоторые другие свойства.

3.5.1. Сравнения. Кольцо классов вычетов

Множество $m\mathbf{Z}$, очевидно, замкнуто относительно операций сложения и умножения, удовлетворяя при этом всем аксиомам кольца. Таким образом, верно следующее утверждение: каждое ненулевое подкольцо кольца $m\mathbf{Z}$ имеет вид $m\mathbf{Z}$, где $m \in \mathbf{N}$.

Теперь, используя подкольцо $m\mathbf{Z} \subset \mathbf{Z}$, построим ненулевое кольцо, состоящее из конечного числа элементов. С этой целью введем следующее **определение**.

Два целых числа **n** и **n'** называются *сравнимыми по модулю* **m**, если при делении на **m** они дают одинаковые остатки. Пишут **n**≡**n'**(**m**) или **n**≡**n'**(mod **m**), а число **m** называют модулем сравнения.

Таким образом, получается разбиение **Z** на классы чисел, сравнимых между собой по mod **m** и называемых *классами вычетов* по mod **m**. Каждый класс вычетов имеет вид:

$$\{r\}_m = r + mZ = \{r + mk \mid k \in Z\},$$

так что

$$Z = \{0\}_m \cup \{1\}_m \cup \ldots \cup \{m-1\}_m.$$

Таким образом, каждым двум классам $\{k\}_m$ и $\{l\}_m$, независимо от выбора в них представителей k, l, можно сопоставить классы, являющиеся их суммой, разностью или произведением, т.е. на множестве $Z_m = Z/mZ$ классов вычетов по модулю m однозначным образом индуцируются операции $\oplus$ и $\otimes$:

$$\{k\}_m \oplus \{l\}_m = \{k+l\}_m,\ \{k\}_m \otimes \{l\}_m = \{kl\}_m.$$

Так как определение этих операций сводится к соответствующим операциям над числами из классов вычетов, т.е. над элементами из **Z**, то $\{Z_m, \oplus, \otimes\}$ будет также коммутативным кольцом с единицей $\{1\}_m = 1 + mZ$. Оно называется кольцом классов вычетов по модулю m. При небольшом навыке (и фиксированном модуле) отказываются от кружочков и оперируют с каким-нибудь фиксированным множеством представителей по модулю m, чаще всего – с множеством $\{0, 1, 2, \ldots m-1\}$ (оно называется приведенной системой вычетов по модулю m). В соответствии с этим соглашением $-k = m-k$, $2(m-1) = -2 = m-2$.

Итак, конечные кольца существуют. Приведем два простейших примера, указывая отдельно таблицы сложения и умножения:

Z_2:

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	0

Z_3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Так как в кольце классов вычетов определена операция умножения, то там можно совершенно естественно определить операцию возведения в степень, а именно:

$$\underbrace{a*a*\ldots*a}_{k} = a^k.$$

Все это, естественно, сравнивается с модулем m.

Очень часто необходимо достаточно быстро вычислять $a^b \pmod m$. Следующий алгоритм позволяет сделать это за $\mathbf{O}(\ln m)$ арифметических операций. При этом, конечно, предполагается что натуральные числа a и b не превосходят m. Последовательность шагов такова.

1. Представляем b в двоичной системе счисления:
$$b = b_0 2^r + b_1 2^{r-1} + \ldots + b_{r-1} 2 + b_r,$$
где b_i –цифры в двоичном представлении, равные 0 или 1.
2. Присваиваем $a_0 = a$ и затем для $i = 1, \ldots, r$ вычисляем
$$a_i = a_{i-1}^2 \cdot a^{b_i} \pmod m.$$
3. a_r есть искомый вычет.

Справедливость данного алгоритма вытекает из сравнения:
$$a_i \equiv a^{b_0 2^i + \ldots b_i} \pmod m.$$

Пример 41. Рассмотрим $a^b \pmod m = 15^{26} \pmod{32}$. Имеем, $26 = 16+8+2 = 1*2^4 + 1*2^3 + 0*2^2 + 1*2^1 + 0*2^0$, т.е. $b_0=1$, $b_1=1$, $b_2=0$, $b_3=1$, $b_4=0$. Далее, полагаем $a_0 = a = 15$. Затем начинаем вычислять:

$a_1 = a_0^2 \cdot a^{b_1} \pmod m = 15^2 \cdot 15^1 \pmod{32} = 225 \cdot 15 \pmod{32} = 15.$
$a_2 = a_1^2 \cdot a^{b_2} \pmod m = 15^2 \cdot 15^0 \pmod{32} = 225 \cdot 1 \pmod{32} = 1.$
$a_3 = a_2^2 \cdot a^{b_3} \pmod m = 1^2 \cdot 15^1 \pmod{32} = 1 \cdot 15 \pmod{32} = 15.$
$a_4 = a_3^2 \cdot a^{b_4} \pmod m = 15^2 \cdot 15^0 \pmod{32} = 225 \cdot 1 \pmod{32} = 1.$ ♦

3.5.2. . Гомоморфизмы и идеалы колец

Отображение $f : n \to \{n\}_m$ обладает следующими свойствами:
$$f(k+l) = f(k) \oplus f(l); \quad f(kl) = f(k) \otimes f(l).$$
Это дает основание говорить о гомоморфизме колец $\mathbf{Z}$ и $\mathbf{Z_m}$ в соответствии с общим определением.

Пусть $\{\mathbf{K}, +, \cdot\}$ и $\{\mathbf{K}', \oplus, \otimes\}$ – кольца. Отображение $f : \mathbf{K} \to \mathbf{K}'$ называется *гомоморфизмом*, если оно сохраняет все операции, т.е. если
$$f(a+b) = f(a) \oplus f(b); \quad f(ab) = f(a) \otimes f(b).$$
При этом, конечно, $f(0) = 0'$; $f(na) = nf(a)$, $n \in \mathbf{Z}$.

Ядром гомоморфизма f называется множество
$$\operatorname{Ker} f = \{a \in \mathbf{K} \mid f(a) = 0'\}.$$

Ясно, что $\operatorname{Ker} f$ – подкольцо в $\mathbf{K}$. Но это не произвольное подкольцо. Действительно, если $\mathbf{L} = \operatorname{Ker} f \subset \mathbf{K}$, то $\mathbf{L} \cdot x \subseteq \mathbf{L}$ (поскольку $f(lx) = f(l) \otimes f(x) = 0 \otimes f(x) = 0'$ для всех $l \in \mathbf{L}$) и $x \cdot \mathbf{L} \subseteq \mathbf{L}$ для всех $x \in \mathbf{K}$. Стало быть, $\mathbf{L} \cdot \mathbf{K} \subseteq \mathbf{L}$ и $\mathbf{K} \cdot \mathbf{L} \subseteq \mathbf{L}$. Подкольцо $\mathbf{L}$, обладающее этими свойствами, называется *идеалом* кольца $\mathbf{K}$. Итак, ядра гомоморфизмов всегда являются идеалами.

Пример 42. При построении $\mathbf{Z_m}$ неявным образом как раз и использовался тот факт, что $m\mathbf{Z}$ – идеал кольца $\mathbf{Z}$. ♦

Мы видим, что в кольце $\mathbf{Z}$ каждое ненулевое подкольцо является идеалом – случайное обстоятельство, которому нет места, скажем, уже в матричном кольце $\mathbf{M_2(Z)}$: множество

$$\left\{\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} | \alpha,\beta,\delta \in Z\right\}$$

является подкольцом, но не идеалом в $\mathbf{M_2(Z)}$.

Пример $m\mathbf{Z}$ подсказывает способ построения идеалов (возможно, не всех) в произвольном коммутативном кольце **K**: если a – какой-то элемент **K**, то множество $a\mathbf{K}$ всегда является идеалом в **K**. Действительно,

$$ax+ay=a(x+y),\ (ax)y=a(xy).$$

Говорят, что $a\mathbf{K}$ – *главный идеал*, порожденный элементом $a\in\mathbf{K}$.

3.5.3. Типы колец

В хорошо известных нам числовых кольцах **Z**, **Q** и **R** из того, что $ab=0$, следует, что либо $a=0$, либо $b=0$. Но кольцо квадратных матриц $\mathbf{M_n}$ этим свойством уже не обладает. Используя матрицы $\mathbf{E_{ij}}$, состоящие из нулей всюду, кроме элемента, стоящего на пересечении i–строки и j-го столбца (равного 1), получаем что $\mathbf{E_{ij}E_{kl}}=0$ при $\mathbf{j}\neq\mathbf{k}$, хотя, конечно, $\mathbf{E_{ij}}\neq0$ и $\mathbf{E_{kl}}\neq0$. Заметим, что $\mathbf{E_{ik}E_{kl}}\neq0$. Можно было бы приписать столь необычный для элементарной арифметики феномен некоммутативности кольца $\mathbf{M_n}$, но это не так. Рассмотрим еще несколько примеров.

Пример 43. Числовые пары (a,b) ($a,b\in\mathbf{Z}$, **Q** или **R**) со сложением и умножением, определенными формулами

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2),$$
$$(a_1,b_1)(a_2,b_2)=(a_1a_2,\ b_1b_2),$$

образуют, очевидно, коммутативное кольцо с единицей (1,1), в котором мы снова встречаемся с тем же явлением: (1,0)(0,1)=(0,0)=0. ♦

Пример 44. В кольце $\mathbf{R^R}$ вещественных функций (примеры 28-30), функции $f:x\to|x|+x$ и $g:x\to|x|-x$ таковы, что $f(x)=0$ для $x\leq 0$ и $g(x)=0$ для $x\geq 0$, а поэтому их поточечным произведением fg будет нулевая функция, хотя $f\neq0$ и $g\neq0$. ♦

Пример 45. Если кольцо состоит из 3 и менее элементов, то это кольцо коммутативное.

a) Если элемент один, тогда он равен нулю.
b) Если два элемента, тогда $aa=a\neq0$.
c) Если три элемента, тогда $a+b=0$, так как третий элемент не совпадает ни с a, ни с b. Следовательно, $ab=-aa$. Это следует из такого рассуждения:

$a(a+b)=aa+ab=0 \Rightarrow aa=-ab$; Но с другой стороны: $(a+b)a=aa+ba$; $\Rightarrow aa=-ba$ $\Rightarrow ab=ba$. ♦

Пример 46. Покажем, что кольцо из четырех элементов может быть не коммутативным. Введем группу по сложению, состоящую из двух элементов 0 и 1. Нейтральным элементом является 0. Следовательно 1+1=0.

Теперь рассмотрим множество из четырех элементов – прямое произведение такой группы на себя. Оно состоит из пар (a,b), где каждая из компонент может принимать значение 0 или 1: (0,0),(0,1),(1,0),(1,1).

Зададим операцию умножения: $(a+b)(c+d)=((a+b)c,(a+b)d)$.

Покажем ассоциативность:

$(a+b)((c+d)(e+f))=(a+b)((c+d)e,(c+d)f)=((a+b)(c+d)e,(a+b)(c+d)f)$.

С другой стороны,

$((a+b)(c+d))(e+f)=((a+b)c,(a+b)d)(e,f)=(((a+b)c+(a+b)d)e,((a+b)c+(a+b)d)f)=((a+b)(c+d)e,(a+b)(c+d)f)$.

Аналогично показывается выполнение двух законов дистрибутивности.

Но это кольцо не коммутативно. Действительно:

(1,0)(1,1)=((1+0)1,(1+0)1)=(1,1)

(1,1)(1,0)=((1+1)1,(1+1)0)=(0,0). ♦

В связи с вышеизложенным, возникает необходимость в следующем **определении**. Если $ab=0$ при $a\neq 0$ и $b\neq 0$ в кольце $\mathbf{K}$, то a называется *левым*, а b – *правым делителем нуля* (в коммутативных кольцах говорят просто о делителях нуля). Сам нуль в кольце $\mathbf{K}\neq 0$ – тривиальный делитель нуля. Если других делителей нуля нет, то $\mathbf{K}$ называется *кольцом без делителей нуля*. Коммутативное кольцо с единицей $1\neq 0$ и без делителей нуля называют *целостным кольцом* (*кольцом целостности* или *областью целостности*).

Справедлива следующая теорема.

Теорема 8. Нетривиальное коммутативное кольцо $\mathbf{K}$ с единицей является целостным тогда и только тогда, когда в нем выполнен закон сокращения:

$ab=ac,\ a\neq 0 \Rightarrow b=c$

для всех $a,b,c\in\mathbf{K}$.

Доказательство. В самом деле, если в $\mathbf{K}$ имеет место закон сокращения, то из $ab=0=a0$ следует, что либо $a=0$, либо $a\neq 0$, но $b=0$. Обратно, если $\mathbf{K}$ – область целостности, то $ab=ac,\ a\neq 0 \Rightarrow a(b-c)=0 \Rightarrow b-c=0 \Rightarrow b=c$. Теорема доказана. ♦

В кольце $\mathbf{K}$ с единицей естественно рассматривать множество обратимых элементов, т.е. $aa^{-1}=a^{-1}a=1$. Точнее следовало бы говорить об элементах обратимых справа или слева, но в коммутативных кольцах, а также в кольцах без делителей нуля эти понятия совпадают. Действительно, из $ab=1$ следует $aba=a$, откуда $a(ba-1)=0$. Так как $a\neq 0$, то $ba-1=0$, т.е. $ba=1$.

Пример 47. В кольце $\mathbf{M_n}$ обратимые элементы – это в точности матрицы с отличным от нуля определителем. ♦

Обратимый элемент a не может быть делителем нуля. Действительно, если $ab=0$ тогда $a^{-1}(ab)=0 \Rightarrow (a^{-1}a)b=0 \Rightarrow 1b=0 \Rightarrow b=0$ (аналогично $ba=0 \Rightarrow b=0$). Неудивительно, поэтому, что имеет место

Теорема 9. Все обратимые элементы кольца **K** с единицей составляют группу **U**(**K**) по умножению.

Доказательство. Действительно, так как множество **U**(**K**) содержит единицу, а ассоциативность по умножению в **K** выполнена, то нам нужно убедиться в замкнутости множества **U**(**K**), т. е. проверить, что произведение ab любых двух элементов a и b из **U**(**K**) будет снова принадлежать **U**(**K**). Но это очевидно, поскольку $(ab)^{-1}=b^{-1}a^{-1}$, $(abb^{-1}a^{-1}=a(bb^{-1})a^{-1}=aa^{-1}=1)$, и, значит, ab обратим. Теорема доказана. ♦

3.6. ПОЛЕ.

3.6.1. Основные понятия

В предыдущем разделе мы получили весьма интересный класс колец – так называемые *кольца с делением*, или *тела*, заменив в определении кольца аксиому (К2) на существенно более сильное условие (К2'): относительно операции умножения множество $\mathbf{K}^*=\mathbf{K}\backslash\{0\}$ является группой. Кольцо с делением, стало быть, всегда будет без делителей нуля, и каждый ненулевой элемент в нем обратим. Операции сложения и умножения в коммутативном кольце становятся почти полностью симметричными. В математике такая структура носит специальное название – поле. Итак, дадим

Определение. *Поле* **P** – это коммутативное кольцо с единицей $1\neq0$, в котором каждый элемент $a\neq0$ обратим. Группа $\mathbf{P}^*=\mathbf{U}(\mathbf{K})$ называется *мультипликативной группой поля*.

Поле представляет собой гибрид двух абелевых групп – аддитивной и мультипликативной, связанных законом дистрибутивности (теперь уже одним ввиду коммутативности). Произведение ab^{-1} записывается обычно в виде дроби (или отношения) a/b. Следовательно, дробь a/b, имеющая смысл только при $b\neq0$, является решением уравнения $bx=a$. Действия с дробями подчиняются нескольким правилам:

$$a/b=c/d \Leftrightarrow ad=bc,\ b,d\neq0,$$
$$a/b+c/d=(ad+bc)/bd,\ b,d\neq0,$$
$$-(a/b)=(-a/b)=(a/-b),\ b\neq0,$$
$$(a/b)(c/d)=(ac/bd)\quad b,d\neq0,$$
$$(a/b)^{-1}=b/a,\quad a,b\neq0.$$

Это обычные школьные правила, но их надо не запоминать, а выводить из аксиом поля. Посмотрим, как это делается для второго правила. Пусть $x=a/b$ и $y=c/d$ – решения уравнений $bx=a$ и $dy=c$. Из этого следует: $dbx=da$ и $bdy=bc \Rightarrow bd(x+y)=da+bc \Rightarrow t=x+y=(da+bc)/bd$ – единственное решение уравнения $bdt=da+bc$.

Подполем **F** поля **P** называется подкольцо в **P**, само являющееся полем.

Пример 48. Поле рациональных чисел **Q** – подполе поля вещественных чисел **R**. ♦

В случае $\mathbf{F}\subset\mathbf{P}$ говорят также, что поле **P** является *расширением* своего подполя **F**. Из определения подполя следует, что ноль и единица поля **P** будут содержаться также в **F** и служить для **F** нулем и единицей. Если взять в **P** пересечение $\mathbf{F_1}$ всех подполей, содержащих **F** и некоторый элемент $a\in\mathbf{P}$, не принадлежащий **F**, то $\mathbf{F_1}$ будет минимальным полем, содержащим множество $\{\mathbf{F},a\}$. Говорят, что расширение $\mathbf{F_1}$ поля **F** получено *присоединением* к **F** элемента a, и отражают этот факт в записи $\mathbf{F_1}=\mathbf{F}(a)$. Аналогично можно говорить о подполе $\mathbf{F_1}=\mathbf{F}(a_1,\ldots a_n)$ поля **P**, полученном присоединением к **F** n элементов $a_1,\ldots a_n$ поля **P**.

Пример 49. Небольшая проверка показывает, что $\mathbf{Q}(\sqrt{2})$ совпадает с множеством чисел $a+b\sqrt{2}$, $a,b\in\mathbf{Q}$, поскольку $\left(\sqrt{2}\right)^2=2$ и $1/(a+b\sqrt{2}) = (a/(a^2-2b^2))-(b/(a^2-2b^2))\sqrt{2}$ при $a+b\sqrt{2}\neq 0$. То же самое относится к $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{5})$ и т.д. ♦

Поля **P** и **P'** называются изоморфными, если они изоморфны как кольца. По определению $f(0)=0'$ и $f(1)=1'$ для любого изоморфного отображения f. Не имеет смысла говорить о гомоморфизмах полей, так как $\mathrm{Ker}\, f \neq 0 \Rightarrow f(a)=0$, $a\neq 0 \Rightarrow f(1)=f(aa^{-1})=f(a)f(a^{-1})=0f(a^{-1})=0\Rightarrow f(b)=f(1b)=0f(b)=0$ $\forall b \Rightarrow \mathrm{Ker}\, f =\mathbf{P}$. Напротив, автоморфизмы, т.е. изоморфные отображения поля **P** на себя, связаны с самыми глубокими свойствами полей и являются мощным инструментом для изучения этих свойств.

3.6.2. Поля Галуа

В 3.5.1 было построено конечное кольцо классов вычетов $\mathbf{Z_m}$ с элементами $0,1,\ldots m-1$ и операциями сложения и умножения. Если $m=st$, $s>1$, $t>1$, то $st=m=0$, т.е. s и t – делители нуля в $\mathbf{Z_m}$. Если $m=p$ – простое число, то справедлива

Теорема 10. Кольцо классов вычетов $\mathbf{Z_m}$ является полем тогда и только тогда, когда $m=p$ – простое число.

Доказательство. Нам достаточно установить существование для каждого $s\in\mathbf{Z_p}$ обратного элемента $s'\in\mathbf{Z_p}$ (целые числа s и s' не должны, очевидно, делится на p).

Рассмотрим элементы s, $2s$, …, $(p-1)s$. Они все отличны от нуля, так как $s\neq 0 \pmod m \Rightarrow ks\neq 0 \pmod m$ при $k=1,2,\ldots,p-1$. Здесь используется простота p. По этой же причине элементы s, $2s$, …, $(p-1)s$ все различны: из $ks=ls$, $k<l$ следовало бы $(l-k)s=0$, что неверно. Итак, последовательность элементов s, $2s$, …, $(p-1)s$ совпадает с последовательностью переставленных каким-то образом элементов $1,2,\ldots,p-1$. В частности, найдется s', $1\le s'\le p-1$, для которого $s's=1$, т.е. s' – обратный к s элемент. Теорема доказана. ♦

Следствие (малая теорема Ферма). Для любого целого числа m, не делящегося на простое число p, имеет место сравнение:

$$m^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Доказательство. Мультипликативная группа $\mathbf{Z}^*_p$ имеет порядок p-1. Из теоремы Лагранжа, утверждающей, что порядок конечной группы делится на порядок каждой своей подгруппы, следует, что p-1 делится на порядок любого элемента из $\mathbf{Z}^*_p$. Таким образом, $1=(m)^{p-1}=m^{p-1}$, т.е. m^{p-1}–1=0. Следствие доказано. ♦

Именно конечное кольцо классов вычетов $\mathbf{Z}_p$ и называется *полем Галуа* и обозначается GF(p).

Образующим элементом q поля GF(p) называется элемент порядка p-1. (Это равносильно тому, что степени q пробегают все элементы GF(p).♦

Всего в GF(p) имеется $\varphi(p-1)$ различных образующих элементов, где $\varphi(p)$ – функция Эйлера (см.главу 2).

Если q – образующий элемент поля GF(p), то q^j является корнем n-ой степени из единицы тогда и только тогда, когда $nj \equiv 0 (\mathrm{mod}\, p-1)$. Число корней n-ой степени из единицы равно НОД(n,p-1). В частности, GF(p) содержит так называемый *примитивный* корень n-ой степени из единицы (т.е. такой элемент ξ, что степени ξ пробегают все корни n-ой степени из единицы), тогда и только тогда, когда $n|p$-1. Если ξ - примитивный корень n-ой степени из единицы в GF(p), то ξ^j – также примитивный корень n-ой степени из единицы, если НОД(n,j)=1.

Квадраты в GF(p)– называются *квадратичными вычетами*. Остальные элементы называются *невычетами*. В GF(p) имеется ровно (p-1)/2 квадратичных вычетов и невычетов

Пример 50. Пусть p=11. Тогда квадратичными вычетами в GF(11) будут следующие числа: $1^2=1$; $2^2=4$; $3^2=9$; $4^2=5$; $5^2=3$; $6^2=3$; $7^2=5$; $8^2=9$; $9^2=4$; $10^2=1$, т.е. числа 1, 3, 4, 5, 9. Невычетами будут числа 2, 6, 7, 8, 10. ♦

Среди квадратичных вычетов присутствуют числа, являющиеся обычными квадратами в $\mathbf{Z}$. В примере 50 это $2^2=4$, $3^2=9$. Числа 2 и 4 называются *главными квадратичными корнями*.

3.7. КОЛЬЦО МНОГОЧЛЕНОВ

3.7.1. Основные понятия и определения

Многочлены составляют старый и хорошо изученный раздел традиционной алгебры. На языке многочленов формулируются или решаются самые различные задачи математики. Тому есть множество причин, и одна из них заключается в свойстве универсальности кольца многочленов.

Пусть $\mathbf{K}$ – коммутативное кольцо с единицей 1, $\mathbf{A}$ – некоторое его подкольцо, содержащее 1. Если $t \in \mathbf{K}$, то наименьшее подкольцо в $\mathbf{K}$, содержащее $\mathbf{A}$ и t, будет, очевидно, состоять из элементов вида:

$$a(t)=a_0+a_1t+a_2t^2+\ldots+a_nt^n, \qquad (*)$$

где $a_i\in\mathbf{A}$, $n\in\mathbf{Z}$, $n\in\geq 0$. Мы обозначим его символом $\mathbf{A}[t]$ и назовем кольцом, полученным из $\mathbf{A}$ присоединением элемента t, а выражение (*) – многочленом от t с коэффициентами в $\mathbf{A}$. Что понимать под суммой и произведением многочленов, видно из простейшего примера.

Пример 51.

$a(t)+b(t)=(a_0+a_1t+a_2t^2)+(b_0+b_1t+b_2t^2)=(a_0+b_0)+(a_1+b_1)t+(a_2+b_2)t^2$.

$a(t)b(t)=ab_0+(a_0b_1+a_1b_0)t+(a_0b_2+a_1b_1+a_2b_0)t^2+(a_1b_2+a_2b_1)t^3+a_2b_2t^4$. ♦

Очевидно, что приведение подобных членов в $\mathbf{A}[t]$ основано на попарной перестановочности всех элементов a_i, b_j, t^k.

Теперь самое время вспомнить, что t – наугад взятый элемент кольца $\mathbf{K}$, и поэтому внешне различные выражения (*) могут на самом деле совпадать. Если, скажем, $\mathbf{A}=\mathbf{Q}$, $t=\sqrt{2}$, то $t^2=2$ и $t^3=2t$ – соотношения, которые никоим образом не вытекают из формальных правил. Чтобы прийти к привычному понятию многочлена, необходимо освободится от всех таких побочных соотношений, для чего под t следует понимать произвольный элемент, не обязательно содержащийся в $\mathbf{K}$. Он призван играть чисто вспомогательную роль. Гораздо большее значение имеют правила, по которым составляются коэффициенты выражений $a(t)+b(t)$, $a(t)b(t)$. Имея в виду эти предварительные замечания, перейдем к точному определению алгебраического объекта, называемого многочленом, и собрания таких объектов – кольца многочленов.

Пусть $\mathbf{A}$ – произвольное коммутативное кольцо с единицей. Построим новое кольцо $\mathbf{B}$, элементами которого являются бесконечные упорядоченные последовательности:

$$f=(f_0, f_1, f_2, \ldots),\ f\in\mathbf{A}, \qquad (1)$$

такие, что все f_i, кроме конечного их числа, равны нулю. Определим на множестве $\mathbf{B}$ операции сложения и умножения, полагая

$$f+g = (f_0, f_1, f_2, \ldots) + (g_0, g_1, g_2, \ldots) = (f_0+g_0,\ f_1+g_1,\ f_2+g_2, \ldots),$$

$$fg=h=(h_0, h_1, h_2, \ldots),$$

где $h_k=\sum_{i+j=k} f_i g_j$, $k=0,1,2,\ldots$

Ясно, что в результате сложения и умножения получится снова последовательность вида (1) с конечным числом отличных от нуля членов, т.е. элементов из $\mathbf{B}$. Проверка всех аксиом кольца, кроме, разве, аксиомы ассоциативности, очевидна. В самом деле, поскольку сложение двух элементов из $\mathbf{B}$ сводится к сложению конечного числа элементов из кольца $\mathbf{A}$, $(\mathbf{B},+)$ является абелевой группой с нулевым элементом $(0, 0, \ldots)$ и элементом $-f=(-f_0, -f_1, -f_2, \ldots)$ обратным к произвольному $f=(f_0, f_1, f_2, \ldots)$. Далее, коммутативность умножения следует непосредственно из симметричности выражения элементов h_k через f_i и g_j. Это же выражение показывает, что в $\mathbf{B}$ выполнен закон дистрибутивности $(f+g)h= fh+gh$. Что касается ассоциативности операции умножения, то пусть $f = (f_0, f_1, f_2, \ldots)$, $g = (g_0, g_1, g_2, \ldots)$, $h=(h_0, h_1, h_2, \ldots)$ – три произвольных элемента множества $\mathbf{B}$.

Тогда $\boldsymbol{fg}=\boldsymbol{d}=(\boldsymbol{d}_0, \boldsymbol{d}_1, \boldsymbol{d}_2, \ldots)$, где $\boldsymbol{d}_l=\sum_{i+j=l} f_i g_j$, $\boldsymbol{l}=0,1,2,\ldots$, а $(\boldsymbol{fg})\boldsymbol{h}=\boldsymbol{dh}=\boldsymbol{e}=(\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2, \ldots)$, где $\boldsymbol{e}_s=\sum_{l+k=s} d_l h_k=\sum_{l+k=s}\left(\sum_{i+j=l} f_i g_j\right)h_k=\sum_{i+j+k=s} f_i g_j h_k$. Вычисление $\boldsymbol{f}(\boldsymbol{gh})$ дает тот же результат. Итак, **B** – коммутативное кольцо с единицей (1,0,0,…).

Последовательности $(\boldsymbol{a}, 0, 0, \ldots)$ складываются и умножаются так же, как элементы кольца **A**. Это позволяет отождествить такие последовательности с соответствующими элементами из **A**, т.е. положить $\boldsymbol{a}=(\boldsymbol{a}, 0, 0, \ldots)$ для всех $\boldsymbol{a}\in\mathbf{A}$. Тем самым **A** становится подкольцом кольца **B**. Обозначим далее $(0, 1, 0, 0,\ldots)$ через **X** и назовем **X** *переменной* (или *неизвестной*) над **A**. Используя введенную на **B** операцию умножения, получим:

$$\begin{aligned}&\mathbf{X}=(0, 1, 0, 0,\ldots),\\ &\mathbf{X}^2=(0, 0, 1, 0,\ldots),\\ &\ldots\ldots\ldots\ldots\\ &\mathbf{X}^n=(0, 0, 0, 0,\ldots 0, 1, 0, \ldots).\end{aligned} \qquad (2)$$

Кроме того, ввиду (2) и включения $\mathbf{A}\subset\mathbf{B}$, имеем:

$$(0, 0, \ldots 0, \boldsymbol{a}, 0, \ldots)=\boldsymbol{a}\mathbf{X}^n=\mathbf{X}^n\boldsymbol{a}.$$

Итак, если $\boldsymbol{f}_n$ – последний отличный от нуля член последовательности $\boldsymbol{f}=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2, \ldots \boldsymbol{f}_n, 0,\ldots)$, то в новых обозначениях:

$$\boldsymbol{f}=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2,\ldots \boldsymbol{f}_{n-1},0,\ldots)+\boldsymbol{f}_n\mathbf{X}^n=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2,\ldots \boldsymbol{f}_{n-2},0,\ldots)+\boldsymbol{f}_{n-1}\mathbf{X}^{n-1}+\boldsymbol{f}_n\mathbf{X}^n=$$
$$\boldsymbol{f}_0+\boldsymbol{f}_1\mathbf{X}^1+\boldsymbol{f}_2\mathbf{X}^2+\ldots+\boldsymbol{f}_n\mathbf{X}^n. \qquad (3)$$

Такое представление элемента $\boldsymbol{f}$ однозначно, поскольку $\boldsymbol{f}_0, \boldsymbol{f}_1, \ldots \boldsymbol{f}_n$ в правой части (3) – это члены последовательности $(\boldsymbol{f}_0, \boldsymbol{f}_1, \ldots \boldsymbol{f}_n, 0,\ldots)$, которая равна нулю тогда и только тогда, когда $\boldsymbol{f}_0=\boldsymbol{f}_1=\ldots=\boldsymbol{f}_n=0$.

Введенное таким образом кольцо **B** обозначается через $\mathbf{A}[\mathbf{X}]$ и называется *кольцом многочленов над* **A** *от одной переменной* **X**, а его элементы – *многочленами* (или *полиномами*).

Введение заглавной буквы **X** – намеренное, чтобы отличить наш специально выделенный многочлен $\boldsymbol{f}=\mathbf{X}$ от теоретико-функциональной переменной $\boldsymbol{x}$, пробегающей какое-то множество значений. Это чисто временное соглашение, придерживаться которого в будущем не обязательно. Более привычной является запись многочлена $\boldsymbol{f}$ в виде:

$$\boldsymbol{f}(\mathbf{X})=\boldsymbol{a}_0+\boldsymbol{a}_1\boldsymbol{x}^1+\boldsymbol{a}_2\boldsymbol{x}^2+\ldots+\boldsymbol{a}_n\boldsymbol{x}^n,$$

или

$$\boldsymbol{f}(\mathbf{X})=\boldsymbol{a}_0\boldsymbol{x}^n+\boldsymbol{a}_1\boldsymbol{x}^{n-1}+\boldsymbol{a}_2\boldsymbol{x}^{n-2}+\ldots+\boldsymbol{a}_{n-1}\boldsymbol{x}+\boldsymbol{a}_n.$$

Элементы $\boldsymbol{a}_i$ называются *коэффициентами* многочлена $\boldsymbol{f}$. Многочлен $\boldsymbol{f}$ – нулевой, когда все его коэффициенты равны нулю. Коэффициент при $\boldsymbol{x}$ в нулевой степени называется еще постоянным членом. Если $\boldsymbol{a}_n\neq 0$ ($\boldsymbol{a}_0\neq 0$), то $\boldsymbol{a}_n$ ($\boldsymbol{a}_0$) называют *старшим* коэффициентом, а $\boldsymbol{n}$ – *степенью* многочлена и пишут $\boldsymbol{n}=\deg \boldsymbol{f}$. Нулевому многочлену приписывают степень $-\infty$ ($\infty+(-\infty)=-\infty$, $-\infty+\boldsymbol{n}=-\infty$, $-\infty<\boldsymbol{n}$ для каждого $\boldsymbol{n}\in\mathbf{N}$).

Роль единицы кольца **A**[**X**] играет единичный элемент 1 кольца **A**, рассматриваемый как многочлен нулевой степени. Непосредственно из определения операций сложения и умножения в **A**[**X**] следует, что для любых двух многочленов

$$f=f_0+f_1x^1+f_2x^2+\ldots+f_nx^n,\ \ g=g_0+g_1x^1+g_2x^2+\ldots+g_mx^m, \qquad (4)$$

степеней n и m соответственно имеют место неравенства:

$$\deg(f+g)\le\max(\deg f,\deg g),\qquad \deg(fg)\le\deg f+\deg g. \qquad (5)$$

Второе из неравенств (5) заменяется равенством

$$\deg(fg)=\deg f+\deg g$$

всякий раз, когда произведение f_ng_m старших многочленов (4) отлично от нуля, поскольку

$$fg=f_0g_0+(f_0g_1+f_1g_0)x+\ldots+(f_ng_m)x^{n+m}.$$

Но это значит, что верна

Теорема 11. Если **A** – целостное кольцо, то и **A**[**X**] является целостным. ♦

3.7.2. Алгоритм деления в кольце многочленов

В **A**[**X**] над целостным кольцом **A** имеет место алгоритм деления с остатком, аналогичный рассмотренному в 2.5.

Теорема 12. Пусть **A** – целостное кольцо и g – многочлен в **A**[**X**] со старшим коэффициентом, обратимым в **A**. Тогда каждому многочлену $f\in$**A**[**X**] сопоставляется одна и только одна пара многочленов q, $r\in$**A**[**X**], для которых

$$f=qg+r,\quad \deg r<\deg g.$$

Доказательство. Пусть

$$f=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n,$$
$$g=b_0x^m+b_1x^{m-1}+b_2x^{m-2}+\ldots+b_m,$$

где $a_0b_0\neq0$ и $b_0|1$. Применим индукцию по n. Если $n=0$ и $m=\deg g>\deg f=0$, то положим $q=0$, $r=f$, а если $n=m=0$, то $r=0$ и $q=a_0b_0^{-1}$. Допустим, что теорема доказана для всех полиномов степени $<n$ ($n>0$). Без ограничения общности считаем, что $m\le n$, поскольку в противном случае возьмем $q=0$ и $r=f$. Раз это так, то

$$f=a_0b_0^{-1}.x^{n-m}g+f',$$

где $\deg f'<n$. По индукции мы можем найти q' и r', для которых $f'=q'g+r$, причем $\deg r<m$. Положив

$$q=a_0b_0^{-1}.x^{n-m}g+q',$$

мы придем к паре многочленов с нужными свойствами.

Обращаясь к свойству единственности частного q и остатка r, предположим, что

$$qg+r=f=q'g+r'.$$

Тогда $(q'-q)g=r-r'$. По теореме 11 имеем: $\deg(r-r')=\deg(q'-q)+\deg g$, что в наших условиях возможно только при $r'=r$ и $q'=q$.

Наконец, приведенные рассуждения показывают, что коэффициенты частного q и остатка r принадлежат тому же целостному кольцу $\mathbf{A}$, т.е. $f, g \in \mathbf{A}[\mathbf{X}]$. Теорема полностью доказана. ♦

Замечание. Процесс евклидова деления многочлена f на g упрощается, если g – *унитарный многочлен*, т.е. его старший коэффициент равен единице. Делимость f на унитарный многочлен g эквивалентна равенству нулю остатка r при евклидовом деления f на g. ♦

Следствие. Все идеалы кольца многочленов $\mathbf{P}[\mathbf{X}]$ над полем $\mathbf{P}$ – главные.

Доказательство. Пусть $\mathbf{T}$ – какой-то ненулевой идеал в $\mathbf{P}[\mathbf{X}]$. Выберем многочлен $t=t(\mathbf{X})$ минимальный степени, содержащийся в $\mathbf{T}$. Если f – любой многочлен из $\mathbf{T}$, то деление с остатком на t ($\mathbf{P}$ – поле, поэтому нет нужды заботится об обратимости старшего коэффициента у $t(\mathbf{X})$) даст нам равенство $f = qt + r$, $\deg r < \deg t$. Из него следует, что $r \in \mathbf{T}$, поскольку f , t, qt – элементы идеала. Ввиду выбора t нам остается заключить, что $r=0$. Значит, $f(\mathbf{X})$ делится на $t(\mathbf{X})$ и $\mathbf{T}=t\mathbf{P}[\mathbf{X}]$, т.е. $\mathbf{T}$ состоит из многочленов, делящихся на $t(\mathbf{X})$, что и требовалось доказать. ♦

3.7.3. Разложение в кольце многочленов

В произвольном целостном кольце $\mathbf{K}$ обратимые элементы называются *делителями единицы*, или *регулярными элементами*. Совершенно очевидно, что многочлен $f \in \mathbf{A}[\mathbf{X}]$ обратим (регулярен) в точности тогда, когда $\deg f = 0$ и $f = f_0$ – обратимый элемент кольца $\mathbf{A}$, поскольку $fg = 1 \Rightarrow \deg f + \deg g = \deg 1 = 0$.

Говорят, что элемент $b \in \mathbf{K}$ *делится* на $a \in \mathbf{K}$ (или b *кратен* a), если существует такой элемент $c \in \mathbf{K}$, что $b=ac$ (обозначается $a|b$). Если $a|b$ и $b|a$, то a и b называются *ассоциированными* элементами. Тогда $b=ua$, где $u|1$. В силу сделанного выше замечания ассоциированность многочленов $f, g \in \mathbf{A}[\mathbf{X}]$ означает, что они отличаются обратимым множителем из $\mathbf{A}$.

Элемент $p \in \mathbf{K}$ называется *простым* (или *неразложимым*), если p необратим и его нельзя представить в виде $p=ab$, где a, b – необратимые элементы. В поле $\mathbf{P}$ каждый ненулевой элемент обратим, и в $\mathbf{P}$ нет простых элементов. Простой элемент кольца $\mathbf{A}[\mathbf{X}]$ называется чаще *неприводимым многочленом*.

Отметим следующие основные свойства отношения делимости в целостном кольце $\mathbf{K}$.

1) Если $a|b$ и $b|c$, то $a|c$. Действительно, мы имеем $b=ab'$, $c=bc'$, где $b', c' \in \mathbf{K}$. Поэтому $c=(ab')c'=a(b'c')$.
2) Если $c|a$ и $c|b$, то $c|(a \pm b)$. В самом деле, по условию $a=ca'$, $b=cb'$ для некоторых $a', b' \in \mathbf{K}$, и ввиду дистрибутивности $a \pm b = c(a' \pm b')$.
3) Если $a|b$, то $a|bc$. Ясно, что $b=ab' \Rightarrow bc=(ab')c=a(b'c)$.

4) Комбинируя 2) и 3), получаем, что, если каждый из элементов $b_1,b_2,\ldots, b_m\in\mathbf{K}$ делится на $a\in\mathbf{K}$, то на a будет делиться также элемент $b_1c_1+b_2c_2+\ldots+b_mc_m$, где $c_1,c_2,\ldots c_m$ – произвольные элементы.

Теперь введем понятие, которое нам понадобится в дальнейшем. Говорят, что целостное кольцо **K** – *кольцо с однозначным разложением на простые множители* (или **K** – *факториальное кольцо*), если любой элемент $a\neq0$ из **K** можно представить в виде

$$a=up_1p_2\ldots p_r,$$

где u – обратимый элемент, а $p_1,p_2,\ldots p_r$ – простые элементы (не обязательно попарно различные), причем из существования другого такого разложения $a=vq_1q_2\ldots q_s$ следует, что $r=s$, и при надлежащей нумерации элементов p_i и q_j будет

$$q_1=u_1p_1,\ \ldots q_r=u_rp_r.,$$

где $u_1,u_2,\ldots u_r$ – обратимые элементы.

Допуская в равенстве $a=up_1p_2\ldots p_r$ значение $r=0$, мы принимаем соглашение, что обратимые элементы в **K** тоже имеют разложение на простые множители. Ясно, что если p – простой, а u – обратимый элемент, то ассоциированный с p элемент up – тоже простой. В кольце **Z** с обратимыми элементами 1 и –1 отношение порядка ($a<b$) дает возможность выделить *положительное* простое число p из двух возможных простых элементов $\pm p$. В кольце **P**[**X**] удобно рассматривать *унитарные* (с равным единице старшим коэффициентом) неприводимые многочлены.

Справедлива следующая общая

Теорема 13. Пусть **K** – произвольное целостное кольцо с разложением на простые множители. Однозначность разложения в **K** (факториальность **K**) имеет место тогда и только тогда, когда любой простой элемент $p\in\mathbf{K}$, делящий произведение $ab\in\mathbf{K}$, делит по крайней мере один из множителей a, b.

Без доказательства. ♦

В произвольном целостном кольце **K** элемент $a\neq0$ вообще не обязан допускать разложение типа $a=up_1p_2\ldots p_r$. Что более интересно, имеются целостные кольца, в которых разложение на простые множители хотя и возможно, но не является однозначным, т.е. условие теоремы 13, кажущееся тривиальным, не всегда выполняется.

Пример 52. Рассмотрим мнимое квадратичное поле $Q(\sqrt{-5})$, в нем – целостное кольцо $\mathbf{K}=\{a+b\sqrt{-5}\,|a,\ b\in\mathbf{Z}\}$. Норма $\mathbf{N}(a+b\sqrt{-5})=a^2+5b^2$ каждого отличного от нуля элемента $\chi\in\mathbf{K}$– целое положительное число. Если χ в **K**, то $\mathbf{N}(\chi)^{-1}=\mathbf{N}(\chi^{-1})\in\mathbf{Z}$, откуда $\mathbf{N}(\chi)=1$. Это возможно лишь при $b=0$, $a=\pm1$. Таким образом, в **K**, как и **Z**, обратимыми элементами являются только ±1. Если $\chi=\varepsilon\chi_1\chi_2\ldots\chi_r\neq0$, $\varepsilon=\pm1$, то $\mathbf{N}(\chi)=\mathbf{N}(\chi_1)\ldots\mathbf{N}(\chi_r)$. Так как $1<\mathbf{N}(\chi_i)\in\mathbf{Z}$, то при заданном χ число множителей r не может неограниченно расти. Стало быть, разложение на простые множители в **K** возможно.

Вместе с тем число 9 (да и не только оно) допускает два существенно различных разложения на простые множители:

$$9=3\cdot3=(2+\sqrt{-5})\cdot(2-\sqrt{-5}).$$

Неассоциированность элементов 3 и $2\pm\sqrt{-5}$ очевидна. Далее, $\mathbf{N}(3)=\mathbf{N}(2\pm\sqrt{-5})=9$. Поэтому из разложения $\chi=\chi_1\chi_2$ для $\chi=3$ или $2\pm\sqrt{-5}$ с необратимыми χ_1,χ_2 следовало бы $9=\mathbf{N}(\chi)=\mathbf{N}(\chi_1)\mathbf{N}(\chi_2)$, т.е. $\mathbf{N}(\chi_i)=3$, i=1,2, что невозможно, поскольку уравнение $\boldsymbol{x}^2+5\boldsymbol{y}^2=3$ с $\boldsymbol{x},\boldsymbol{y}\in\mathbf{Z}$ неразрешимо. Этим доказана простата элементов 3 и $2\pm\sqrt{-5}$. ♦

3.7.4. Факториальность евклидовых колец

Алгоритм деления с остатком в **Z** и **P**[**X**] делает естественным рассмотрение целостного кольца **K**, в котором каждому элементу $\boldsymbol{a}\neq0$ поставлено в соответствие неотрицательное целое число $\delta(\boldsymbol{a})$, т.е. определено отображение

$$\delta:\ \mathbf{K}\backslash\{0\}=\mathbf{K}^*\to\mathbf{N}\cup\{0\}$$

так, что при этом выполняются условия:

(E1) $\delta(\boldsymbol{ab})\geq\delta(\boldsymbol{a})$ для всех $\boldsymbol{a},\boldsymbol{b}\neq0$ из **K**;

(E2) Каковы бы ни были $\boldsymbol{a},\boldsymbol{b}\in\mathbf{K}$, $\boldsymbol{b}\neq0$, найдутся $\boldsymbol{q},\boldsymbol{r}\in\mathbf{K}$ ($\boldsymbol{q}$ – *частное*, $\boldsymbol{r}$ – *остаток*), для которых

$$\boldsymbol{a}=\boldsymbol{qb}+\boldsymbol{r};\qquad \delta(\boldsymbol{r})<\delta(\boldsymbol{b}) \text{ или } \boldsymbol{r}=0. \tag{6}$$

Целостное кольцо **K** с этими свойствами называется *евклидовым кольцом*.

Пример 53. Полагая $\delta(\boldsymbol{a})=|\boldsymbol{a}|$ для $\boldsymbol{a}\in\mathbf{Z}$ и $\delta(\boldsymbol{a})=\deg\boldsymbol{a}$ для $\boldsymbol{a}\in\mathbf{P}[\mathbf{X}]$, мы приходим к выводу, что **Z** и **P**[**X**] – евклидовы кольца. ♦

В евклидовых кольцах существует способ нахождения НОД($\boldsymbol{a},\boldsymbol{b}$), называемый *алгоритмом последовательного деления* или *алгоритмом Евклида* и заключающийся в следующем.

Пусть даны ненулевые элементы $\boldsymbol{a},\boldsymbol{b}$ евклидова кольца **K**. Применяя достаточно большое (но конечное) число раз предписание (E2), мы получим систему равенств типа (6) с последним нулевым остатком:

$$\begin{aligned}
\boldsymbol{a}&=\boldsymbol{q}_1\boldsymbol{b}+\boldsymbol{r}_1, && \delta(\boldsymbol{r}_1)<\delta(\boldsymbol{b})\\
\boldsymbol{b}&=\boldsymbol{q}_2\boldsymbol{r}_1+\boldsymbol{r}_2, && \delta(\boldsymbol{r}_2)<\delta(\boldsymbol{r}_1)\\
\boldsymbol{r}_1&=\boldsymbol{q}_3\boldsymbol{r}_2+\boldsymbol{r}_3, && \delta(\boldsymbol{r}_3)<\delta(\boldsymbol{r}_2)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\boldsymbol{r}_{k-2}&=\boldsymbol{q}_k\boldsymbol{r}_{k-1}+\boldsymbol{r}_k, && \delta(\boldsymbol{r}_k)<\delta(\boldsymbol{r}_{k-1})\\
\boldsymbol{r}_{k-1}&=\boldsymbol{q}_{k+1}\boldsymbol{r}_k, && \boldsymbol{r}_{k+1}=0.
\end{aligned}$$

Это действительно так, поскольку убывающая цепочка неотрицательных целых чисел $\delta(\boldsymbol{b})>\delta(\boldsymbol{r}_1)>\delta(\boldsymbol{r}_2)>\ldots$ должна оборваться, а обрыв может произойти только за счет обращения в нуль одного из остатков. Последний отличный от нуля остаток $\boldsymbol{r}_k$ = НОД($\boldsymbol{a},\boldsymbol{b}$).

Непосредственным шагом к установлению факториальности евклидова кольца служит

Лемма 2. Всякое евклидово кольцо **K** является кольцом с разложением (т.е. любой элемент $a\neq 0$ из **K** записывается в виде $a=up_1p_2\ldots p_r$).

Доказательство. Пусть элемент $a\in\mathbf{K}$ обладает собственным делителем b: $a=bc$, где b и c – необратимые элементы (другими словами, a и b не ассоциированы). Докажем, что $\delta(b)<\delta(a)$.

В самом деле, согласно (E1), непосредственно имеем $\delta(b)\le\delta(bc)=\delta(a)$. Предположив выполнение равенства $\delta(b)=\delta(a)$, воспользуемся условием (E2) и найдем q,r с $b=qa+r$, где $\delta(r)<\delta(a)$ или же $r=0$. Случай $r=0$ отпадает ввиду неассоциированности a и b. По той же причине $1-qc\neq 0$. Стало быть, снова по (E2) (с заменой a на b) имеем:

$$\delta(a)=\delta(b)\le\delta(b(1-qc))=\delta(b-qa)=\delta(r)<\delta(a)$$

– противоречие. Итак, $\delta(b)<\delta(a)$.

Если теперь $a=a_1a_2\ldots a_n$, где все a_i необратимы, то $a_{m+1}a_{m+2}\ldots a_n$ – собственный делитель $a_ma_{m+1}a_{m+2}\ldots a_n$, и по доказанному:

$$\delta(a)=\delta(a_1a_2\ldots a_n)>\delta(a_2\ldots a_n)>\ldots>\delta(a_n)>\delta(1).$$

Эта строго убывающая цепочка неотрицательных чисел имеет длину $n\le\delta(a)$. Значит, имеется максимальное разложение a на простые множители. Лемма доказана. ♦

Теорема 14. Всякое евклидово кольцо **K** факториально (**K** обладает свойством однозначности разложения на простые множители).

Доказательство. С учетом леммы и критерия факториальности, содержащегося в теореме 13, нам остается показать, что если p – простой элемент кольца **K**, делящий произведение bc каких-то элементов $b,c\in\mathbf{K}$, то p делит либо b, либо c.

Действительно, при $b=0$ или $c=0$ доказывать нечего. Если же $bc\neq 0$ и $d=\text{НОД}(b,c)$, то d, будучи делителем простого элемента p, либо равен 1 (точнее, является делителем 1), либо ассоциирован с p. В первом случае b и p оказываются взаимно простыми, и поэтому $p|c$. Во втором случае $d=up$, $u|1$ и, значит, $p|b$. Теорема доказана. ♦

Следствие. Кольца **Z** и **P**[**X**] – факториальны (**P** – произвольное поле). ♦

3.7.5. Неприводимые многочлены

Специализируя данное ранее определение простого элемента, еще раз подчеркнем, что многочлен f ненулевой степени из кольца **P**[**X**] называется неприводимым в **P**[**X**] (или неприводимым над полем **P**), если он не делится ни на какой многочлен $g\in\mathbf{P}[\mathbf{X}]$, у которого $0<\deg g<\deg f$. В частности, всякий многочлен первой степени неприводим. Совершенно очевидно, что неприводимость многочлена степени >1 или разложение его на простые множители – понятия, тесно связанные с основным полем **P**,

как это показывает многочлен в поле комплексных чисел **C** – $x^2+1=(x-i)(x+i)$. Многочлен x^4+4 приводим над **Q**, хотя об этом нелегко догадаться:

$$x^4+4=(x^2-2x+2)(x^2+2x+2).$$

Оба множителя справа неприводимы не только над **Q**, но и над **R**, будучи приводимы, однако, над **C**.

Как простых чисел в **Z**, так и унитарных *неприводимых многочленов над произвольным полем* **P** *бесконечно много*.

В случае бесконечного поля **P** это ясно: достаточно рассмотреть неприводимые многочлены вида $x-c, c\in\mathbf{P}$.

Если же поле **P** конечно, то годится рассуждение Евклида. Именно, пусть уже найдены n неприводимых многочленов $p_1,p_2,\ldots p_n$. Многочлен $f=p_1p_2\ldots p_n+1$ имеет хотя бы один унитарный простой делитель, поскольку $\deg f \geq n$. Обозначим его через p_{n+1}. Он отличен от $p_1,p_2,\ldots p_n$, поскольку из $p_{n+1}=p_s$ для какого-то $s\leq n$ следовало бы $p_s|(f-p_1p_2\ldots p_n)$, т.е. $p_s|1$, что и требовалось доказать.

Так как над конечным полем количество многочленов заданной степени ограничено, то можно сделать следующее полезное **заключение**:

Над любым конечным полем существуют неприводимые многочлены сколь угодно высокой степени.

А теперь приведем (без доказательства)

Критерий неприводимости (Эйзенштейн).

Пусть

$$f(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\in\mathbf{Z}[x]$$

– унитарный многочлен над **Z**, все коэффициенты $a_1,\ldots,a_n$ которого делятся на некоторое простое число p, но a_n не делится на p^2. Тогда $f[x]$ неприводим над **Q**. ♦

Примечание. Критерий действует и в том случае, когда старший коэффициент отличен от 1, но не делится на p. ♦

Пример 54. Многочлен $f(x)=x^{p-1}+x^{p-2}+\ldots+x+1$ неприводим над **Q** при любом простом p. Для этого достаточно заметить, что вопрос о неприводимости $f(x)$ эквивалентен вопросу о неприводимости многочлена

$$f(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=x^{p-1}+C_1^p x^{p-2}+\ldots+C_{p-2}^p x+C_{p-1}^p,$$

где $C_m^n=\dfrac{n!}{m!(n-m)!}$, и коэффициенты, кроме старшего, делятся на p в первой степени, и, следовательно, применим критерий Эйзенштейна. ♦

4. ДИОФАНТОВЫ УРАВНЕНИЯ

4.1. ДИОФАНТОВО УРАВНЕНИЕ ПЕРВОЙ СТЕПЕНИ

Для нахождения секретных ключей в криптосистемах с открытым ключом, часто применяется математический аппарат на базе диофантовых уравнений. Рассмотрим его основные положения.

Поставим задачу отыскания целочисленного решения так называемого линейного диофантова уравнения:

$$ax-by=c, \qquad (7)$$

где $a, b, c \in \mathbf{Z}$.

Такое уравнение называется диофантовым. Рассмотрим два метода его решения.

Так как $\mathbf{Z}$ – евклидово факториальное кольцо (см. 3.7.4), то в нем всегда возможно нахождение наибольшего общего делителя чисел a и b - НОД(a,b) при помощи алгоритма Евклида. Находим его. Если НОД(a,b)=0, то уравнению удовлетворяют любые целые x и y. Если НОД(a,b) не равен 0, и c на НОД(a,b) не делится, то уравнение не имеет решения. Иначе производим сокращение коэффициентов a,b,c и получаем уравнение вида (7), но с взаимно простыми a,b,c.

При первом методе, для нахождения решения (7), число a/b обращают в конечную цепную дробь при помощи алгоритма Евклида:

$$\begin{aligned}
a&=bq_0+a_1,\\
b&=a_1q_1+a_2,\\
a_1&=a_2q_2+a_3,\\
a_2&=a_3q_3+a_4,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
a_{k-2}&=a_{k-1}q_{k-1}+a_k,\\
a_{k-1}&=a_kq_k+0;
\end{aligned}$$

Цепная дробь имеет вид: $a/b = [q_0,q_1,q_2,\ldots q_k]$, а последовательности $\{\mathbf{P_n}\}$ и $\{\mathbf{Q_n}\}$ числителей и знаменателей подходящих дробей к цепной дроби определяются рекуррентно:

$$\begin{aligned}
&\mathbf{P_{-2}}=0,\ \mathbf{P_{-1}}=1;\\
&\mathbf{Q_{-2}}=1,\ \mathbf{Q_{-1}}=0;\\
n\geq 0 \Rightarrow\ &\mathbf{P_n} = q_n\mathbf{P_{n-1}} + \mathbf{P_{n-2}},\\
n\geq 0 \Rightarrow\ &\mathbf{Q_n} = q_n\mathbf{Q_{n-1}} + \mathbf{Q_{n-2}}.
\end{aligned}$$

Их вычисление удобно оформлять в виде таблицы:

N	-2	-1	0	1	2	…	k-1	K
q_n			q_0	q_1	q_2	…	q_{k-1}	q_k
$\mathbf{P_n}$	0	1	$\mathbf{P_0}$	$\mathbf{P_1}$	$\mathbf{P_2}$	…	$\mathbf{P_{k-1}}$	$\mathbf{P_k}$
$\mathbf{Q_n}$	1	0	$\mathbf{Q_0}$	$\mathbf{Q_1}$	$\mathbf{Q_2}$	…	$\mathbf{Q_{k-1}}$	$\mathbf{Q_k}$

Но известно, что $\mathbf{P_kQ_{k-1}}-\mathbf{P_{k-1}Q_k}=(-1)^{k-1}$ и $a/b = \mathbf{P_k}/\mathbf{Q_k}$. Следовательно, $(-1)^{k-1}\mathbf{P_kQ_{k-1}}-\mathbf{P_{k-1}}(-1)^{k-1}\mathbf{Q_k}=1$.

А так как НОД($\boldsymbol{a}$,$\boldsymbol{m}$)=1, то $\mathbf{P_k} = \boldsymbol{a}$, $\mathbf{Q_k} = \boldsymbol{b}$. Поэтому

$$(-1)^{k-1}\mathbf{Q_{k-1}}\boldsymbol{a} - \boldsymbol{b}(-1)^{k-1}\mathbf{P_{k-1}}=1.$$

Другими словами, пара ($\boldsymbol{x}$,$\boldsymbol{y}$), где $\boldsymbol{x}=(-1)^{k-1}\mathbf{Q_{k-1}}$; $\boldsymbol{y}=(-1)^{k-1}\mathbf{P_{k-1}}$, являются целочисленным решением уравнения (7).

Пример 55. Решить уравнение:

$$17745*x - 19362240*y=15. \qquad (*)$$

Находим НОД(17745, 19362240)=15.

Производим сокращение коэффициентов $\boldsymbol{a}$,$\boldsymbol{b}$,$\boldsymbol{c}$ и получаем уравнение вида (7), но с взаимно простыми $\boldsymbol{a}$,$\boldsymbol{b}$,$\boldsymbol{c}$.

$$1183*x-1290816*y=1. \qquad (**)$$

Имеем далее.

N	-2	-1	0	1	2	3	4	5	6	7
q_n			0	1091	7	3	1	7	2	2
P_n	0	1	0	1	7	22	29	225	479	1183
Q_n	1	0	1	1091	7638	24005	31643	245506	522655	1290816

1183=1290816∗0+1183
1290816=1183∗1091+163
1183=163∗7+42
163=42∗3+37
42=37∗1+5
37=5∗7+2
5=2∗2+1
2=1∗2+0
k=7; x=$(-1)^6$×522655=522655; y= $(-1)^6$×479=479; (1183∗522655-1290816∗479=618300865- 618300864=1.

Таким образом, x=522655 и y=479 являются решением (**). Чтобы получить решение (*), умножим x и y на НОД(17745, 19362240)=15 и получим x=522655*15= 7839825 и y=479*15=7185.♦

Второй метод решения (7) также опирается на алгоритм Евклида. Последовательность действий такова.

0. Определяем матрицу $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
1. Вычисляем $\boldsymbol{r}$ – остаток от деления числа $\boldsymbol{a}$ на $\boldsymbol{b}$: $\boldsymbol{a}=\boldsymbol{bq}+\boldsymbol{r}$, $0 \le \boldsymbol{r} < |\boldsymbol{b}|$.
2. Если $\boldsymbol{r}=0$, то второй столбец матрицы $\boldsymbol{A}$ дает вектор $\begin{pmatrix} x \\ y \end{pmatrix}$ решений уравнения (7).
3. Если $\boldsymbol{r}\neq 0$, то заменим матрицу $\boldsymbol{A}$ матрицей $A = A * \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}$.
4. Заменяем пару ($\boldsymbol{a}$,$\boldsymbol{b}$) парой ($\boldsymbol{b}$,$\boldsymbol{r}$) и переходим к шагу 1.

Пример 56. Решить уравнение:

$$1183*x-1290816*y=1. \qquad (***)$$

Это уравнение совпадает с уравнением из предыдущего примера. Имеем.

Определяем матрицу $A=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$.

Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
1183=1290816∗0+1183.

Т.к. ***r***≠0, то заменяем матрицу ***A*** матрицей $A=A*\begin{pmatrix}0 & 1\\ 1 & q\end{pmatrix}=$

$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}*\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

Заменяем пару (***a***,***b***) парой (***b***,***r***): ***a*** = 1290816; ***b***=1183.

Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
1290816=1183∗1091+163.

Т.к. ***r***≠0, то заменяем матрицу ***A*** матрицей $A=A*\begin{pmatrix}0 & 1\\ 1 & q\end{pmatrix}=$

$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}*\begin{pmatrix}0 & 1\\ 1 & 1091\end{pmatrix}=\begin{pmatrix}1 & 1091\\ 0 & 1\end{pmatrix}$.

Заменяем пару (***a***,***b***) парой (***b***,***r***): ***a*** = 1183; ***b***=163.

Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
1183=163∗7+42.

Т.к. ***r***≠0, то заменяем матрицу ***A*** матрицей $A=A*\begin{pmatrix}0 & 1\\ 1 & q\end{pmatrix}=$

$\begin{pmatrix}1 & 1091\\ 0 & 1\end{pmatrix}*\begin{pmatrix}0 & 1\\ 1 & 7\end{pmatrix}=\begin{pmatrix}1091 & 7638\\ 1 & 7\end{pmatrix}$.

Заменяем пару (***a***,***b***) парой (***b***,***r***): ***a*** = 163; ***b***=42.

Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
163=42∗3+37

Т.к. ***r***≠0, то заменяем матрицу ***A*** матрицей $A=A*\begin{pmatrix}0 & 1\\ 1 & q\end{pmatrix}=$

$\begin{pmatrix}1091 & 7638\\ 1 & 7\end{pmatrix}*\begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}=\begin{pmatrix}7638 & 24005\\ 7 & 22\end{pmatrix}$.

Заменяем пару (***a***,***b***) парой (***b***,***r***): ***a*** = 42; ***b***=37.

Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
42=37∗1+5.

Т.к. ***r***≠0, то заменяем матрицу ***A*** матрицей $A=A*\begin{pmatrix}0 & 1\\ 1 & q\end{pmatrix}=$

$\begin{pmatrix}7638 & 24005\\ 7 & 22\end{pmatrix}*\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}24005 & 31643\\ 22 & 29\end{pmatrix}$.

Заменяем пару (***a***,***b***) парой (***b***,***r***): ***a*** = 37; ***b***=5.
Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
37=5∗7+2.

Т.к. ***r***≠0, то заменяем матрицу ***A*** матрицей $A = A*\begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}=$

$\begin{pmatrix} 24005 & 31643 \\ 22 & 29 \end{pmatrix}*\begin{pmatrix} 0 & 1 \\ 1 & 7 \end{pmatrix}=\begin{pmatrix} 31643 & 245506 \\ 29 & 225 \end{pmatrix}$.

Заменяем пару (***a***,***b***) парой (***b***,***r***): ***a*** = 5; ***b***=2.
Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
5=2∗2+1.

Т.к. ***r***≠0, то заменяем матрицу ***A*** матрицей $A = A*\begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}=$

$\begin{pmatrix} 31643 & 245506 \\ 29 & 225 \end{pmatrix}*\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}=\begin{pmatrix} 245506 & 522655 \\ 225 & 479 \end{pmatrix}$.

Заменяем пару (***a***,***b***) парой (***b***,***r***): ***a*** = 2; ***b***=1.
Вычисляем ***r*** – остаток от деления числа ***a*** на ***b***: ***a***=***bq***+***r***, 0≤ ***r*** < |***b***|.
2=1∗2+0

Т.к. ***r***=0, то второй столбец матрицы ***A***, а именно $\begin{pmatrix} 522655 \\ 479 \end{pmatrix}$ и есть решение (***). ♦

4.2. РЕШЕНИЕ СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

Чтобы найти решение сравнения $ax \equiv 1 \pmod m$, где НОД(***a***,***m***)=1, обычно пользуются алгоритмом Евклида, и тогда $x \equiv (-1)^{k-1} Q_{k-1} \pmod m$, где Q_{k-1} – знаменатель предпоследней подходящей дроби разложения ***a***/***m*** в цепную дробь, или теоремой *Ферма-Эйлера*, которая утверждает, что если НОД(***a***,***m***)=1, то

$$a^{\varphi(m)} \equiv 1 \pmod m,$$

где $\varphi(m)$ – функция Эйлера.

Следовательно

$$x \equiv a^{\varphi(m)-1} \pmod m.$$

Пример 57. Решить сравнение:

$$143*x \equiv 1 \pmod{8531}.$$

Функция Эйлера равна:

$$\varphi(m) = \varphi(8531) = 8531*(1-1/19)*(1-1/449) = 8064.$$

Отсюда следует, что $x \equiv a^{\varphi(m)-1} \pmod m = 143^{8063} = 6443 \pmod{8531}$.

Проверка: 143*6443=921349=1(**mod** 8531). ♦

Но таким способом решение уравнения сравнения ищут редко. Это связано с тем, что при больших ***m***, нахождение функции $\varphi(m)$ становится достаточно сложной задачей, особенно при неизвестном разложении. Поэтому, обычно применют методы, рассмотренные в пункте 4.1.

Пример 58. Решить сравнение:

$$7283*x\equiv 1(\mathbf{mod}\ 190116)$$

Имеем

$$7283=190116*0+7283$$
$$190116=7283*26+758$$
$$7283=758*9+461$$
$$758=461*1+297$$
$$461=297*1+164$$
$$297=164*1+133$$
$$164=133*1+31$$
$$133=31*4+9$$
$$31=9*3+4$$
$$9=4*2+1$$
$$4=1*4+0$$

n			0	1	2	3	4	5	6	7	8	9	10
q_n			0	26	9	1	1	1	1	4	3	2	4
Q_n	1	0	1	26	235	261	496	757	1253	5769	18560	42889	190116

Действительно, k=10; $x\equiv(-1)^9\times 42889$ (**mod** 190116)= -42889 (**mod** 190116) = 147227(**mod** 190116); (7283*147227-1)/ 190116=5640 ♦

5. СИММЕТРИЧЕСКИЕ КРИПТОСИСТЕМЫ

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в 3 этапа:

1. отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);
2. отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;
3. получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

Криптографические алгоритмы обычно строятся с использованием простых и быстро выполняемых операторов нескольких типов. Множество обратимых операторов, преобразующих текст длиной n бит в текст длиной n бит, являются элементами группы обратимых операторов по умножению (например, подстановок n-разрядных слов). Пусть f, g, h — обратимые операторы, то есть существуют f^{1}, g^{-1} и h^{-1}. Поэтому hgf – последовательное выполнение операторов fgh - тоже обратимый оператор (операторы выполняются справа налево) с обратным оператором к этому произведению, $h^{-1}g^{-1}f^{1}$. Поэтому дешифратор выполняет те же операции, что и шифратор, но в обратном порядке, и каждый оператор расшифрования является обратным к соответствующему оператору шифрования. Некоторые операторы являются взаимно обратными, то есть выполнение подряд два раза некоторой операции над текстом дает исходный текст.

Все многообразие существующих криптографических методов с секретным ключом можно свести к следующим классам преобразований (рис.6):

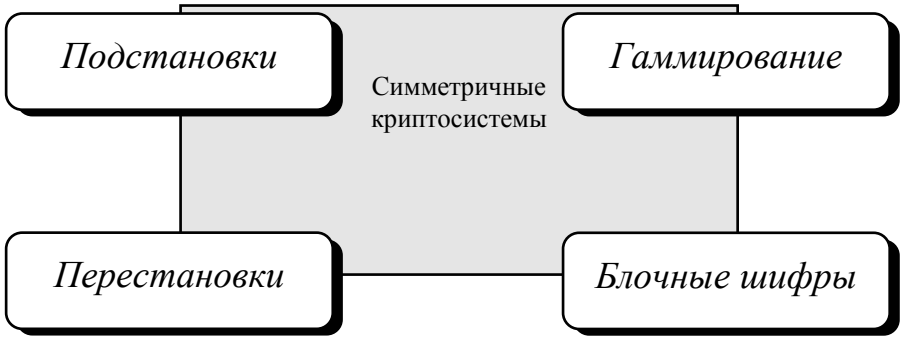

Рис.6. Основные криптографические методы с секретным ключом

Рассмотрим их подробнее.

5.1 Моно- и многоалфавитные подстановки

Моно- и многоалфавитные подстановки являются наиболее простыми из преобразований, заключающимися в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Определение. *Подстановкой* π на алфавите $\mathbf{Z_n}$ называется автоморфизм, при котором буквы исходного текста t замещены буквами шифрованного текста $\pi(\mathbf{t})$:

$$\mathbf{Z_n} \rightarrow \mathbf{Z_n};\quad \pi: \mathbf{t} \rightarrow \pi(\mathbf{t}).$$

Набор всех подстановок из $\mathbf{Z_n}$ с операцией умножения является симметрической группой, которую будем обозначать $\mathbf{S(Z_n)}$. Для доказательства этого утверждения необходимо показать выполнение всех аксиом группы.

Доказательство.

1. *Замкнутость*: произведение подстановок $\pi_1\pi_2$ является подстановкой:
$$\pi: \mathbf{t}\rightarrow\pi_1(\pi_2(\mathbf{t})).$$
2. *Ассоциативность*: результат произведения $\pi_1\pi_2\pi_3$ не зависит от порядка расстановки скобок:
$$(\pi_1\pi_2)\pi_3=\pi_1(\pi_2\pi_3)$$
3. *Существование нейтрального элемента*: постановка $\boldsymbol{i}$, определяемая как $\boldsymbol{i}(\mathbf{t})=\mathbf{t}$, $0\le\mathbf{t}<\mathbf{m}$, является нейтральным элементом $\mathbf{S(Z_n)}$ по операции умножения: $\boldsymbol{i}\pi=\pi\boldsymbol{i}$ для $\forall\pi\in\mathbf{S(Z_n)}$.
4. *Существование обратного*: для любой подстановки π существует единственная обратная подстановка π^{-1}, удовлетворяющая условию:
$$\pi\pi^{-1}=\pi^{-1}\pi=\boldsymbol{i}.\ \blacklozenge$$

Определение. *Ключом* подстановки $\boldsymbol{k}$ для $\mathbf{Z_n}$ называется последовательность элементов симметрической группы $\mathbf{S(Z_n)}$:

$$\boldsymbol{k}=(\boldsymbol{p}_0,\boldsymbol{p}_1,...,\boldsymbol{p}_{n-1},...),\ \boldsymbol{p}_i\in\mathbf{S(Z_n)},\ 0\le\mathbf{n}<\infty.$$

Подстановка, определяемая ключом $\boldsymbol{k}$, является криптографическим преобразованием $\mathbf{T}_{\boldsymbol{k}}$, при помощи которого осуществляется преобразование $\boldsymbol{n}$-граммы[1] исходного текста $(\boldsymbol{x}_0,\boldsymbol{x}_1,..,\boldsymbol{x}_{n-1})$ в $\boldsymbol{n}$-грамму шифрованного текста $(\boldsymbol{y}_0,\boldsymbol{y}_1,...,\boldsymbol{y}_{n-1})$:

$$\boldsymbol{y}_i=\boldsymbol{p}(\boldsymbol{x}_i),\quad 0\le\mathbf{i}<\boldsymbol{n}$$

где $\boldsymbol{n}$ – произвольное ($\boldsymbol{n}$=1,2,..). $\mathbf{T}_{\boldsymbol{k}}$ называется моноалфавитной подстановкой, если $\boldsymbol{p}$ неизменно при любом $\mathbf{i}$, $\mathbf{i}$=0,1,..., в противном случае $\mathbf{T}_{\boldsymbol{k}}$ называется многоалфавитной подстановкой.

Примечание. К наиболее существенным особенностям подстановки $\mathbf{T}_{\boldsymbol{k}}$ относятся следующие:

1. *Исходный текст шифруется посимвольно*. Шифрования n-граммы $(\boldsymbol{x}_0,\boldsymbol{x}_1,..,\boldsymbol{x}_{n-1})$ и ее префикса $(\boldsymbol{x}_0,\boldsymbol{x}_1,..,\boldsymbol{x}_{s-1})$ связаны соотношениями:

[1] n-граммой называется последовательность из n символов алфавита

$$\mathbf{T_k}(x_0,x_1,..,x_{n-1})=(y_0,y_1,...,y_{n-1})$$

$$\mathbf{T_k}(x_0,x_1,..,x_{s-1})=(y_0,y_1,...,y_{s-1})$$

2. Буква шифрованного текста y_i является функцией только i-ой компоненты ключа p_i и i-ой буквы исходного текста x_i.

Кратко рассмотренный в п. 1.2 шифр Цезаря, является самым простым вариантом подстановки. Она относится к группе моноалфавитных подстановок.

Определение. Подмножество $C_n=\{C_k: 0\le k<n\}$ симметрической группы $\mathbf{S(Z_n)}$, содержащее n подстановок

$$C_k: j\to(j+k)\ (\mathbf{mod}\ n),\ 0\le k<n,$$

называется подстановкой Цезаря.

Рассмотрим свойства подстановки Цезаря. Умножение коммутативно, $C_kC_j=C_jC_k=C_{j+k}$, C_0 – единичная подстановка, а обратной к $C_к$ является $C_k^{-1}=C_{n-k}$, где $0<k<n$.

Семейство подстановок Цезаря названо по имени римского императора Гая Юлия Цезаря, который поручал Марку Туллию Цицерону составлять послания с использованием 50-буквенного алфавита и подстановки C_3.

Подстановка определяется по таблице замещения, содержащей пары соответствующих букв “исходный текст – шифрованный текст”. Для C_3 подстановки приведены в Табл. 2. Стрелка (→) означает, что буква исходного текста (слева) шифруется при помощи C_3 в букву шифрованного текста (справа).

Таблица 2.

0	А→г	9	Й→м	18	Т→х	27	Ы→ю
1	Б→д	10	К→н	19	У→ц	28	Ь→я
2	В→е	11	Л→о	20	Ф→ч	29	Э→_
3	Г→ж	12	М→п	21	Х→ш	30	Ю→а
4	Д→з	13	Н→р	22	Ц→щ	31	Я→б
5	Е→и	14	О→с	23	Ч→ъ	32	_→в
6	Ж→й	15	П→т	24	Ш→ы		
7	З→к	16	Р→у	25	Щ→ь		
8	И→л	17	С→ф	26	Ъ→э		

Определение. *Системой Цезаря* называется моноалфавитная подстановка, преобразующая n-грамму исходного текста $(x_0,x_1,..,x_{n-1})$ в n-грамму шифрованного текста $(y_0,y_1,...,y_{n-1})$ в соответствии с правилом:

$$y_i=C_k(x_i),\ 0\le i<n.$$

Пример 59. Сообщение ИЗУЧАЙТЕ_КРИПТОГРАФИЮ посредством подстановки C_3 преобразуется в лкцъгмхивнултсжугчла. ♦

При своей несложности система легко уязвима. Если злоумышленник имеет:

1) шифрованный и соответствующий исходный текст или
2) шифрованный текст выбранного злоумышленником исходного текста,

то определение ключа и дешифрование исходного текста тривиальны.

Более эффективны обобщения подстановки Цезаря - *шифр Хилла* и *шифр Плэйфера*. Они основаны на подстановке не отдельных символов, а 2-грамм (шифр Плэйфера) или *n*-грамм (шифр Хилла). При более высокой криптостойкости они значительно сложнее для реализации и требуют достаточно большого количества ключевой информации.

Слабая криптостойкость моноалфавитных подстановок преодолевается с применением многоалфавитных подстановок, которые определяются ключом $\pi=(\pi_1,\pi_2, ...)$, содержащим не менее двух различных подстановок. В начале рассмотрим многоалфавитные системы подстановок с нулевым начальным смещением.

Пусть $\{K_i: 0\le i<n\}$ - независимые случайные переменные с одинаковым распределением вероятностей, принимающие значения на множестве $\mathbf{Z}_m$:

$$\mathbf{P}\{(K_0, K_1, ..., K_{n-1})=(k_0, k_1, ..., k_{n-1})\}=(1/m)^n.$$

Система одноразового использования преобразует исходный текст:

$$\mathbf{X}=(x_0, x_1, ..., x_{n-1})$$

в шифрованный текст:

$$\mathbf{Y}=(y_0, y_1, ..., y_{n-1})$$

при помощи подстановки Цезаря:

$$y_i=C_{Ki}(x_i)=(K_i+x_i)\ (\mathbf{mod}\ m) \quad i=0,1,\ldots n-1.$$

Для такой системы подстановки используют также термин “одноразовая лента” и “одноразовый блокнот”. Пространство ключей K системы одноразовой подстановки является вектором ранга $(K_0, K_1,...,K_{n-1})$ и содержит mn точек.

Пример 60. В качестве ключа примем текст:

“НЕ_ЛЕНИТЕСЬ ИЗУЧАТЬ КРИПТОГРАФИЮ”.

Зашифруем с помощью его и таблицы 2 текст “ПОПРОБУЙ_ РАЗГАДАЙ ”. Шифрование оформим в таблицу:

ПОПРОБУЙ_ РАЗГАДАЙ	15	14	15	16	14	1	19	9	32	16	0	7	3	0	4	0	9
НЕ ЛЕНИТЕСЬ ИЗУЧАТЬ КРИПТОГРАФИЮ	13	5	32	11	5	13	8	18	5	17	28	32	8	19	23	0	18
ЬУБЫНОЫЫДБЬЖЛУЫАЫ	28	19	1	27	19	14	27	27	4	1	28	6	11	19	27	0	27

♦

Наложение белого шума в виде бесконечного ключа на исходный текст меняет статистические характеристики языка источника. Системы одноразового использования теоретически нерасшифруемы, так как не содержат достаточной информации для восстановления текста. Но эти системы практически не применяются для обеспечения секретности при

обработке информации ввиду того, что они непрактичны, так как требуют независимого выбора значения ключа для каждой буквы исходного текста. Хотя такое требование может быть и не слишком трудным при переписке, но для информационных каналов оно непосильно, поскольку придется шифровать многие миллионы знаков.

5.2 Системы шифрования Вижинера

Ослабим требование шифровать каждую букву исходного текста отдельным значением ключа. Начнем с конечной последовательности ключа:

$$\boldsymbol{k} = (\boldsymbol{k}_0,\boldsymbol{k}_1,...,\boldsymbol{k}_n),$$

которая называется *ключом пользователя*, и продлим ее до бесконечной последовательности, повторяя цепочку. Таким образом, получим *рабочий ключ* $\boldsymbol{k} = (\boldsymbol{k}_0,\boldsymbol{k}_1,...,\boldsymbol{k}_n)$, $\boldsymbol{k}_j = \boldsymbol{k}_{(j \bmod r)}$, $0 \le \boldsymbol{j} < \infty$. Например, при $\boldsymbol{r} = \infty$ и ключе пользователя 17 23 11 56 43 97 25 рабочий ключ будет периодической последовательностью:

17 23 11 56 43 97 25 17 23 11 56 43 97 2517 23 11 56 43 97 25...

Определение. Подстановка Вижинера $\mathrm{VIG_k}$ определяется так $\mathbf{VIG_k}$: $(\boldsymbol{x}_0, \boldsymbol{x}_1, ..., \boldsymbol{x}_{n-1}) \rightarrow (\boldsymbol{y}_0, \boldsymbol{y}_1, ..., \boldsymbol{y}_{n-1}) = (\boldsymbol{x}_0+\boldsymbol{k}, \boldsymbol{x}_1+\boldsymbol{k},. .., \boldsymbol{x}_{n-1}+\boldsymbol{k})$.

Таким образом:

1) исходный текст *x* делится на *r* фрагментов $\mathbf{x_i}=(\boldsymbol{x_i}, \boldsymbol{x_{i+r}},..., \boldsymbol{x_{i+r(n-1)}})$, $0 \le \boldsymbol{i} < \boldsymbol{r}$;

2) ***i***-й фрагмент исходного текста $\mathbf{x_i}$ шифруется при помощи подстановки Цезаря $\boldsymbol{C_k}$:$(\boldsymbol{x_i}, \boldsymbol{x_{i+r}}, ..., \boldsymbol{x_{i+r(n-1)}}) \rightarrow (\boldsymbol{y_i}, \boldsymbol{y_{i+r}}, ..., \boldsymbol{y_{i+r(n-1)}})$.

Вариант системы подстановок Вижинера при $\boldsymbol{m}$=2 называется *системой Вернама (1917 г)*. В то время ключ $\boldsymbol{k}=(\boldsymbol{k}_0,\boldsymbol{k}_1,...,\boldsymbol{k}_{к-1})$ записывался на бумажной ленте. Каждая буква исходного текста в алфавите, расширенном некоторыми дополнительными знаками, сначала переводилась с использованием *кода Бодо* в пятибитовый символ. К исходному тексту Бодо добавлялся ключ (по модулю 2). Старинный телетайп фирмы AT&T со считывающим устройством Вернама и оборудованием для шифрования, использовался корпусом связи армии США.

Очень распространена плохая с точки зрения секретности практика использовать слово или фразу в качестве ключа для того, чтобы $\boldsymbol{k}=(\boldsymbol{k}_0, \boldsymbol{k}_1, ..., \boldsymbol{k}_{к-1})$ было легко запомнить. В информационных системах для обеспечения безопасности информации это недопустимо. Для получения ключей должны использоваться программные или аппаратные средства случайной генерации ключей.

Пример 61. Преобразование текста с помощью подстановки Вижинера при $\boldsymbol{r}$=5.

Исходный текст – РАБОТАЙТЕ АККУРАТНО

Ключ: ПЕСНЯ

Разобьем исходный текст на блоки по 5 символов: РАБОТ АЙТЕ АККУР АТНО
и наложим на них ключ (используя таблицу Вижинера):
Р+П=Я, А+Е=Е и т.д. Получаем зашифрованный текст: ЯЕТЫР ППВТЮ ППЫ_О ПЧЮЫЯ ♦

Можно выдвинуть и обобщенную систему Вижинера. Ее можно сформулировать не только при помощи подстановки Цезаря.

Пусть $\mathbf{x} \subset \mathbf{Z_m}$ - подмножество.

Определение. ***r**-многоалфавитный ключ* шифрования есть ***r***-набор $\pi = (\pi_0, \pi_1, ..., \pi_{r-1})$ перестановок $\pi \subset \mathbf{S(Z_m)}$.

Обобщенная система Вижинера преобразует исходный текст $(x_0, x_1,...,x_{n-1})$ в шифрованный текст $(y_0,y_1,...,y_{n-1})$ при помощи ключа $\pi = (\pi_0, \pi_1, ..., \pi_{r-1})$ по правилу $VIG_k : (x_0,x_1,...,x_{n-1}) \rightarrow (y_0,y_1,...,y_{n-1}) = (\pi_0(x_0), \pi_1(x_1), ..., \pi_{n-1}(x_{n-1}))$, где $\pi_i = \pi_{i \bmod r}$.

Следует признать, что и многоалфавитные подстановки в принципе доступны криптоаналитическому исследованию. Криптостойкость многоалфавитных систем резко убывает с уменьшением длины ключа.

Тем не менее такая система как шифр Вижинера допускает несложную аппаратную или программную реализацию и при достаточно большой длине ключа может быть использован в современных ИС.

5.3 Перестановки

Перестановки являются также несложным методом криптографического преобразования. Используется как правило в сочетании с другими методами. Определение перестановки было дано в 5.2.

Введем обозначение σ для взаимно-однозначного отображения набора $S=\{s_0,s_1, ...,s_{n-1}\}$, состоящего из n элементов, на себя, т.е. $\sigma: S \rightarrow S$, $\sigma: s_i \rightarrow s_{\sigma(i)}$, $0 \le i < n$. Будем говорить, что в этом смысле σ является *перестановкой элементов* S. И, наоборот, автоморфизм S соответствует перестановке целых чисел (0,1,2,.., n-1).

Криптографическим преобразованием $\mathbf{T}$ для алфавита $\mathbf{Z_m}$ называется последовательность автоморфизмов: $\mathbf{T}=\{\mathbf{T}^{(n)}: 1 \le n < \infty\}$ $\mathbf{T}^{(n)}: \mathbf{Z_m} \rightarrow \mathbf{Z_m}$, $1 \le n < \infty$. Каждое $\mathbf{T}^{(n)}$ является, таким образом, перестановкой n-грамм из $\mathbf{Z_m}$. Поскольку $\mathbf{T}^{(i)}$ и $\mathbf{T}^{(j)}$ могут быть определены независимо при $i \ne j$, число криптографических преобразований исходного текста размерности n равно $(m^n)!$[2]. Оно возрастает непропорционально при увеличении m и n: так, при m=33 и n=2 число различных криптографических преобразований равно 1089!. Отсюда следует, что потенциально существует большое число отображений исходного текста в шифрованный.

Практическая реализация криптографических систем требует, чтобы преобразования $\{\mathbf{T}_k: k \in K\}$, где K – множество ключей, были определе-

ны алгоритмами, зависящими от относительно небольшого числа параметров (ключей).

5.4 Гаммирование

Гаммирование является также широко применяемым криптографическим преобразованием. На самом деле граница между гаммированием и использованием бесконечных ключей и шифров Вижинера, о которых речь шла выше, весьма условная.

Шифром гаммирования называется шифр с алфавитом открытых сообщений $\mathbf{Z_m}$, совпадающим с алфавитом шифрованных сообщений и ключевым множеством $\boldsymbol{K}$. При этом для любого открытого текста $\mathbf{A}=\{\boldsymbol{a}_1, \boldsymbol{a}_2,.\boldsymbol{a}_s,\ldots\} \in \mathbf{Z_m}$ и $\forall\ \boldsymbol{k} \in \boldsymbol{K}$

$$\mathbf{F}(\mathbf{A},\boldsymbol{k})= \boldsymbol{b}_1,\boldsymbol{b}_2,...\boldsymbol{b}_s\ ,\ldots$$

$$\boldsymbol{b}_1=\boldsymbol{a}_1 + \Psi_1(\boldsymbol{k})\ \mathbf{mod}\ (\boldsymbol{m})$$

$$\boldsymbol{b}_i =\boldsymbol{a}_i + \Psi_i(\boldsymbol{a}_1,\boldsymbol{a}_2, ..., \boldsymbol{a}_{i-1},\boldsymbol{k})\ \mathbf{mod}\ (\boldsymbol{m}),\ \ \boldsymbol{i}=2,3,...$$

Таким образом, шифр гаммирования, заключается в сложении по модулю $\boldsymbol{m}$ (мощность алфавита открытых сообщений) открытого текста с некой последовательностью чисел из $\mathbf{Z_m}$ - гаммой, полученной из исходного ключа и предыдущих знаков открытого текста. Очевидно, что в данной формулировке шифр Вернама также является шифром гаммирования.

Обычно в настоящее время используется $\boldsymbol{K}=(\mathbf{Z}_{\boldsymbol{m}})^{\boldsymbol{n}}$.

Зависимость знаков гаммы от знаков открытого текста используется достаточно редко.

Объем ключевой информации ограничивается в данном случае тем, что для шифрования сообщений используется ключ фиксированной длины в независимости от длины сообщения. Отсюда очевидным образом следует, что гамма не может быть произвольной последовательностью чисел из $\mathbf{Z}_{\boldsymbol{m}}$, а следовательно речи о «совершенной стойкости» идти не может.

Задача создания качественного шифра гаммирования заключается в обеспечении следующих свойств.

1. Максимальную близость гаммы по статистическим свойствам к случайной равновероятной последовательности независимых величин (далее по аналогии с термином «белый шум», известным из физики, такую последовательность будем называть «белой гаммой»).
2. Отсутствие возможности практического восстановления неизвестных отрезков гаммы и ключа по известным.

Первое свойство необходимо обеспечивать для невозможности дешифрования шифра гаммирования статистическими методами. Это свойство характеризует в некотором смысле близость конкретного шифра к шифру Вернама. Второе - для того чтобы по части открытого текста невозможно было восстановить весь текст или другие его отрезки.

К достоинствам шифров гаммирования следует отнести следующее:

1. Возможность достижения высоких скоростей шифрования.
2. Коэффициент размножения ошибки равен единице.
3. Поточность шифрования и расшифрования.
4. Сохранение размера текста при шифровании

К недостаткам относится:

1. Нестойкость шифра при повторном использовании ключа
2. Последовательность доступа к информации

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей. По сути дела гамма шифра должна изменяться случайным образом для каждого шифруемого слова. Фактически же, если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (пробой на ключ). Криптостойкость в этом случае определяется размером ключа.

Метод гаммирования становится бессильным, если злоумышленнику становится известен фрагмент исходного текста и соответствующая ему шифрограмма. Простым вычитанием по модулю получается отрезок почти случайной последовательности (ПСП) и по нему восстанавливается вся последовательность. Злоумышленники может сделать это на основе догадок о содержании исходного текста. Так, если большинство посылаемых сообщений начинается со слов “СОВ.СЕКРЕТНО”, то криптоанализ всего текста значительно облегчается. Это следует учитывать при создании реальных систем информационной безопасности. Ниже рассматриваются наиболее распространенные методы генерации гамм, которые могут быть использованы на практике. Этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

5.5 Датчики почти случайных чисел

Чтобы получить линейные последовательности элементов гаммы, длина которых превышает размер шифруемых данных, используются *датчики почти случайных чисел (ПСЧ)*. На основе теории групп было разработано несколько типов таких датчиков.

Конгруэнтные датчики

В настоящее время наиболее доступными и эффективными являются *конгруэнтные* генераторы ПСП. Для этого класса генераторов можно сделать математически строгое заключение о том, какими свойствами об-

ладают выходные сигналы этих генераторов с точки зрения периодичности и случайности.

Одним из хороших конгруэнтных генераторов является линейный конгруэнтный датчик ПСЧ. Он вырабатывает последовательности псевдослучайных чисел **T(*i*)**, описываемые соотношением

T(***i***+1) = (**A**∗**T**(***i***)+**C**) **mod** ***m***,

где **A** и **C** - константы, **T**(0) - исходная величина, выбранная в качестве порождающего числа. Очевидно, что эти три величины и образуют ключ.

Такой датчик ПСЧ генерирует псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений **A** и **C**. Значение ***m*** обычно устанавливается равным 2^{n} , где ***n*** - длина машинного слова в битах. Датчик имеет максимальный период ***m*** до того, как генерируемая последовательность начнет повторяться. По причине, отмеченной ранее, необходимо выбирать числа **A** и **C** такие, чтобы период ***m*** был максимальным. Как показано Д. Кнутом, линейный конгруэнтный датчик ПСЧ имеет максимальную длину **M** тогда и только тогда, когда **C** - нечетное, и **A mod** 4 = 1.

Для шифрования данных с помощью датчика ПСЧ может быть выбран ключ любого размера. Например, пусть ключ состоит из набора чисел ***x***(***j***) размерностью ***n***, где ***j***=1, 2, ..., ***n***. Тогда создаваемую гамму шифра **G** можно представить как объединение непересекающихся множеств **H**(***j***).

Датчики М-последовательностей

Популярность М-последовательностей объясняется относительно легкой их реализаций.

М-последовательности представляют собой линейные рекуррентные последовательности максимального периода, формируемые ***k***-разрядными генераторами на основе регистров сдвига. На каждом такте поступивший бит сдвигает ***k*** предыдущих и к нему добавляется их сумма по модулю 2. Вытесняемый бит добавляется к гамме. Строго это можно представить в виде следующих отношений:

$r_1 := r_0 \quad r_2 := r_1 \quad \ldots \quad r_{k-1} := r_{k-2}$

$r_0 := a_0 r_1 \oplus a_1 r_2 \oplus \ldots \oplus a_{k-2} r_{k-1}$

$\Gamma_i := r_{k-}$

Здесь $r_0\ r_1 \ldots\ r_{k-1}$ - ***k*** однобитных регистров, $a_0\ a_1 \ldots\ a_{k-1}$ – коэффициенты неприводимого двоичного полинома степени ***k***-1. Γ_i - ***i***-е значение выходной гаммы.

Период **M**-последовательности, исходя из ее свойств, равен 2^{k}-1.

Другим важным свойством **M**-последовательности является *объем ансамбля*, т.е. количество различных **M**-последовательностей для заданного ***k***. Эта характеристика приведена в таблице 3.

Таблица 3

k	Объем ансамбля
5	6
6	8
7	18
8	16
9	48
10	60
16	2048

Очевидно, что такие объемы ансамблей последовательности неприемлемы. Поэтому на практике часто используют последовательности Голда, образующиеся суммированием нескольких **M**-последовательностей. Объем ансамблей этих последовательностей на несколько порядков превосходят объемы ансамблей порождающих **M**-последовательностей. Так при k=10 ансамбль увеличивается от 1023 (**M**-последовательности) до 388000.

Также перспективными представляются нелинейные датчики ПСП (например сдвиговые регистры с элементом И в цепи обратной связи), однако их свойства еще недостаточно изучены. Возможны и другие, более сложные варианты выбора порождающих чисел для гаммы шифра.

Шифрование с помощью датчика ПСЧ является распространенным криптографическим методом. Во многом качество шифра, построенного на основе датчика ПСЧ, определяется не только и не столько характеристиками датчика, сколько алгоритмом получения гаммы. Один из фундаментальных принципов криптологической практики гласит: даже сложные шифры могут быть очень чувствительны к простым воздействиям.

5.6 Стандарт шифрования DES

Одним из самых распространенных алгоритмов шифрования является DES - алгоритм (Data Encryption Standart), разработанный в 1977 г. и рекомендованный Национальным бюро стандартов США совместно с АНБ в качестве основного средства криптографической защиты информации как в государственных, так и в коммерческих структурах. Однако в 1988 г. АНБ рекомендовало использовать DES только в системах электронного перевода. В последнее время, с учетом выявленных слабостей DES, появляются изменения в начальном варианте стандарта и новые алгоритмы, использующие в качестве основы DES - NewDes, TripleDES и др. Появление новых алгоритмов было обусловлено развитием за многолетнее существование данного алгоритма большого количества атак на DES. Кроме того, бурное развитие производительности и быстродействия средств вычислительной и микропроцессорной техники привело к тому, что 56 битного ключа используемого в оригинальном варианте DES стало

недостаточно, чтобы противостоять атаке методом грубой силы. Тем не менее, DES и на сегодняшний день он остается одним из самых применяемых алгоритмов блочного шифрования в коммерческой сфере и в системах электронных расчетов.

DES является блочным алгоритмом шифрования с длиной блока 64 бита и симметричными ключами длиною 56 бит. На практике обычно ключ имеет длину 64 бита, где каждый восьмой бит используется для контроля четности остальных битов ключа.

Всего для получения блока зашифрованного сообщения проходит 16 раундов. В DES используется 16 раундов по следующим причинам:

- 12 раундов является минимально необходимым для обеспечения должного уровня криптографической защиты
- при аппаратной реализации использование 16 раундов позволяет вернуть преобразованный ключ в исходное состояние для дальнейших преобразований
- данное количество раундов необходимо для того, чтобы исключить возможность проведения атаки на блок зашифрованного текста с двух сторон

В некоторых реализациях DES блоки открытого сообщения перед тем как будут загружены в регистр сдвига длиной равной 2 ячейки и размером ячейки 32 бита, проходят процедуру начальной перестановки, которая применяется для того, чтобы провести начальное рассеивание статистической структуры сообщения.

DES предусматривает 4 режима работы:

- ECB (Electronic Codebook) электронный шифрблокнот;
- CBC (Cipher Block Chaining) цепочка блоков;
- CFB (Cipher Feedback) обратная связь по шифртексту;
- OFB (Output Feedback) обратная связь по выходу.

Говоря о DES невозможно было бы обойти стороной тему безопасности данного алгоритма и возможных атак на него. Многолетний опыт эксплуатации DES и его открытость (исходные тексты алгоритма и документацию на него можно встретить в открытых источниках) привели к тому, что DES стал одним из популярнейших алгоритмов с точки зрения криптоанализа. На сегодняшний день существует ряд атак на DES учитывающих слабости алгоритма, которых за столь долгий срок эксплуатации было выявлено достаточное количество. Некоторые из атак реализуемы только в предположении, что атакующий обладает некоторыми возможностями и в ряде случаев атаки с точки зрения практической реализации можно смело отнести эти атаки к теоретически возможным. Хотя не исключено, что со временем они перейдут в разряд практически возможных.

Среди основных недостатков DES существенно снижающих уровень безопасности при использовании данного алгоритма можно выделить следующие:

- наличие слабых ключей, вызванное тем, что при генерации ключевой последовательности используются 2 регистра сдвига, которые работают независимо друг от друга. Примером, слабого ключа может служить 1F1F1F1F 0E0E0E0E (с учетом битов контроля четности). В данном случае результатом генерации будут ключевые последовательности одинаковые с исходным ключом во всех 16 раундах. Существуют также разновидности слабых ключей, которые дают при генерации всего лишь 2 (4) ключевые последовательности. Так же для неполнораундовых схем DES характерно наличие связанных ключей, например, ключ полученный из другого ключа посредством инверсии одного бита;
- небольшая длина ключа 56 бит (или 64 бита с контролем четности). При современном уровне развития микропроцессорной средств данная длина ключа не может обеспечивать должный уровень защиты для некоторых типов информации. Применение тройного DES (TripleDES) не дают ощутимого результата хотя и используются 3 разных ключа (К1, К2, К3). В конечном итоге эквивалентно зашифрованию на другом ключе К4, т.е. для любых К1, К2, К3 найдется ключ К4 такой, что: ЕК3(DК2(ЕК1(Р)))=ЕК4(Р);
- наличие избыточности ключа, обусловленное контролем четности для каждого байта ключа отдельно. Бихам и Шамир предложили достаточно эффективную атаку на реализацию DES в смарт-картах или банковских криптографических модулях, использующих EEPROM память для хранения ключей. Данная атака демонстрирует очередную слабость DES, состоящую в наличие контроля четности каждого байта ключа, который создает избыточность ключа и позволяет восстанавливать ключи, хранящиеся в памяти устройства, в случае сбоя в данном участке памяти;
- использование статических подстановок в S-боксах, что несмотря на большое количество раундов позволяет криптоаналитикам проводит атаки, учитывающие данный факт. Хотя на сегодняшний день автору не известно успешных атак на 16 раундовый DES, основанных на данном факте. Но успешные атаки на неполнораундовые схемы DES имеют место быть. Так Мартин Хэллман предложил атаку на 8 раундовый DES. Предложенная атака позволяет успешно восстанавливать 10 бит ключа за 10 сек. на рабочей станции SUN-4 и имеет вероятность успеха 80% в случае выбора 512 открытых текстов и 95% в случае выбора 768 открытых текстов. Восстановив 10 бит ключа можно воспользоваться алгоритмами перебора всех оставшихся вариантов, и свести таким образом задачу нахождения 56- битного ключа к нахождения 46-битного ключа

Учитывая выше сказанное можно с уверенностью сказать, что использование DES на сегодняшний день является опасным с точки зрения криптографической стойкости и обеспечения надежного функционирова-

ния систем криптографической защиты информации, использующих данный алгоритм.

5.7 Стандарт шифрования ГОСТ-28147-89

Важной задачей в обеспечении гарантированной безопасности информации в ИС является разработка и использования стандартных алгоритмов шифрования данных. Первым среди подобных стандартов стал американский алгоритм DES, представляющий собой последовательное использование замен и перестановок. В настоящее время все чаще говорят о неоправданной сложности и невысокой криптостойкости. На практике приходится использовать его модификации.

Более эффективным является отечественный стандарт шифрования данных ГОСТ-28147-89.

Он рекомендован к использованию для защиты любых данных, представленных в виде двоичного кода, хотя не исключаются и другие методы шифрования. Данный стандарт формировался с учетом мирового опыта, и в частности, были приняты во внимание недостатки и нереализованные возможности алгоритма DES, поэтому использование стандарта ГОСТ предпочтительнее. Алгоритм достаточно сложен и ниже будет описана в основном его концепция.

Введем ассоциативную операцию конкатенации, используя для нее мультипликативную запись. Кроме того, будем использовать следующие операции сложения:

- A⊕B - побитовое сложение по модулю 2;
- A[+]B - сложение по модулю 2^{32};
- A{+}B - сложение по модулю 2^{32}-1;.

Алгоритм криптографического преобразования предусматривает несколько режимов работы. Во всех режимах используется ключ W длиной 256 бит, представляемый в виде восьми 32-разрядных чисел $\boldsymbol{x}(\boldsymbol{i})$:

$$W=\boldsymbol{x}(7)\boldsymbol{x}(6)\,\boldsymbol{x}(5)\,\boldsymbol{x}(4)\boldsymbol{x}(3)\boldsymbol{x}(2)\boldsymbol{x}(1)\boldsymbol{x}(0).$$

Для дешифрования используется тот же ключ, но процесс дешифрования является инверсным по отношению к исходному.

Самый простой из возможных режимов - *замена.*

Пусть открытые блоки разбиты на блоки по 64 бит в каждом, которые обозначим как $\mathbf{T}(\boldsymbol{j})$.

Очередная последовательность бит $\mathbf{T}(\boldsymbol{j})$ разделяется на две последовательности **B** и **A** по 32 бита (правый и левый блоки). Далее выполняется итеративный процесс шифрования описываемый следующими формулами, вид который зависит от $\boldsymbol{i}$:

- Для $\boldsymbol{i}$=1, 2, ..., 24, $\boldsymbol{j}$=($\boldsymbol{i}$-1) mod 8;

$$\mathbf{A}(\boldsymbol{i}) = \boldsymbol{f}(\mathbf{A}(\boldsymbol{i}\text{-}1)\ [+]\ \boldsymbol{x}(j)) \oplus \mathbf{B}(\boldsymbol{i}\text{-}1)$$
$$\mathbf{B}(\boldsymbol{i}) = \mathbf{A}(\boldsymbol{i}\text{-}1)$$

- Для i=25, 26, ..., 31, j=32-i;

$$\mathbf{A}(i) = f(\mathbf{A}(i\text{-}1)\ [+]\ x(j)) \oplus \mathbf{B}(i\text{-}1)$$
$$\mathbf{B}(i) = \mathbf{A}(i\text{-}1)$$

- Для i=32

$$\mathbf{A}(32) = \mathbf{A}(31)$$
$$\mathbf{B}(32) = f(\mathbf{A}(31)\ [+]\ x(0)) \oplus \mathbf{B}(31).$$

Здесь i обозначает номер итерации. Функция f – функция шифрования, включающая две операции над 32-разрядным аргументом.

Первая операция является подстановкой K. Блок подстановки K состоит из 8 узлов замены $K(1)...K(8)$ с памятью 64 бита каждый. Поступающий на блок подстановки 32-разрядный вектор разбивается на 8 последовательно идущих 4-разрядных вектора, каждый из который преобразуется в 4-разрядный вектор соответствующим узлом замены, представляющим из себя таблицу из 16 целых чисел в диапазоне 0...15. Входной вектор определяет адрес строки в таблице, число из которой является выходным вектором. Затем 4-разрядные векторы последовательно объединяются в 32-разрядный выходной.

Вторая операция - циклический сдвиг влево 32-разрядного вектора, полученного в результате подстановки К. 64-разрядный блок зашифрованных данных T представляется в виде:

$$T=\mathbf{A}(32)\mathbf{B}(32).$$

Остальные блоки открытых данных в режиме простой замены зашифровываются аналогично.

Следует учитывать, что данный режим шифрования обладает ограниченной криптостойкостью.

Другой режим шифрования называется *режимом гаммирования*.

Открытые данные, разбитые на 64-разрядные блоки $T(i)$ (i=1,2,...,m) (m определяется объемом шифруемых данных), зашифровываются в режиме гаммирования путем поразрядного сложения по модулю 2 с гаммой шифра $\Gamma_ш$, которая вырабатывается блоками по 64 бит, т.е.

$$\Gamma_ш=(\Gamma(1),\Gamma(2),....,\Gamma(m)).$$

Уравнение шифрования данных в режиме гаммирования может быть представлено в следующем виде:

$$\mathbf{Ш}(i)=\mathbf{A}(Y(i\text{-}1) \oplus \mathbf{C}2,\ \mathbf{Z}(i\text{-}1))\ \{+\}\ \mathbf{C}1 \oplus T(\mathrm{i})=\Gamma(i) \oplus T(i)$$

В этом уравнении $\mathbf{Ш}(i)$ обозначает 64-разрядный блок зашифрованного текста, **A** - функцию шифрования в режиме простой замены (аргументами этой функции являются два 32-разрядных числа). **C**1 и **C**2 - константы, заданные в ГОСТ 28147-89. Величины $y(i)$ и $\mathbf{Z}(i)$ определяются итерационно по мере формирования гаммы следующим образом:

$(\mathbf{Y}(0),\mathbf{Z}(0))=\mathbf{A}(\mathbf{S})$, **S** - 64-разрядная двоичная последовательность

$(\mathbf{Y}(i),Z(i))=(\mathbf{Y}(i\text{-}1)\ [+]\ \mathbf{C}2,\ \mathbf{Z}(i\text{-}1)\ \{+\}\ \mathbf{C}(1))$, i=1, 2, ..., m.

64-разрядная последовательность, называемая синхропосылкой, не является секретным элементом шифра, но ее наличие необходимо как на передающей стороне, так и на приемной.

Режим гаммирования с обратной связью очень похож на режим гаммирования. Как и в режиме гаммирования открытые данные, разбитые на 64-разрядные блоки $\mathbf{T}(i)$, зашифровываются путем поразрядного сложения по модулю 2 с гаммой шифра $\Gamma_ш$, которая вырабатывается блоками по 64 бит:

$$\Gamma_ш=(\Gamma(1), \Gamma(2), ..., \Gamma(m)).$$

Уравнение шифрования данных в режиме гаммирования с обратной связью выглядят следующим образом:

$$\mathbf{Ш}(1)=\mathbf{A}(\mathbf{S})\oplus\mathbf{T}(1)=\Gamma(1)\oplus T(1),$$
$$\mathbf{Ш}(i)=\mathbf{A}(\mathbf{Ш}(i\text{-}1)\oplus\mathbf{T}(i)=\Gamma(i)\oplus\mathbf{T}(i),\ i=2, 3, ..., m.$$

Следует отметить, что в отличие от DES, у ГОСТ 28147-89 блок подстановки можно произвольно изменять, то есть он является дополнительным 512-битовым ключом.

В ГОСТ 28147-89 определяется процесс выработки имитовставки, который единообразен для всех режимов шифрования. Имитовставка - это блок из p бит (имитовставка $И_р$), который вырабатывается либо перед шифрованием всего сообщения. либо параллельно с шифрованием по блокам. Параметр p выбирается в соответствии с необходимым уровнем имитозащищенности.

Для получения имитовставки открытые данные представляются также в виде блоков по 64 бит. Первый блок открытых данных $\mathbf{T}(1)$ подвергается преобразованию, соответствующему первым 16 циклам алгоритма режима простой замены. Причем в качестве ключа используется тот же ключ, что и для шифрования данных. Полученное 64-разрядно число суммируется с открытым блоком $\mathbf{T}(2)$ и сумма вновь подвергается 16 циклам шифрования для режима простой замены. Данная процедура повторятся для всех m блоков сообщения. Из полученного 64-разрядного числа выбирается отрезок $И_р$ длиной p бит.

Имитовставка передается по каналу связи после зашифрованных данных. На приемной стороне аналогичным образом из принятого сообщения выделяется имитовставка и сравнивается с полученной ранее. В случае несовпадения имитовставок сообщение считается ложным.

5.8 Блочные шифры

Блочные алгоритмы шифрования являются основным средством криптографической защиты информации, хранящейся на компьютере пользователя или передаваемой по общедоступной сети передачи информации. Столь пристальное внимание к данному типу алгоритмов шифрования обусловлено не только их многолетней историей, а преимущества-

ми их практического (по сравнению с асимметричными алгоритмами шифрования) применения, среди которых следует отметить:

- Возможность эффективной программной реализации на современных аппаратно-программных средствах
- Высокая скорость шифрования/расшифрования как при аппаратной, так и при программной реализации
- Высокая гарантированная стойкость, причем стойкость алгоритма блочного шифрования может быть доказана при помощи математического аппарата.

Входная последовательность блочных алгоритмов шифрования разбивается на блоки определенной длины (обычно 64 бита для удобства реализации на процессорах с внутренними регистрами длиною 32 или 64 бита) и преобразования совершаются в алгоритме блочного шифрования над каждым блоком отдельно. Соответственно выходная последовательность алгоритма блочного шифрования представляет из себя блоки, у которых длина равна длине входных блоков. В случае если длина открытого текста не кратна длине входных блоков в алгоритме шифрования, то применяется операция дополнения (padding) последнего блока открытого текста до необходимой длины. Дополнение осуществляется приписыванием необходимого числа нулей либо случайного набора символов, в общем случае содержание того, чем мы дополняем блок открытого текста не играет роли с точки зрения криптографической стойкости. На приемной стороне необходимо знать какое количество символов было добавлено, для этого на приемной стороне вместе с данными дополнения приписывается длина этих данных.

Суть алгоритмов блочного шифрования заключается в применении к блоку открытого текста многократного математического преобразования. Многократность применения обуславливает то, что результирующее преобразование оказывается криптографически более сильным, чем само преобразование. Основная цель осуществляемых преобразований - это создать зависимость каждого бита блока зашифрованного сообщения от каждого бита ключа и каждого бита блока открытого сообщения. Преобразования, лежащие в основе данных алгоритмов можно разделить на "сложные" преобразования, в современных алгоритмах это обычно нелинейные операции, и "простые" преобразования, в основе которых лежат перемешивающие операции. Аналитическая сложность раскрытия алгоритмов блочного шифрования лежит в основном на конструкции первого типа преобразований.

Специфика организации различных типов секретной связи обусловила появление следующих типов использования алгоритмов блочного шифрования:

- Режим простой замены или режим электронной кодовой книги (Electronic Codebook Mode - ECB)
- Режим гаммирования

- Режим гаммирования с самовостановлением или шифрование с обратной связью (Cipher-Feedback mode - CFB)
- Режим гаммирования с обратной связью по выходу (Output-Feedback mode - OFB)
- Режим шифрования со сцеплением блоков (Cipher Block Chaining mode - CBC)

Блочные шифры бывают двух основных видов:

- шифры перестановки (transposition, permutation, P-блоки);
- шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок и шифры замены были рассмотрены выше.

Блочное шифрование можно осуществлять двояко:

1. Без обратной связи (ОС). Несколько битов (блок) исходного текста шифруются одновременно, и каждый бит исходного текста влияет на каждый бит шифртекста. Однако взаимного влияния блоков нет, то есть два одинаковых блока исходного текста будут представлены одинаковым шифртекстом. Поэтому подобные алгоритмы можно использовать только для шифрования случайной последовательности битов (например, ключей). Примерами являются DES в режиме ECB и ГОСТ 28147-89 в режиме простой замены.

2. С обратной связью. Обычно ОС организуется так: предыдущий шифрованный блок складывается по модулю 2 с текущим блоком. В качестве первого блока в цепи ОС используется инициализирующее значение. Ошибка в одном бите влияет на два блока - ошибочный и следующий за ним. Пример - DES в режиме CBC.

Генератор ПСЧ может применяться и при блочном шифровании:

1. Поблочное шифрование потока данных. Шифрование последовательных блоков (подстановки и перестановки) зависит от генератора ПСЧ, управляемого ключом.

2. Поблочное шифрование потока данных с ОС. Генератор ПСЧ управляется шифрованным или исходным текстом или обоими вместе.

Блочные алгоритмы могут использоваться и для выработки гаммы. В этом случае гамма вырабатывается блоками и поблочно складывается по модулю 2 с исходным текстом. В качестве примера можно назвать B-Crypt, DES в режимах CFB и OFB, ГОСТ 28147-89 в режимах гаммирования и гаммирования с обратной связью.

6.КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

6.1. ОДНОСТОРОННИЕ ФУНКЦИИ

Одним из центральных понятий криптосистем с открытым ключом является понятие односторонней функции.

Односторонней функцией называется функция заданная на множестве **X** и областью значений в множестве **Y**, т.е. $f: \mathbf{X}\to\mathbf{Y}$, обладающая двумя свойствами:

1. Существует полиномиальный алгоритм вычисления $f(x)$.
2. Не существует полиномиальный алгоритм инвертирования функции $f(x)$, т.е. решения уравнения $f(x)=y$ относительно y.

Отметим, что для односторонней функции характерна сложность вычислений и инвертирования. Вопрос о существовании односторонних функций пока открыт, т.к. нынешнее состояние знаний не позволяет нам доказать, что однонаправленные функции вообще существуют. Однако, несмотря на это, имеются кандидаты среди функций, эффективное вычисление которых мы знаем, тогда как никаких эффективных алгоритмов их обращения (во всяком случае среди общедоступных) неизвестно.

Первым примером кандидата на однонаправленную функцию является умножение в кольце целых чисел **Z**. Это объясняется тем, что умножать даже очень большие числа относительно нетрудно. В то время как даже самый мощный компьютер не в состоянии быстро (за полиномиальное время) разложить на множители с наилучшим имеющимся в его распоряжении алгоритмом тысячазначное целое число, являющееся произведением двух примерно одинакового размера простых чисел.

Другим важным примером кандидата на однонаправленную функцию является модульное возведение в степень или модульное экспонирование в кольце классов вычетов по модулю n - $\mathbf{Z}_n$. Пусть $a,m\in\mathbf{Z}$. Тогда модульное возведение в степень m (относительно основания a и модуля n) это такая функция $f[a,n]$: $\mathbf{Z}_n\to\mathbf{Z}_n$, определяемая как $f[a,n](m)=a^m \bmod(n)$. Сразу не очевидно, что такую функцию можно вычислить эффективно, когда длина каждого из трех параметров a, n и m составляет несколько сотен знаков. То, что это возможно, и в самом деле так, показывает следующий пример.

Пример 62. $x^{49}=((((x^2*x)^2)^2)^2)^2*x$ ♦

Пример 62 показывает, как можно вычислить x^{49} с помощью лишь пяти возведений в квадрат и еще двух умножений. При вычислении $a^m \bmod(n)$ приведение по модулю n желательно делать после каждого возведения в квадрат и каждого умножения, чтобы избежать получения очень больших целых чисел.

По аналогии с действительным анализом обратная операция в $\mathbf{Z}_n$ известна как задача дискретного логарифмирования: даны целые числа a,

n и x, требуется найти такое целое m (если оно существует), что $a^m \bmod(n) = x$. Например, $18^{16} \bmod(43) = 9$. Здесь 16 является дискретным логарифмом 9 с основанием 18 по модулю 43. Можно проверить, что число 3 вообще не имеет логарифма с основанием 5 по модулю 21.

Несмотря на то, что вычисление больших модульных экспонент может быть осуществлено эффективно, в настоящее время неизвестно ни одного алгоритма для вычисления дискретных логарифмов больших чисел за приемлемое время даже на самых быстродействующих компьютерах.

При этом, хотя и не доказано, что таких алгоритмов вообще не существует, имеется предположение, что модульное возведение в степень действительно является однонаправленной функцией.

Очевидно, что однонаправленные функции не могут непосредственно использоваться в качестве криптосистем (когда m шифруется как $f(m)$, поскольку тогда даже законный получатель не сможет расшифровать полученное сообщение. Но тем не менее, такие функции могут быть полезны для защиты паролей.

Более употребимым понятием в криптографии является понятие *функции с секретом*. Иногда еще употребляется термин *функция с ловушкой*. Функцией с секретом K называется функция $f_K : \mathbf{X} \to \mathbf{Y}$, зависящая от параметра K и обладающая тремя свойствами:

1. При любом K существует полиномиальный алгоритм вычисления значений $f_K(x)$;
2. При неизвестном K не существует полиномиального алгоритма инвертирования $f_K(x)$.
3. При известном K существует полиномиальный алгоритм инвертирования $f_K(x)$.

Про существование функций с секретом можно сказать то же самое, что сказано про односторонние функции. Для практических целей криптографии было построено несколько функций, которые могут оказаться функциями с секретом. Для них свойство 2) пока строго не доказано, но считается, что задача инвертирования эквивалентна некоторой давно изучаемой трудной математической задаче.

Первый кандидат на однонаправленную функцию с секретом похож на нашего второго кандидата на просто однонаправленную функцию: модульное возведение в степень с фиксированной экспонентой и модулем. Пусть $m,n \in \mathbf{Z}$. Тогда модульное возведение в степень (относительно экспоненты m и модуля n) есть функция $g[m,n]$: $\mathbf{Z}_n \to \mathbf{Z}_n$, определена следующим образом: $g[m,n](a) = a^m \bmod(n)$.

Необходимо понимать различия между функциями $f[a,n]$ и $g[m,n]$.

Опять по аналогии с действительным анализом, операция обратная $g[m,n]$ известна под названием взятия корня m-той степени из x по модулю n: даны целые числа m, n и x. Требуется найти такое целое a(если оно существует), что $a^m \bmod(n) = x$. Например, 18 это корень 16-ой степени из

9 по модулю 43, так как $18^{16} \bmod(43) = 9$. Очевидно, что 25 также является корнем 16-ой степени из 9 по модулю 43.

В противоположность задаче дискретного логарифмирования, тем не менее, известно, что существует также и эффективный алгоритм взятия корня ***m***-ой степени из ***x*** по модулю ***n*** (или выяснения, что его не существует) для любого заданного ***x***. Любопытный феномен заключается в том, что неизвестно, как построить этот эффективный алгоритм при заданных лишь ***m*** и ***n***. Другими словами, функция ***g***[***m***,***n***] в действительности не является однонаправленной, поскольку мы знаем, что она может быть эффективно обращена. Но, несмотря на этот факт, мы не знаем, как это сделать.

Тем не менее, легко построить эффективный алгоритм вычисления ***m***-ого корня по модулю ***n*** при условии, что известно разложение ***n*** на простые множители. Именно по этой причине ***g***[***m***,***n***] и является кандидатом на однонаправленную функцию с секретом, для которой ***m*** и ***n*** используются как открытая информация, тогда как разложение служит в качестве секрета ***K***.

Применение функций с секретом в криптографии позволяет:
1) организовать обмен шифрованными сообщениями с использованием только открытых каналов связи, т.е. отказаться от секретных каналов связи для предварительного обмена ключами;
2) включить в задачу вскрытия шифра трудную математическую задачу и тем самым повысить обоснованность стойкости шифра;
3) решать новые криптографические задачи, отличные от шифрования (цифровая подпись и др.).

6.2. ГЕНЕРАЦИЯ КЛЮЧЕЙ

В 1976 году американцы Уитфилд Диффи и Мартин Хеллман (Diffi W., Hellman M.) в статье "Новые направления в криптографии" предложили новый принцип построения криптосистем, не требующий не только передачи ключа принимающему сообщение, но даже сохранения в тайне метода шифрования. Этот метод получил название “метод экспоненциального ключевого обмена” и является первой криптосистемой с открытым ключом. Метод запатентован, но срок действия патента истек 29 апреля 1997 года. Рассмотрим его основные положения.

Пусть абоненты ***A*** и ***B*** условились организовать секретную переписку между собой используя секретный ключ сгенерированный при помощи алгоритма Диффи–Хеллмана. Для этого они вместе выбирают два достаточно больших простых числа ***n*** и ***q*** так, чтобы ***q*** было примитивным элементом в GF(***n***). Эти два числа необязательно хранить в секрете. Абоненты ***A*** и ***B*** могут передать эти числа по открытому каналу связи. Затем абоненты реализуют следующий алгоритм.

1 ***A*** выбирает случайное большое целое число α, вычисляет $x=q^{\alpha} \bmod n$ и посылает ***B*** число ***x***.
2 ***B*** выбирает случайное большое целое число β, вычисляет $y=q^{\beta} \bmod n$ и посылает ***A*** число ***y***.
3 ***A*** вычисляет $k_1=y^{\alpha} \bmod n$.
4 ***B*** вычисляет $k_2=x^{\beta} \bmod n$.

В итоге ***A*** и ***B*** получили такие числа, что $k_1=k_2=q^{\alpha\beta} \bmod n$. Никто из злоумышленников, имеющих доступ к этому открытому каналу не может определить эти значения, так как им известны ***n***, ***q***, ***x*** и ***y***, но неизвестны α и β. Для получения α и β необходимо вычислить дискретный логарифм, что является трудной в вычислительном плане задачей. Таким образом, величина $k=k_1=k_2$ может являться секретным ключом, который ***A*** и ***B*** вычислили независимо. В данном алгоритме выбор ***n*** и ***q*** существенно влияет на криптостойкость.

Пример 63. Пусть абоненты ***A*** и ***B*** условились организовать секретную переписку между собой используя секретный ключ сгенерированный при помощи алгоритма Диффи–Хеллмана. Тогда они вместе выбирают числа $n=67$ и $q=11$. Затем

1. ***A*** выбирает случайное целое число $\alpha=47$, вычисляет $x=q^{\alpha} \bmod n = 11^{47} \bmod 67 = 2$ и посылает ***B*** число 2.
2. ***B*** выбирает случайное целое число $\beta=51$ вычисляет $y=q^{\beta} \bmod n = 11^{51} \bmod 67 = 3$ и посылает ***A*** число 3.
3. ***A*** вычисляет $k_1=y^{\alpha} \bmod n = 3^{47} \bmod 67 = 27$
4. ***B*** вычисляет $k_2=x^{\beta} \bmod n = 2^{51} \bmod 67 = 27$

В итоге А и В получили секретный ключ $k= k_1= k_2=27$. ♦

Пример 64. А теперь рассмотрим похожий пример, но с большими числами, а именно $n=$1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541618443187 и $q=$49800579826409539765001781692627092282535544714523695034061649412796239935953073850781054161808534613. Тогда

1. ***A*** выбирает случайное целое число $\alpha=$1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541618443136 7 вычисляет $x=q^{\alpha} \bmod n =$4980057982640953976500178169262709228253554471452369503406164941279623993595307385078105416180853461$^{1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541618443136 7}$ $\bmod$ 1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541618443087 7=1707898771420490189036182320364824629870888864570628383436341394008976949807175044603463218465795703 6 и посылает ***B*** число ***x*** .
2. ***B*** выбирает случайное целое число $\beta=$4374501449566023848745004454235242730706338861786424872851541212819905998398751846447026354046454419 вычисляет $y=q^{\beta} \bmod n =$4980057982640953976500 1

781692627092282535544714523695034061649412796239935953073850781054161808534614374501449566023848745004454235242730706338861786424872851541 2128199059983987518464470263540464544 19 **mod** 1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541 6184430877 = 9446043995490484971892239232298678418450409052905625061872522661677845494058935332443487281531990777 и посылает ***A*** число ***y***.

3. ***A*** вычисляет $k_1=y^{\alpha}$ **mod** n =9446043995490484971892239232298678418450409052905625061872522661677845494058935332443487281531990777 0777^{1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541616184431367} **mod** 1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541616184430877 = 1203419001139627736370826683447563462740343725027845634563745588 93324663431303085275268329152545940 34
4. ***B*** вычисляет $k_2=x^{\beta}$ **mod** n =1707898771420490189036182320364824629870888864570628383436341394008976949807175044603463218465795 7036^{4374501449566023848745004454235242730706338861786424872851541212819905998398751846447026354046454419} **mod** 1749800579826409539498001781694097092282535544714569949140616485127962399359500738578810541616184430877 =1203419001139627736370826683447563462740343725027845634563745588933246634313030852752683291525459403 4.

В итоге А и В получили секретный ключ $k= k_1= k_2$=1203419001139627736370826683447563462740343725027845634563745589933246634313030852752683291525459403 4. ♦

Без дополнительных мер безопасности (введения сертификатов открытых ключей), рассмотренный метод ключевого обмена уязвим с точки зрения атаки, известной под названием “человек посередине” (main in the midlle attact).

Предположим, что злоумышленник **C** может не только подслушивать сообщения между **A** и **B**, но также изменять, удалять и создавать новые ложные сообщения. Тогда **C** может выдавать себя за **A**, что сообщающего **B**, и за **B**, что сообщающего **A**. Атака состоит в следующем:

1. **A** посылает **B** свой открытый ключ. **C** перехватывает его и посылает **B** свой собственный открытый ключ.
2. **B** посылает **A** свой открытый ключ. **C** перехватывает его и посылает **A** свой собственный открытый ключ.
3. Когда **A** посылает сообщения **B**, зашифрованное на его открытом ключе, **C** перехватывает его. Т.к. сообщение в действительности зашифровано на открытом ключе **C**, он расшифровывает его, снова зашифровывает его на открытом ключе **B** и посылает **B**.
4. Когда **B** посылает сообщения **A**, зашифрованное на его открытом ключе, **C** перехватывает его. Так как сообщение в действительности зашифровано на открытом ключе **C**, он расшифровывает его, снова зашифровывает его на открытом ключе **A** и посылает **A**.

Атака возможна, даже если открытые ключи **A** и **B** и хранятся в БД. Злоумышленник **C** может перехватить запрос **A** к БД и подменить открытый ключ. Данная атака очень эффективна. Открытые ключи должны проходить сертификацию, чтобы предотвратить подобные атаки, связанные с подменой ключей и должны регулярно меняться.

6.3. ОСНОВНЫЕ ПОЛОЖЕНИЯ КРИПТОСИСТЕМЫ RSA

В 1978 г. Рональд Ривест, Ади Шамир и Леонард Адлеман (R.Rivest, A.Shamir, L.Adleman) предложили пример функции, обладающей рядом замечательных свойств. На ее основе была построена реально используемая система шифрования, получившая название по первым буквам фамилий авторов – система RSA. Рассмотрим ее основные положения на примере криптосистемы с открытым ключом.

Теоретические положения построения криптографических систем с открытым ключом в основном базируются на следующих фактах:

1 Кольцо целых чисел является факториальным (см. теорему 14). Но задача разложения больших чисел на простые множители за полиномиальное время не разрешима.
2 Задача вычисление логарифма за полиномиальное время не разрешима.
3 Следствие теоремы 10.
4 Функции Эйлера (см. п.2.5)

Приведем общую схему алгоритма RSA. Пусть абоненты A и B условились организовать секретную переписку между собой с открытым ключом. Тогда каждый из них, независимо от другого, выбирает два достаточно больших простых числа, находит их произведение, функцию Эйлера от этого произведения и выбирает случайное число, меньшее этого вычисленного значения функции Эйлера и взаимно простое с ним. Итак,

$$A: p_1, p_2,\ r_A = p_1 p_2,\ \varphi(r_A),\ \text{НОД}(a, \varphi(r_A)) = 1,\ 0 < a < \varphi(r_A),$$
$$B: q_1, q_2,\ r_B = q_1 q_2,\ \varphi(r_B),\ \text{НОД}(b, \varphi(r_B)) = 1,\ 0 < b < \varphi(r_B).$$

Затем печатается телефонная книга, доступная всем желающим, которая имеет вид:

A: r_A,a
B: r_B,b

r_A – произведение двух простых чисел, известных только A, a – открытый ключ, доступный каждому, кто хочет передать секретное сообщение A, r_B – произведение двух простых чисел, известных только B. b – открытый ключ, доступный каждому, кто хочет передать секретное сообщение B.

Каждый из абонентов находит свой секретный ключ из сравнений $a \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(r_A))$, $0 < \alpha < \varphi(r_A)$, $b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_B))$, $0 < \beta < \varphi(r_B)$.

Итак,

Абонент	Открытые ключи	Секретные ключи
A	r_A, a	α
B	r_B, b	β

Пусть абонент A решает послать сообщение m абоненту B:

A: $m \to B$ и пусть $0 < m < r_B$, иначе текст делят на куски длины меньше r_B. Сначала A зашифровывает сообщение открытым ключом абонента B, который есть в телефонной книге, и находит:

$$m_1 \equiv m^b (\mathbf{mod}\ r_B),\ 0 < m_1 < r_B,$$

и отправляет абоненту B. Абонент B, расшифровывает это сообщение своим секретным ключом:

$$m_2 \equiv m_1^{\beta} (\mathbf{mod}\ r_B),\ 0 < m_2 < r_B,$$

и получает $m_2 = m$.

В самом деле: $m_2 \equiv m_1^{\beta} \equiv (m^{\beta})^b \equiv m^{b\beta} (\mathbf{mod}\ r_B)$.

Но $b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_B))$, следовательно $m_2 \equiv m (\mathbf{mod}\ r_B)$. Но так как $0 < m < r_B$, $0 < m_2 < r_B$ то $m_2 = m$.

Пример 65. Пусть абоненты **A** и **B** решили установить между собой скрытую связь с открытым ключом.

Абонент **A** выбрал простые числа p_1=7643 и p_2=8753, их произведение r_A=66899179, функцию Эйлера $\varphi(r_A) = p_1 p_2 (1-1/p_1)(1-1/p_2)$=66882784. Затем он выбирает случайное число a=9467 (открытый ключ) и находит секретный ключ из решения сравнения: $a \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(r_A))$=$9467 \cdot \alpha \equiv 1 (\mathbf{mod}$ 66882784), $0 < \alpha < \varphi(r_A)$, т.е. α=30993427.

Абонент **B** выбрал простые числа q_1=7481 и q_2=9539, их произведение r_B=71361259, функцию Эйлера $\varphi(r_B) = r_B(1-1/q_1)(1-1/q_2)$=71344240. Затем он выбирает случайное число b=74671 (открытый ключ) и находит секретный ключ из решения сравнения: $b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_B))$=$74671 \cdot \beta \equiv 1 (\mathbf{mod}$ 71344240), $0 < \beta < \varphi(r_B)$, т.е. β=33289711.

Таким образом, имеется следующая таблица:

Абонент	Открытые ключи	Секретные ключи
A	66899179, 9467	30993427
B	71361259, 74671	33289711

Абонент **A** решает послать сверхсекретное сообщение абоненту **B** m=95637. Тогда он шифрует сообщение открытым ключом абонента **B**:

$$m_1 \equiv m^b (\mathbf{mod}\ r_B) = 95637^{74671} (\mathbf{mod}\ 71361259) = 25963634.$$

Абонент **B**, получив это сообщение, расшифровывает его своим секретным ключом:

$$m_2 \equiv m_1^{\beta} (\mathbf{mod}\ p) = 25963634^{33289711} (\mathbf{mod}\ 71361259) = 95637. \blacklozenge$$

Пример 66. А теперь рассмотрим похожий пример, но с большими числами, а именно: p_1=7643 и p_2=8753, их произведение r_A=66899179, $\varphi(r_A) = p_1 p_2 (1-1/p_1)(1-1/p_2)$=66882784, a=9467 и α=30993427. Далее, q_1=17014118346046923173168730371588410572 7, q_2=1035079443105516238671861923746823456 9, b=1826877046663628647754606040895353774569915678 71. Тогда имеем: r_B=17610964142557596262140073765579909937745937199933968196397372400446799363 68. Находим секретный ключ из решения сравнения: $b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_B))$

=18268770466636286477546060408953537745699156787 1·β≡1(**mod** 176109641425575962621400737655799099377459371999339681963973724004467 9936368), 0<β<φ(r_B), т.е. β=16513586832236884205611880099558235975948478079538542594781799059818797301 11.

Таким образом имеется таблица:

Абонент	Открытые ключи	Секретные ключи
A	66899179, 9467	30993427
B	176109641425575962621400737655799099395508 569788492121375814316299803227666 3, 18268770466636286477546060408953537745699 1567871	16513586832236884205611880099558235975948478079538542594781799059818797301 11

Абонент **A** решает послать сверхсекретное сообщение абоненту **B** m=95637123523488976723896413962186095671 72. Тогда он шифрует сообщение открытым ключом абонента **B**: $m_1 \equiv m^b (\mathbf{mod}\ r_B)$=9563712352348897672389641396218609567172$^{18268770466636286477546060408953537745699156787 1}$(**mod** 176109641425575962621400737655799099395508569788492121375814316299803227666 3)=83255471600987219023332593780878672784122613750592044594478223942973656948.

Абонент **B**, получив это сообщение, расшифровывает его своим секретным ключом: $m_2 \equiv m_1^{\beta} (\mathbf{mod}\ p)$=83255471600987219023332593780878672784122613750592044594478223942973656948$^{16513586832236884205611880099558235975948478079538542594781799059818797301 11}$(**mod** 176109641425575962621400737655799099395508569788492121375814316299803227666 3)=95637123523488976723896413962186095671 72.♦

6.4. НАДЕЖНОСТЬ СИСТЕМЫ RSA

В рассмотренной криптосистеме с открытым ключом для расшифровки сообщения m необходимо найти секретный ключ β. Это возможно в двух случаях:

1) если известно разложение r_B на простые множители;
2) если известен модуль φ(r_B) сравнения $b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_B))$.

Но так как $r_B = q_1 q_2$, то $\varphi(r_B) = \varphi(q_1)\varphi(q_2) = (q_1-1)(q_2-1) = q_1 q_2 - (q_1+q_2)+1$ и $(q_1-q_2)^2 = q_1^2 + q_2^2 - 2q_1q_2 = (q_1+q_2)^2 - 4q_1q_2$.

Следовательно, мы имеем равенства:

$$\varphi(r_B) = r_B - (q_1+q_2)+1,$$
$$(q_1-q_2)^2 = (q_1+q_2)^2 - 4q_1q_2,$$

а значит, зная φ(r_B), можно решить эту систему и найти q_1 и q_2, а зная q_1 и q_2, легко вычислить φ(r_B). Таким образом, оба подхода определения ключа β эквивалентны, т.е. задачи одной сложности. Таким образом, встает задача разложения на простые множители натурального числа.

В теории чисел, несмотря на ее многолетнюю историю и на очень интенсивные поиски в течение последних 30 лет, эффективный алгоритм разложения натуральных чисел на множители так и не найден. Конечно, можно, перебирая все простые числа до $(r_B)^{1/2}$, и деля на них r_B, найти требуемое разложение. Но учитывая, что количество простых чисел в этом промежутке асимптотически равно $2\cdot(r_B)^{1/2}\cdot(\ln r_B)^{-1}$, находим, что при r_B, записываемом 1000 десятичными цифрами, найдется не менее 10^{497} простых чисел, на которые придется делить r_B при разложении его на множители, что при современных возможностях вычислительной техники затянется на долгие годы.

Известны и более эффективные алгоритмы разложения целых чисел на множители, чем простой перебор простых делителей, но и они работают очень медленно.

Необходимо также отметить, что система RSA обладает *мультипликативным* свойством. Поясним сказанное. Пусть m_1 и m_2 - 2 различных открытых текста, а c_1 и c_2 - соответствующие им шифртексты. Заметим, что

$$(m_1m_2)^{\alpha}= m_1{}^{\alpha}m_2{}^{\alpha}= c_1c_2(\mathbf{mod}\ n).$$

Другими словами, шифртекст открытого текста $m=m_1m_2$ есть $c= c_1c_2(\mathrm{mod}\ n)$. Это свойство, называемое также *гомоморфным свойством* RSA, позволяет осуществить атаку по выбранному шифртексту. Его нужно учитывать при совмещении схем шифрования на основе RSA и цифровой подписи RSA.

Кроме того, известно еще несколько атак на RSA. Рассмотрим из них две.

Первая из них называется ”Метод безключевого чтения RSA”. Суть заключается в следующем.

Криптоаналитику известны открытый ключ (a, n) и шифротекст C. Тогда он подбирает такое число k, для которого выполняется следующее соотношение: $C^{ak}(\mathbf{mod}\ n)=C$. Т.е. криптоаналитик просто проводит k раз зашифрование на открытом ключе перехваченного шифротекста. Это выглядит следующим образом: $(((C^a)^a)^a\ldots)^a=C^{ak}=C^{\varphi(n)-1}=C(\mathbf{mod}\ n)$. Найдя такое k, криптоаналитик вычисляет $C^k=m^{ak}=m^{\varphi(n)-1}=m(\mathbf{mod}\ n)$, т.е. получает открытый текст m.

Пример 67. Пусть абонент **A** хочет послать сообщение m=193263 абоненту **B**. **A** знает n=212887 и открытый ключ a=3061. Он зашифровывает сообщение открытым ключом, т.е. $m^a=193263^{3061}=C=$ 35947 и посылает это число в открытый канал связи. Таким образом, криптоаналитику становится известно сообщение C, модуль n и a. Далее криптоаналитик вычисляет $C^a(\mathbf{mod}\ n)=35947^{3061}(\mathbf{mod}\ 212887)$. Затем он находит такое k, чтобы выполнялось $C^{ak}=35947^{3061k}=35947=C$. Получили k=1084. И, наконец, вычисляем $C^k=35947^{1084}=193263$. ♦

Следующая атака осуществляется на базе общего модуля. Основные предпосылки для ее осуществления заключаются в следующем.

При реализации RSA можно раздать всем абонентам криптосети одинаковый модуль n, но каждому свои значения a_i(открытый ключ) и α_I (секретный ключ). При этом наиболее очевидная проблема заключается в том, что если одно и то же сообщение когда-нибудь шифровалось разными a_i и a_k, причем НОД(a_i,a_k)=1 (как обычно и бывает), то открытый текст может быть раскрыт даже при неизвестных α_i и α_k.

Таким образом, пусть заданы: m – сообщение, a и b – два открытых ключа шифрования, n – модуль. Тогда щифротекстами являются $c_1 = m^a (\mathbf{mod}\ n)$ и $c_2 = m^b (\mathbf{mod}\ n)$. Криптоаналитику известны: n, a, b, c_1 и c_2. Далее, так как a и b взаимно – простые числа, то воспользовавшись результатами главы 4, можно найти такие целые числа x и y, что $ax + by = 1$. Тогда, возведя c_1 в степень x, а c_2 – в степень y, получим: $c_1^x c_2^y = (m^a)^x (m^b)^y = m^{ax+by} = m^1 = m$.

Пример 68. Пусть абонент **А** хочет послать сообщение m=237135 другим абонентам. **В**. Абоненту **А** даны n=399799 и открытый ключ a=4397. Он зашифровывает сообщение открытым ключом, т.е. $m^a = c_1 = 237135^{4397} = 268100 (\mathbf{mod}\ 399799)$ и посылает это число в открытый канал связи. Абонент **В** хочет также послать сообщение m=237135 другим абонентам. Для **В** даны n=399799 и открытый ключ b=7517. Он зашифровывает сообщение открытым ключом, т.е. $m^b = c_2 = 237135^{7517} = 263851$ (**mod** 399799) и также посылает это число в открытый канал связи. Таким образом, криптоаналитику известно: зашифрованные сообщения c_1 и c_2, модуль n, открытые ключи a и b. Далее криптоаналитик решает уравнение $ax+by=1=4397x+7517y$ и получает $x=-1607$ и y=940. Затем он возводит c_1 в степень $|x|$, т.е. $c_1^{|x|} = d_1 = 268100^{1607} = 12105 (\mathbf{mod}\ 399799)$, а c_2 в степень $|y|$, т.е. $c_2^{|y|} = d_2 = 263851^{940} = 362154 (\mathbf{mod}\ 399799)$. Так как $x<0$, то находится $(d_1)^{-1} = 12105^{-1} = 39501 (\mathbf{mod}\ 399799)$. (При $y<0$ искали бы $(d_2)^{-1}$). Далее, перемножая $(d_1)^{-1} * d_2 = 39501 * 362154 = 237135 (\mathbf{mod}\ 399799) = m$, т.е. получили открытый текст. ♦

6.5. ПРОБЛЕМЫ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ RSA

В настоящее время алгоритм RSA активно реализуется как в виде самостоятельных криптографических продуктов, так и в качестве встроенных средств в популярных приложениях.

Важнейшей проблемой практической реализации - *генерация больших простых чисел*. Решение задачи «в лоб» - генерация случайного большого числа n (нечетного) и проверка его делимости на множители от 3 вплоть до $n^{0.5}$. В случае неуспеха следует взять n+2 и так далее[1].

В принципе в качестве p и q можно использовать «почти» простые числа, то есть числа для которых вероятность того, что они простые, стремится к 1. Но в случае, если использовано составное число, а не простое,

[1] В теории чисел показано, что вероятность того, что число порядка n будет простым составляет $1/\ln n$

криптостойкость RSA падает. Имеются неплохие алгоритмы, которые позволяют генерировать «почти» простые числа с уровнем доверия 2^{-100}.

Поскольку простые числа должны выбираться таким образом, чтобы факторизовать их произведение было вычислительно невозможно, рекомендуется брать их очень большими и одинаковой длины. Так, для $n = pq$ длины 1024 бита, p и q должны быть длиной 512 бит.

Разность чисел p и q (p-q) также не должна быть маленькой, поскольку в этом случае $p \sim q$ и, следовательно, $p \sim (n)^{1/2}$. Таким образом, разложение n может быть найдено простым делением на все числа порядка $(n)^{1/2}$.

Кроме того, числа p и q должны быть также "устойчивыми" простыми числами.

Число p является *устойчивым* (*strong*), если оно удовлетворяет трем условиям:

1. p-1 имеет большой простой делитель, обозначим его как r (т.е. $p \equiv 1 (\mathrm{mod}\ r)$);
2. p+1 имеет большой простой делитель, обозначим как s (т.е. $p \equiv s-1 (\mathrm{mod}\ s)$);
3. r-1 имеет большой простой делитель, обозначим его как t (т.е. $r \equiv 1 (\mathrm{mod}\ t)$).

Условие 1 не позволит успешно факторизовать n (p-1) методом Полларда, который позволяет быстро разложить число n на множители, если его делитель p имеет небольшие (скажем, меньше миллиона) простые делители. Условие 2 позволит избежать p+1 метода Ульямса, позволяющего разложить n при условии, что p+1 имеет небольшие делители. Условие 3 позволит избежать метода безключевого чтения RSA (циклической атаки). Если p выбирается случайно и имеет довольно большой размер, то, как правило, p-1 и p+1 будут иметь большие простые делители. Однако выбор устойчивых простых чисел не защищает систему от атаки алгоритмом факторизации на основе эллиптических кривых.

Получить устойчивые простые числа можно следующим способом. Генерируем большие простые числа s и t. Затем получаем такое простое число r, что r-1 делится на t (для этого рассматриваем нечетные числа вида $r = kt+1$, где k - последовательные натуральные числа, и проверяем их на простоту, пока не найдем простое). Теперь, имея простые r и s, строим новое простое p. Для этого вычисляем $p = ((s^{r-1} - r^{s-1}) \bmod rs) + xrs$, где x – некоторое целое число и проверяя p на простоту, находим устойчивое простое число p.

Следующая проблема - какой длины ключи следует использовать?

Для практической реализации алгоритмов RSA полезно знать оценки трудоемкости разложения простых чисел различной длины, сделанные Шроппелем.

lg ***n***	Число операций	Примечания
50	$1.4*10^{10}$	Раскрываем на суперкомпьютерах
100	$2.3*10^{15}$	На пределе современных технологий
200	$1.2*10^{23}$	За пределами современных технологий
400	$2.7*10^{34}$	Требует существенных изменений в технологии
800	$1.3*10^{51}$	Не раскрываем

В конце 1995 года удалось практически реализовать раскрытие шифра RSA для 500-значного ключа. Для этого с помощью сети Интернет было задействовано 1600 компьютеров.

Сами авторы RSA рекомендуют использовать следующие размеры модуля ***n***:

- 768 бит - для частных лиц;
- 1024 бит - для коммерческой информации;
- 2048 бит - для секретной информации[1].

Третий немаловажный аспект реализации RSA - *вычислительный*, приходится использовать аппарат длинной арифметики. Если используется ключ длиной ***k*** бит, то для операций по открытому ключу требуется $O(k^2)$ операций, по закрытому ключу - $O(k^3)$ операций, а для генерации новых ключей требуется $O(k^4)$ операций.

По сравнению с тем же алгоритмом DES, RSA требует в тысячи и десятки тысяч раз большее время.

6.6. КРИПТОСИСТЕМА БЕЗ ПЕРЕДАЧИ КЛЮЧЕЙ

Пусть абоненты ***A, B, C,*** ... условились организовать секретную переписку между собой. Для этой цели они выбирают достаточно большое простое число ***p*** и такое, что ***p***-1 хорошо разлагается на не очень большие простые множители. Если среди множителей такого числа кратных нет, то число ***p***-1 называют *евклидовым*. Каждый из абонентов независимо один от другого выбирает случайное число, натуральное, взаимно простое с числом ***p***-1**:** ***A, B, C,*** ... – абоненты; ***a***, ***b***, ***c***, ... – выбранные ими случайные числа. Далее, абонент ***A*** находит число α из условия

$$a\cdot\alpha\equiv 1(\mathbf{mod}\ \varphi(p)),\ 0<\alpha<p-1; \qquad (8)$$

абонент ***B*** находит число β из условия

$$b\cdot\beta\equiv 1(\mathbf{mod}\ \varphi(p)),\ 0<\beta<p-1, \qquad (9)$$

где $\varphi(p)$ – функция Эйлера, ***a***, α – секретные ключи абонента ***A;*** ***b***, β – секретные ключи абонента ***B*** и т.д.

Пусть абонент ***A*** решает послать сообщение ***m*** абоненту ***B***. Можно предполагать, что $0 < m < p-1$. Тогда он сначала зашифровывает это сообщение своим первым секретным ключом, находит:

$$m_1\equiv m^a(\mathbf{mod}\ p),\ 0<m_1<p \qquad (10)$$

[1] Данные оценки сделаны с учетом развития вычислительной техники вплоть до 2004 года.

и отправляет абоненту ***B.*** Абонент ***B,*** в свою очередь, зашифровывает вновь это сообщение также своим первым ключом:

$$m_2 \equiv m_1^{\,b} (\mathbf{mod}\ p),\ 0 < m_2 < p \qquad (11)$$

и пересылает его обратно абоненту ***A.*** Абонент ***A,*** получив обратно свое дважды зашифрованное сообщение, шифрует его же в третий раз своим вторым ключом:

$$m_3 \equiv m_2^{\,\alpha} (\mathbf{mod}\ p),\ 0 < m_3 < p \qquad (12)$$

и вновь отправляет его абоненту ***B.*** Последний расшифровывает эту шифротелеграмму при помощи своего второго ключа:

$$m_4 \equiv m_3^{\,\beta} (\mathbf{mod}\ p),\ 0 < m_4 < p.$$

В самом деле, из сравнений (10) – (12) имеем:

$$m_4 \equiv m^{k} (\mathbf{mod}\ p),$$

где $k \equiv a \cdot \alpha \cdot b \cdot \beta (\mathbf{mod}\ p\text{-}1)$.

В силу (8) и (9) $k \equiv 1 (\mathbf{mod}\ \varphi(p))$. Поэтому $m_4 \equiv m (\mathbf{mod}\ p)$, а так как каждое из них положительно и меньше p, то $m_4 = m$.

Пример 69. Пусть абоненты **A** и **B** решили установить между собой скрытую связь без передачи ключей. Они выбрали для этого простое число p = 9551. Тогда p-1=9550.

Абонент **A** выбирает случайное число a=8159, а абонент **B** – b=7159. Абонент **A** решает сравнение: $8159 \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(9551))$, $0 < \alpha < 9550$ и находит α= 6639, а абонент **B** решает сравнение: $7159 \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(9551))$, $0 < \beta < 9550$ и находит β= 6139.

Абонент **A** решает послать секретное сообщение абоненту **B** m=7032. Тогда он сначала шифрует сообщение своим первым ключом: $m_1 \equiv m^{a} (\mathbf{mod}\ p) = 7032^{81593} (\mathbf{mod}\ 9551) = 153$.

Абонент **B**, получив это сообщение, шифрует его своим первым ключом: $m_2 \equiv m_1^{\,b} (\mathbf{mod}\ p) = 153^{7159} (\mathbf{mod}\ 9551) = 4896$, и пересылает его абоненту ***A***, который, получив зашифрованное сообщение, шифрует его же в третий раз своим вторым ключом: $m_3 \equiv m_2^{\,\alpha} (\mathbf{mod}\ p) = 4896^{6639} (\mathbf{mod}\ 9551) = 7577$ и отправляет его абоненту ***B***, который расшифровывает эту шифротелеграмму при помощи своего второго ключа: $m_4 \equiv m_3^{\,\beta} (\mathbf{mod}\ p) = 7577^{6139} (\mathbf{mod}\ 9551) = 7032$.♦

Пример 70. А теперь рассмотрим похожий пример, но с большими числами, а именно пусть абоненты **A** и **B** выбирают случайное число p =3618502788666131106986593281521497120414687020801267626233049500247285301313. Далее абонент **A** выбирает случайное число a=3291009114642412084309938365114247285301313, а абонент **B** – b=72133456729194312009114642445656781208430934647938365165454 65843. Абонент **A** решает сравнение: $3291009114642412084309938365114 7010099654717312671597266972181 19 \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(3618502788666131106 986593281521497120414687020801267626233049500247285301313))$, $0 < \alpha < 3618502788666131106986593281521497120414687020801267626233049500247285301312$ и находит α=7182890946724276712267540712060414209

9575840582862256961336950427223165477 5, а абонент **B** решает сравнение: 7213345672919431200911464244565678120843093464793836516545465843·β ≡1(**mod** φ(11972621413014756705924586149611790497021399392059391)), 0 < β < 1197262141301475670592458614961179049702139939205 9390 и находит β= 20507850089479826167721544736489099017840580106 89679595249365486507640220987.

Абонент **A** решает послать секретное сообщение абоненту **B** ***m***=164395308562370233597340474556219234532123890 86. Тогда он сначала шифрует сообщение своим первым ключом: $m_1 \equiv m^a (\mathbf{mod}\ p) =$ 164395308562370233597340474556219234532123890 86$^{32910091146424120843099383651147010099654717312671597266972181 19}$(**mod** 36185027886661311069865932815214971204146870208012676262330495002472853013 13)=2340488471726089607124556756264169338202290949701335616973062664572414115995.

Абонент **B**, получив это сообщение, шифрует его своим первым ключом: $m_2 \equiv m_1^b (\mathbf{mod}\ p) =$ 2340488471726089607124556756264169338202290949701335616973062664572414115995^{72133456729194312009114642445656781208430934647938365165454658433}(**mod** 36185027886661311069865932815214971204146870208012676262330495002472853013 13) =2008471523091061336918900208993851807662985672512619192514870979350742436070, и пересылает его абоненту ***A.*** Абонент ***A,*** получив зашифрованное сообщение, шифрует его же в третий раз своим вторым ключом: $m_3 \equiv m_2^{\alpha} (\mathbf{mod}\ p) =$ 2008471523091061336918900208993851807662985672512619192514870979350742436070$^{7182890946724276712267540712060414209957584058286225696133695042722316547 75}$(**mod** 3618502788666131106986593281521497120414687020801267626233049500247285301313) = 3374267956066404491443963921356203649752330364752225196611392536160948437196 и отправляет его абоненту ***B***, который расшифровывает эту шифротелеграмму при помощи своего второго ключа: $m_4 \equiv m_3^{\beta} (\mathbf{mod}\ p) =$ 3374267956066404491443963921356203649752330364752225196611392536160948437196$^{20507850089479826167721544736489099017840580106896795952493654865076402209 87}$(**mod** 3618502788666131106986593281521497120414687020801267626233049500247285301313)=16439530856237023359734047455621923453212389086♦

6.7. АЛГОРИТМ ЭЛЬ-ГАМАЛЯ

Поиски более эффективных систем открытого шифрования привели к тому, что в 1985 году Т.Эль-Гамаль (США) предложил алгоритм на основе возведения в степень по модулю большого простого числа ***p***. Криптоалгоритм не запатентован, но попадал под действие патента на метод ключевого обмена Диффи-Хеллмана.

В отличие от RSA, метод Эль-Гамаля основан на проблеме дискретного логарифма. Этим он и похож на алгоритм Диффи-Хелмана. Если возводить число в степень в конечном поле достаточно легко, то восстановить аргумент по значению (то есть найти логарифм) довольно трудно.

Рассмотрим схему алгоритма.

Основу системы составляют параметры p и n - числа, первое из которых - простое, а второе - целое.

Абонент **А** генерирует секретный ключ α и вычисляет открытый ключ $y = n^{\alpha} \bmod p$. Если абонент **Б** хочет послать **А** сообщение m, то он выбирает случайное число k, меньшее p и вычисляет:

$$y_1 = n^{k} \bmod p \text{ и}$$

$$y_2 = m \oplus y^{k},$$

где $\oplus$ - побитовое сложение по модулю 2.

Затем **Б** посылает (y_1, y_2) **А**.

А, получив зашифрованное сообщение, восстанавливает его:

$$m = (y_1^{\alpha} \bmod p) \oplus y_2.$$

Известен вариант схемы, когда операция $\oplus$ заменяется на умножение по модулю p. Это удобнее в том смысле, что в первом случае текст необходимо разбивать на блоки той же длины, что и число $y^{k} \bmod p$. Во втором случае этого не требуется. Значит можно обрабатывать блоки текста заранее заданной фиксированной длины меньшей, чем число p. Уравнение расшифровки в этом случае будет иметь вид:

$$m = y_2 / y_1^{k} \bmod p.$$

Пример 71. Пусть абоненты **А** и **В** решили установить между собой скрытую связь с открытым ключом на базе алгоритма Эль-Гамаля.

Абонент **А** выбрал простое число p=1125899906842679 и целое число n = 745819352812378.

Затем абонент **А** генерирует секретный ключ α = 725391906243661, и вычисляет открытый ключ $y = n^{\alpha} \bmod p$ =$745819352812378^{725391906243661} \bmod 1125899906842679$=1124568734648807 и передает числа p, n и y в открытый канал.

Пусть абонент **Б** хочет послать **А** сообщение m=4567345. Он выбирает случайное число k= 51394216073587 меньшее p и вычисляет: $\mathbf{y_1} = n^{k} \bmod p$ =440797012227888, $\mathbf{y^{k}} \bmod p$ = $1124568734648807^{51394216073587}$=3804 8 8279630195, $\mathbf{y_2} = \mathbf{m} \oplus \mathbf{y^{k}}$=380488283459650 и посылает **А** пару ($\mathbf{y_1}$, $\mathbf{y_2}$).

Абонент **А**, получив зашифрованное сообщение, восстанавливает его: $m = (y_1^{\alpha} \bmod p) \oplus y_2$.=($440797012227888^{725391906243661} \bmod 1125899906842679 \oplus 380488283459650$)= $380488279630195 \oplus 380488283459650$=4567345.♦

При использовании метода Эль-Гамаля в системе открытого шифрования с модулем модулем p из 150 знаков достигается та же степень защиты, что для алгоритма RSA с модулем из 200 знаков. Это позволяет в 5-7 раз увеличить скорость обработки информации. Однако в таком варианте открытого шифрования нет подтверждения подлинности сообщений.

Однако схема Эль-Гамаля не лишена определенных недостатков. Среди них можно выделить следующие.

1.Отсутствие семантической стойкости. Если g – примитивный элемент GF(p), то за полиномиальное время можно определить, является ли

некоторое число x квадратичным вычетом, или нет. Это делается возведением в степень $x^{(p-1)/2} \bmod p$. Если результат равен 1, то x - квадратичный вычет, если –1, то x квадратичный невычет. Затем пассивный противник проверяет, являются ли g^k и g^t квадратичными вычетами. g^{kt} будет квадратичными вычетом тогда и только тогда, когда g^k и g^t являются квадратичными вычетами. Если это так, то $y_2 = my^k \bmod p$ будет квадратичным вычетом тогда и только тогда, когда сообщение m будет само квадратичным вычетом. То есть, пассивный противник будет иметь некоторую информацию об открытом тексте имея лишь шифрованный текст и открытый ключ.

2. Делимость шифра. Если дан шифрованный текст (y_1, y_2), то можно получить другой шифрованный текст, изменив только вторую часть сообщения. Действительно, умножив y_2 на g^u ($u \neq 0$), мы получим шифротекст для другого сообщения $m_1 = mg^u$.

Для защиты от подобных атак Шнорром и Якобсоном было предложено объединить схему шифрования Эль-Гамаля с цифровой подписью Шнорра. Это позволяет не только шифровать сообщение, но и аутентифицировать его.

В заключении заметим, что алгоритм цифровой подписи DSA, разработанный NIST (National Institute of Standard and Technology) и являющийся частью стандарта DSS, опирается на рассмотренный метод.

6.8. КРИПТОСИСТЕМЫ НА БАЗЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Рассмотренная выше криптосистема Эль-Гамаля, базируется на том, что задача логарифмирования в конечном поле является достаточно сложной с вычислительной точки зрения. Однако конечные поля являются не единственными алгебраическими структурами, в которых может быть поставлена задача вычисления дискретного логарифма. В 1985 году Коблиц и Миллер (причем независимо друг от друга) предложили использовать для построения криптосистем алгебраические структуры, определенные на множестве точек эллиптической кривой (ЭК). Рассмотрим определение ЭК над полями Галуа.

Пусть $p > 3$ простое число, $a, b \in \mathbf{GF}(p)$, такие, что $4a^2 + 27b^2 \neq 0$. *Эллиптической кривой* E над полем $\mathbf{GF}(p)$ называется множество решений (x, y) уравнения:

$$y^2 = x^3 + ax + b \bmod (p) \qquad (13)$$

над полем $\mathbf{GF}(p)$ вместе с дополнительной точкой ∞, называемой точкой в бесконечности.

Представление ЭК в виде уравнения (13) носит название *эллиптической кривой в форме Веерштрасса.*

Если обозначить количество точек на кривой E через NE. Тогда, согласно теореме *Хассе*, $NE=p+1-t$, где $|t|\le 2(p)^{0.5}$.

NE называется *порядком* кривой E, а – t *следом* кривой E.

Для точек на кривой вводится бинарная операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах RSA и Эль-Гамаля:

1. $\infty+\infty=\infty$
2. Для любых $(x,y)\in E$, $(x,y)+\infty=(x,y)$
3. Для любых $(x,y)\in E$, $(x,y)+(x,-y)=\infty$
4. Для любых $(x_1,y_1)\in E$, и $(x_2,y_2)\in E$, $x_1\neq x_2$, $(x_1,y_1)+(x_2,y_2)=(x_3,y_3)$, где $x_3=\lambda^2- x_1- x_2$, $y_3=\lambda(x_1-x_3)-y_1$, $\lambda= (y_2-y_1)/(x_2-x_1)$.
5. Для любых $(x_1,y_1)\in E$, и $y_1\neq 0$, $(x_1,y_1)+(x_1,y_1)=(x_3,y_3)$, где $x_3=\lambda^2-2x_1$, $y_3=\lambda(x_1-x_3)-y_1$, $\lambda= (3 x_1^2+a)/2y_1$.

Множество точек на кривой E, с заданным таким образом бинарной операцией, образует абелеву группу.

Если $NE=p+1$,то E называется *суперсингулярной*.

Пользуясь операцией сложения точек на кривой, можно естественным образом ввести операцию умножения точки $P\in E$ на произвольное целое число k:

$$kP=P+P+\ldots+P.$$

Где операция выполняется k раз.

Построим теперь одностороннюю функцию, на базе которой будем строить криптосистему.

Пусть E – ЭК, точка $P\in E$. Возьмем $k\in Z$, причем $k<NE$. В качестве прямой функции выберем произведение kP. Для его вычисления по оптимальному алгоритму требуется не более $2\cdot\log_2 k$ операций сложения. Обратную задачу определим так: по заданным ЭК, точке $P\in E$ и произведении kP найти k. В настоящее время такая задача за полиномиальное время неразрешима.

Теперь рассмотрим криптографический протокол, аналогичный протоколу Диффи-Хелмана.

Для установления секретной связи два пользователя **A** и **B** выбирают ЭК E и точку P на ней. Затем **A** и **B** генерируют независимо друг от друга по секретному числу α и β. Затем пользователь **A** вычисляет произведение αP и пересылает его **B,** а пользователь **B** вычисляет βP и пересылает его **A**. При этом параметры кривой, координаты точки на ней, значения произведений являются открытыми и могут передаваться по незащищенным каналам связи. Далее пользователь **A** умножает присланное значение βP на α, получив после этого $\alpha\beta P$, пользователь **B** умножает присланное значение αP на β, получая такой же результат – $\alpha\beta P$. Таким образом, оба пользователя получили общее секретное значение (координаты точки $\alpha\beta P$ на ЭК), которое они могут использовать для получения секретного ключа шифрования. Необходимо отметить, что криптоаналитику

для восстановления ключа потребуется решить сложную с вычислительной точки зрения математическую задачу восстановления α и β по известным E, P, αP и βP.

Пример 72. Пусть абоненты **A** и **B** решили провести передачу сообщений используя криптосистему на базе ЭК. Для этого они выбрали ЭК

$$E: y^2 = x^3 + 157x + 223 \ \mathbf{mod}(743),$$

и точку $P(117,692)$ на ней. Затем **A** генерирует секретное число $\alpha = 735$. Пользователь **B** генерирует секретное число $\beta = 529$.

Затем пользователь **A** вычисляет произведение $\alpha P = (517,488)$ и пересылает его **B,** а пользователь **B** вычисляет $\beta P = (472,687)$ и пересылает его **A**. Далее пользователь **A** умножает присланное значение βP на α, получив после этого $\alpha\beta P=(332,590)$. Пользователь **B** умножает присланное значение αP на β, получая такой же результат – $\alpha\beta P=(332,590)$. Таким образом, оба пользователя получили общее секретное значение (координаты точки $\alpha\beta P$ на ЭК), которое они будут использовать в качестве общего секретного ключа. ♦

Переход на "эллиптическую" криптографию позволяет сохранить приемлемую длину ключа при резком (на порядки) увеличении стойкости криптосистем. Появление "эллиптической" криптографии и было обусловлено именно этой причиной.

7. АУТЕНТИФИКАЦИЯ И ЭЛЕКТРОННАЯ ПОДПИСЬ

7.1. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ

Назначение и суть протоколов аутентификации (иногда называемых протоколами идентификации) состоит в подтверждении подлинности информации. Например, предотвращение доступа к компьютерной системе лиц, не являющихся ее пользователями, а также предотвращение доступа пользователей к тем ресурсам, на которые у них нет полномочий. Одним из наиболее эффективных практических протоколов аутентификации является протокол Шнорра. Рассмотрим его схему.

Пусть p и q – простые числа, причем q делит p-1. Пусть $g \in \mathbf{GF}(p)$ такое, что $g^q \equiv 1 (\mathbf{mod}\ p)$, $g \neq 1$. Далее, пусть $k \in \mathbf{GF}(q)$ и $y = g^{-k} (\mathbf{mod}\ p)$, Таким образом, опять возникла задача дискретного логарифмирования, т.е. по заданному значению y и при известных p, q, и g, необходимо найти k. Тогда алгоритм аутентификации будет состоять в следующем.

1. Абонент A выбирает случайное число a из множества {1,…, q-1}, вычисляет $r = g^a (\mathbf{mod}\ p)$ и посылает его абоненту B. (Величина r может быть вычислена заранее)
2. Абонент B выбирает случайное число e из множества {1,…, 2^t-1}, где t – некоторый параметр, и посылает его абоненту A.
3. Абонент A вычисляет $s = a + ke (\mathbf{mod}\ q)$ и посылает его абоненту B.
4. Абонент B проверяет соотношение $r = g^s y^e (\mathbf{mod}\ p)$ и, если оно выполняется, принимает доказательство, иначе отвергает.

Пример 73. Пусть абонент B решил проверить полномочия абонента A. Для этого они с абонентом B выбрали числа q=984563, p=11814757 и g=10112979. Затем абонент A выбирает секретный ключ k= 729417 и вычисляет открытый ключ $y = g^{-k} (\mathbf{mod}\ p) = 10112979^{-729417} (\mathbf{mod}$ 11814757)=3767753. Затем абонент A выбирает случайное число a= 519231 и вычисляет $r = g^a (\mathbf{mod}\ p) = 10112979^{519231} (\mathbf{mod}$ 11814757)=7848734 и посылает его абоненту B. Абонент B выбирает случайное число e= 76314858 и посылает его абоненту A. Абонент A, получив это число, вычисляет $s = a + ke (\mathbf{mod}\ q) = (519231 + 729417 * 76314858) (\mathbf{mod}$ 984563)=471575 и посылает его абоненту B. Абонент B, получив это число, вычисляет $g^s y^e (\mathbf{mod}\ p) = 10112979^{471575} 3767753^{76314858} (\mathbf{mod}$ 11814757)=7848734. ♦

Пример 74. А теперь рассмотрим пример на эту же тему, но с большими числами. Пусть абонент B решил проверить полномочия абонента A. Для этого они с абонентом B выбрали числа q= 97579826939276 72234742336702169126293378710411851 3, p=21467561926640878916433140744772077845433162906072 87 и g=81011297946901347894325670350185478935475349017949. Затем абонент A выбирает секретный ключ k= 72956238690105817529579017623906706754879458675 63 и вычисляет от-

крытый ключ $y=g^{-k}(\mathbf{mod}\ p)$=810112979469013478943256703501854789354753490179497295623869010581752957901762390670675487945867563(**mod** 214675619266408789164331407447720778454331629060728 7)=16818586664932695256303604118437531417248949508333 09. Затем абонент ***A*** выбирает случайное число ***a***=519038897879775406783276659623812789524596 3785, вычисляет $r=g^{a}(\mathbf{mod}\ p)$=975798269392767223474233670216912629337871041185135190388978797754067832766596238127895245963785(**mod** 214675619266408789164331407447720778454331629060728 7)=35968892273536885220686976354633375367290382284977 1 и посылает его абоненту ***B***. Абонент ***B*** выбирает случайное число ***e***=763194645767980471859654794586946873978659678037272456748 58 и посылает его абоненту ***A***. Абонент ***A***, получив это число, вычисляет $s=a+ke(\mathbf{mod}\ q)$=(519038897879775406783276659623812789524596 3785 + 729562386901058175295790176239067067548794586756 3*763194645767980471859654794586946873978659678037272456748 58)(**mod** 975798269392767223474233670216912629337871041185 13)=490459097050876699091817569441825722066551725188 8 и посылает его абоненту ***B***. Абонент ***B***, получив это число, вычисляет $g^{s}y^{e}(\mathbf{mod}\ p)$=810112979469013478943256703501854789354753490179494904590970508766990918175694418257220665517251888^{763194645767980471859654794586946873978659678037272456748 58}16818586664932695256303604118437531417248949508333 09(**mod** 214675619266408789164331407447720778454331629060728 7)=10376438331583218532246262650568801277099560919608 95*167575118711433806350094900918867482420854108518188 3(**mod** 214675619266408789164331407447720778454331629060728 7)=35968892273536885220686976354633375367290382284977 1 ♦

Существуют также и другие схемы. Рассмотрим из них схему аутентификации Фейге-Фиата-Шамира.

Пусть ***n*** – произведение двух больших простых чисел. Для генерации открытых и закрытых ключей абонент ***A*** выбирает ***k*** различных чисел $\lambda_1, \lambda_2,\ldots\lambda_k$, каждое из которых является квадратичным вычетом (см. гл. 3.6) по модулю ***n***. Строка $\lambda_1, \lambda_2,\ldots\lambda_k$ служит открытым ключом. Затем вычисляются наименьшие значения $\beta_1, \beta_2,\ldots\beta_k$, для которых $\beta_i=sqrt(\lambda_I^{-1})$ (**mod** ***n***). Строка $\beta_1, \beta_2,\ldots\beta_k$ служит секретным ключом. Далее выполняется следующий протокол.

1. Абонент ***A*** выбирает случайное число ***a*** из множества {1,…, ***n***-1} и вычисляет $r=a^2(\mathbf{mod}\ n)$ и посылает его абоненту ***B***.
2. Абонент ***B*** посылает ***A*** строку из ***k*** случайных битов – $c_1, c_2,\ldots c_k$
3. Абонент ***A*** вычисляет $y= a\cdot(\beta_1^{c_1}\cdot\beta_2^{c_2}\cdot\ldots\cdot\beta_k^{c_k})(\mathbf{mod}\ n)$ и посылает его абоненту ***B***.
4. Абонент ***B*** проверяет, что $r=y^2\cdot(\lambda_1^{c_1}\cdot\lambda_2^{c_2}\cdot\ldots\cdot\lambda_k^{c_k})(\mathbf{mod}\ n)$

Абонент ***A*** и ***B*** повторяют этот протокол ***t*** раз, пока ***B*** не убедится, что ***A*** знает $\beta_1, \beta_2,\ldots \beta_k$. Шанс, что ***A*** обманет ***B*** ***t*** раз, равен 1 из 2^{kt}.

Пример 75. Рассмотрим работу этого алгоритма сначала на примере небольших чисел. Пусть $n = 11 \cdot 13 = 143$. Тогда возможными квадратичными остатками являются числа:

1. $1/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 1, 12, 131, 142$.
2. $3/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 17, 61, 82, 126$.
3. $4/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 2, 24, 119, 141$.
4. $9/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 3, 36, 107, 140$.
5. $12/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 21, 34, 109, 122$.
6. $14/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 27, 38, 105, 116$.
7. $16/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 4, 48, 95, 139$.
8. $22/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 55, 88$.
9. $23/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 32, 45, 98, 111$.
10. $25/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 5, 60, 83, 138$.
11. $26/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 13, 130$.
12. $27/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 40, 51, 92, 103$.
13. $36/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 6, 71, 72, 137$.
14. $38/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 18, 70, 73, 125$.
15. $42/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 31, 57, 86, 112$.
16. $48/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 42, 68, 75, 101$.
17. $49/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 7, 59, 84, 136$.
18. $53/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 14, 25, 118, 129$.
19. $55/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 22, 121$.
20. $56/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 54, 67, 76, 89$.
21. $64/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 8, 47, 96, 135$.
22. $66/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 66, 77$.
23. $69/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 28, 50, 93, 115$.
24. $75/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 19, 58, 85, 124$.
25. $77/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 44, 99$.
26. $78/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 65, 78$.
27. $81/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 9, 35, 108, 134$.
28. $82/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 15, 37, 106, 128$.
29. $88/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 33, 110$.
30. $91/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 39, 104$.
31. $92/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 53, 64, 79, 90$.
32. $100/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 10, 23, 120, 133$.
33. $103/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 31, 57, 86, 112$.
34. $104/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 26, 117$.
35. $108/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 41, 63, 80, 102$.
36. $113/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 16, 49, 94, 127$.
37. $114/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 20, 46, 97, 123$.
38. $121/x^2 \equiv 1 \pmod{143}$ имеет решения $x = 11, 132$.

39. $126/x^2 \equiv 1 \pmod{143}$ имеет решения x=29, 62, 81, 114.
40. $130/x^2 \equiv 1 \pmod{143}$ имеет решения x=52, 91.
41. $133/x^2 \equiv 1 \pmod{143}$ имеет решения x=43, 56, 87, 100.

Обратными значениями (по mod 143) и их квадратными корнями являются следующие числа:

	λ	λ^{-1}	$\beta=sqrt(\lambda^{-1})$
1.	1	1	1
2.	3	48	42
3.	4	36	6
4.	9	16	4
5.	12	12	21
6.	14	92	53
7.	16	9	3
8.	22		
9.	23	56	54
10.	25	103	31
11.	26		
12.	27	53	14
13.	36	4	2
14.	38	64	8
15.	42	126	29
16.	48	3	17
17.	49	108	41
18.	53	27	40
19.	55		
20.	56	23	32
21.	64	38	18
22.	66		
23.	69	114	20
24.	75	82	15
25.	77		
26.	78		
27.	81	113	16
28.	82	75	19
29.	88		
30.	91		
31.	92	14	27
32.	100	133	43
33.	103	25	5
34.	104		
35.	108	49	7
36.	113	81	9
37.	114	69	28
38.	121		

39. 126 42 30
40. 130
41. 133 100 10

Видим, что у чисел 22, 26, 55, 66, 77, 78, 88, 91, 104, 121 и 130 нет обратных значений. Это объясняется тем, что они не взаимно просты с числом 143. Кроме того, должно быть ровно (11-1)(13-1)/4=30 квадратичных остатков по mod 143.

Выбираем число k = 27. Таким образом, абонент A получает открытый ключ состоящий из 27 значений, например, λ = (9, 12, 14, 16, 23, 25, 27, 36, 38, 42, 48, 49, 53, 56, 64, 69, 75, 81, 82, 92, 100, 103, 108, 113, 114, 126, 133). Соттветственно секретным ключом является β =(4, 21, 53, 3, 54, 31, 14, 2, 8, 29, 17, 41, 40, 32, 18, 20, 15, 16, 19, 27, 43, 5, 7, 9, 28, 30,10).

Дальше выполняется протокол.

1. Абонент A выбирает случайным образом число a=113 меньше n и вычисляет $r=a^2(\mathbf{mod}\ n)= 113^2(\mathbf{mod}\ 143)=42$.
2. Абонент B посылает A строку из k случайных битов (c_1, c_2,… c_k) – (1 0 0 0 1 0 1 0 0 1 1 0 1 1 0 1 0 1 1 1 0 0 0 0 1 0 1).
3. Абонент A вычисляет $y= a\cdot(\beta_1^{c_1}\cdot\beta_2^{c_2}\cdot\ldots\cdot\beta_k^{c_k})(\mathbf{mod}\ n)$ =70 и посылает его абоненту B.
4. Абонент B вычисляет $y^2\cdot(\lambda_1^{c_1}\cdot\lambda_2^{c_2}\cdot\ldots\cdot\lambda_k^{c_k})(\mathbf{mod}\ n)$=42 и убеждается, что это значение совпадает с r.
2. Абонент A и B повторяют этот протокол столько раз, пока B не убедится, что A знает секретный ключ. ♦

А теперь приведем похожий пример, но с большими числами.

Пример 76. Пусть n = 97·127=12319. Выбираем число k = 105. Затем определяем k квадратичных вычетов (λ_1, λ_2,…λ_k), которые будут открытым ключом – (11264, 1120, 3297, 7657, 9840, 12025, 1893, 4082, 6273, 539, 2738, 4939, 7142, 9347, 11554, 3655, 5868, 8083, 10300, 200, 2421, 9096, 11325, 1237, 3470, 5705, 7942, 103, 2346, 4591, 6838, 9087, 11338, 5784, 8043, 10304, 248, 2513, 4780, 9320, 11593, 1549, 3826, 6105, 8386, 2922, 5211, 7502, 9795, 12090, 2068, 6668, 8971, 11276, 1264, 3573, 5884, 10512, 510, 2829, 5150, 7473, 9798, 4466, 6799, 9134, 11471, 1491, 3832, 8520, 10867, 897, 3248, 5601, 7956, 2714, 5077, 7442, 9809, 12178, 2230, 6978, 9355, 11734, 1796, 4179, 6564, 1412, 3805, 6200, 8597, 10996, 1078, 5886, 8293, 10702, 794, 3207, 5622, 560, 2983, 5408, 7835, 10264, 376). После этого определяем (β_1, β_2,…β_k), которые будут являться секретным ключом – (34, 157, 1865, 2518, 3170, 541, 1340, 45, 281, 482, 2475, 505, 158, 2848, 3416, 2818, 4251, 2257, 2977, 2998, 377, 1616, 3878, 2714, 2877, 2347, 1233, 4647, 4820, 362, 274, 1644, 5603, 3819, 2833, 3736, 3198, 3467, 1510, 3447, 1376, 1981, 3461, 974, 2096, 1906, 2476, 1482, 2191, 3886, 3408, 5223, 4939, 4991, 4976, 4117, 1055, 3573, 4326, 1285, 1390, 1504, 2521, 243, 1487, 315, 718, 3476, 4767, 2468, 2454, 2663, 1447, 2992, 5051, 137, 749, 3737,

1809, 3432, 3999, 683, 3752, 735, 3474, 2089, 475, 1258, 341, 4094, 1685, 811,173,3012, 2311, 1481, 1522, 379, 1735, 2004, 681, 1065, 161, 2697, 2453).

Далее выполняется следующий протокол.

1. Абонент A выбирает случайным образом число a=11678 меньше n и вычисляет $r=a^2(\mathbf{mod}\ n)$=4354.
2. Абонент B посылает A строку из k случайных битов (c_1, c_2,… c_k) – (1 0 0 1 0 1 1 1 1 0 0 1 0 1 1 1 0 0 0 0 0 1 0 1 0 0 0 0 1 0 0 0 1 1 1 1 0 0 1 1 0 0 0 1 1 1 1 0 1 1 0 1 1 1 0 1 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 1 0 0 1 1 1 1 0 0 1 0 0 1 1 1 1 1 0 0 1 0 1 0 1 1 1 1 1 0 1 1 0 1).
3. Абонент A вычисляет $y= a\cdot(\beta_1^{c_1}\cdot\beta_2^{c_2}\cdot\ldots\cdot\beta_k^{c_k})(\mathbf{mod}\ n)$ =10751 и посылает его абоненту B.
4. Абонент B вычисляет $y^2\cdot(\lambda_1^{c_1}\cdot\lambda_2^{c_2}\cdot\ldots\cdot\lambda_k^{c_k})(\mathbf{mod}\ n)$=4354 и убеждается, что это значение совпадает с r.

Абонент A и B повторяют этот протокол столько раз, пока B не убедится, что A знает секретный ключ. ♦

7.2. ЦИФРОВАЯ ПОДПИСЬ

Криптосистема "открытый ключ" неудобна в том смысле, что получатель сообщения не знает, кто является отправителем сообщения. Этого недостатка лишены протоколы "электронной подписи". Рассмотрим из них два. Первый – на базе RSA, а второй на основе алгоритма Эль-Гамаля.

Пусть имеется банкир A и несколько вкладчиков – $\mathbf{B}_1$, $\mathbf{B}_2$, $\mathbf{B}_3$, …. Банкир и каждый из вкладчиков независимо друг от друга выбирают два больших простых числа и держат их в секрете. Пусть $\mathbf{P}$ и $\mathbf{Q}$ – простые числа банкира, p_i и q_i – простые числа вкладчика $\mathbf{B}_i$, i = 1, 2, 3, … . Пусть далее $\mathbf{R} = \mathbf{PQ}$, $r_i = q_i p_i$, i = 1, 2, 3, … . И пусть банкир выбирает случайно целое число $\mathbf{S}$ с условиями $0 < \mathbf{S} < \varphi(\mathbf{R})$, $(\mathbf{S}, \varphi(\mathbf{R}))=1$, а каждый из вкладчиков также случайно и независимо друг от друга выбирает число s_i с условиями $0 < s_i < \varphi(r_i)$, $(s_i, \varphi(r_i))=1$, i = 1, 2, 3, … . После этого публикуется всем доступная телефонная книга:

A: $\mathbf{R}$, $\mathbf{S}$
$\mathbf{B}_1$: r_1, s_1
$\mathbf{B}_2$: r_2, s_2
.....

Далее каждый из них, и банкир и вкладчики, находят свои секретные $\mathbf{T}$, t_i ключи из условий:

$$\mathbf{S}\cdot\mathbf{T}\equiv 1(\mathbf{mod}\ \varphi(\mathbf{R})),\ 0 < \mathbf{T} < \varphi(\mathbf{R}),$$
$$s_i\cdot t_i\equiv 1(\mathbf{mod}\ \varphi(r_i)),\ 0 < t_i < \varphi(r_i),\ i = 1, 2, 3, \ldots .$$

Пусть вкладчик $\mathbf{B}_k$ собирается дать распоряжение m банкиру A, и пусть

$$0 < r_k < \mathbf{R}.$$

Последнее неравенство существенно для дальнейшего. Положим для удобства записи $\mathbf{B}=\mathbf{B}_k$, $r=r_k$, $t=t_k$, $s=s_k$. Будем считать $m < r$ и $(m, r)=1$. Вкладчик **B** шифрует распоряжение m сначала своим секретным ключом:

$$m_1 \equiv m^t (\mathbf{mod}\ r),\ 0 < m_1 < r,$$

а потом открытым ключом банкира:

$$m_2 \equiv m_1^{\mathbf{S}} (\mathbf{mod}\ \mathbf{R}),\ 0 < m_2 < \mathbf{R}.$$

Банкир A, получив шифрованную телеграмму m_2, расшифровывает ее пользуясь сначала своим секретным ключом **T**:

$$m_3 \equiv m_2^{\mathbf{T}} (\mathbf{mod}\ \mathbf{R}),\ 0 < m_3 < \mathbf{R}.$$

а потом открытым ключом s вкладчика:

$$m_4 \equiv m_3^{s} (\mathbf{mod}\ r),\ 0 < m_4 < r,$$

и получает $m_4 = m$.

Действительно, так как $m_3 \equiv m_2^{\mathbf{T}} (\mathbf{mod}\ \mathbf{R})$, а $m_2 \equiv m_1^{\mathbf{S}} (\mathbf{mod}\ \mathbf{R})$, то $m_3 \equiv m_1^{\mathbf{TS}} (\mathbf{mod}\ \mathbf{R})$, где $\mathbf{S}\cdot\mathbf{T} \equiv 1 (\mathbf{mod}\ \varphi(\mathbf{R}))$. Если $(m_1, \mathbf{R})=1$, то по теореме Ферма-Эйлера $m_1^{\mathbf{TS}} \equiv m_1 (\mathbf{mod}\ \mathbf{R})$, т.е. $m_3 \equiv m_1 (\mathbf{mod}\ \mathbf{R})$. Но $0 < m_3 < \mathbf{R}$, $0 < m_1 < r < \mathbf{R}$, следовательно $m_3 \equiv m_1$. Имеем $m_4 \equiv m_3^{s} \equiv m_1^{s} \equiv m^{st} (\mathbf{mod}\ r)$, $s\cdot t \equiv 1 (\mathbf{mod}\ \varphi(r))$ и $(m, r)=1$, а значит $m_4 \equiv m (\mathbf{mod}\ r)$, но каждое из них меньше r и больше 0. Следовательно, эти числа равны, т.е. $m_4 \equiv m_1$. Таким образом, банкир A получит распоряжение m от вкладчика **B**.

Пример 77. Пусть банкир A выбирает простые числа 10243 и 57037. Вкладчик **B** выбирает простые числа 175261 и 817549. Таким образом, $\mathbf{R}=10243\cdot 57037=584229991$ и $r=175261\cdot 817549=143284455289$.

Пусть 381259693 и 3387425143 – открытые ключи банкира и вкладчика соответственно.

Находим секретный ключ банкира из условия:

$\mathbf{S}\cdot\mathbf{T} \equiv 1 (\mathbf{mod}\ \varphi(\mathbf{R}))=381259693\cdot\mathbf{T} \equiv 1 (\mathbf{mod}\ \varphi(584229991)),\ 0 < \mathbf{T} < 584162712.$

Откуда $\mathbf{T}=182938789$.

Далее находим секретный ключи вкладчика из условия:

$s\cdot t \equiv 1 (\mathbf{mod}\ \varphi(r))=3387425143\cdot t \equiv 1 (\mathbf{mod}\ \varphi(143284455289)),\ 0<t<143283462480$

Откуда $t=111788667367$.

Тогда открытая телефонная книга имеет вид:

A: 584229991, 381259693;

B: 143284455289, 3387425143.

Вкладчик **B** дает поручение $m=134645771$ своему банкиру A и замечая, что $\mathbf{R}<r$, шифрует его сначала открытым ключом банкира, а потом своим секретным ключом:

$$m_1 = 134645771^{381259693} \equiv 116030491 (\mathbf{mod}\ 584229991),$$

$$m_2 = 116030491^{111788667367} \equiv 38467700641 (\mathbf{mod}\ 143284455289).$$

Банкир A, получив шифрованную телеграмму $m_2 = 38467700641$, и замечая, что $\mathbf{R}<r$, расшифровывает ее пользуясь сначала открытым ключом s вкладчика, а потом своим секретным ключом **T**:

$$m_3 = 38467700641^{3387425143} \equiv 116030491 (\mathbf{mod}\ 143284455289),$$

$$m_4 = 116030491^{182938789} \equiv 134645771 (\mathbf{mod}\ 584229991).$$

А так как 134645771<584229991, то банкир делает вывод, что 134645771 и есть распоряжение вкладчика. ♦

Пример 78. А теперь рассмотрим похожий пример, но с большими числами, а именно пусть банкир ***A*** выбирает простые числа **P**=194266889 22257290709194619068235189066424068390521395212518124097389042852052084982 21 и **Q**=198929294563914656862152899258728336040182460318939086976185590757263798805013350213277 7. Вкладчик **B** выбирает простые числа **p**=417184967953302750467777676986240647383340727022783744130281564027777290191531357426359782635 1 и **q**=2669983794901137602993777132711940143253380652945815962433802009777774657225800687528702608670 81. Таким образом, **R**=**P**·**Q**=3864537523017258344695351890931987344298927329706434998657235251451519142289560424626786245033085001726650883132403334350820436786561409950278676776821404280671468710289717 и ***r***=**p**·**q**=1113877103911668754551067286547922686741510866027480451801560673315252726369306002564920120031468182531702861728994369209436657549958984742232427841226232435332781707353985214366888130251431)), 0<***t***< 111387710391166875455106728654792268674151086602748045180156067331525272636930600256492012003114701230253321494119031371939560112915981326966761840754154941871472646872948983203975427155800. Откуда ***t***=109056550252289161829269902041753432224720341556643787880247773505328317235725448934782022536313214300223668805791968234988454323890072579294198446361623371822691409185898377739703441 6153319.

Вкладчик **B** дает поручение m=8123412425215154359032004312451233436749517375161233436749517375 16 своему банкиру A и замечая, что **R**<r, шифрует его сначала открытым ключом банкира, а потом своим секретным ключом:
m_1=8123412425215154359032004312451233436749517375161238761322052083357622784236013≡2485118227779378115516541275214643274377178128995632330660637496138268551978832175234052223930872088054190338920418878926479375920337706284851138975131623170385268669095130 (**mod** 3865375230172583446953518909319873442989273297064349986572352514515191422895604246267862450330852001726650883132403334350820436786561409950278676776821404280671468710289717), m_2=2485118227779378115516541275214643274377178128995632330660637496138268551978832175234052223930872088054190338920418878926479375920337706284851138975131623170385268669095130^109056550252289161829269902041753432224720341556643787880247773505328317235725448934782022536313214300223668805791968234988454323890072579294198446361623371822691409185898377739703441615331 9≡7348974255440206045469170280963118693281776781305750244088201689811543729592373210225923005200398839487519368071635351668554279001969186804332113952364535683806660485590593555006958958830 62 (**mod** 1113877103911668754551067286547922686741510866027480451801560673315252726369306002564920120031468182531702861728994369209436657549958984742232427841226232435332781707353985214366888130251431), m_3=7348974255440206045469170280963118693281776781305750244088201689811543729592373210225923005200398839487519368071635351668554279001969186804332113952364535683806660485590593555006958958830 62^178639387836316 4227858270210279≡2485118227779378115516541275214643274377178128995632330660637496138268551978832175234052223930872088054190338920418878926479375920337706284851138975131623170385268669095130 (**mod** 1113877103911668754551067286547922686741510866027480451801560673315252726369306002564920120031468182531702861728994369209436657549958984742232427841226232435332781707353985214366888130251431), m_4=2485118227779378115516541275214643274377178128995632330660637496138268551978832175234052223930872088054190338920418878926479375920337706284851138975131623170385268669095130^230726595042411533980460039812836889993533377268207609168020100852629367124284848087897991782386868391546511979031816145699166271734056411976690385722713794043481025746040 1≡8123412425215154359032004312451233436749517375161 (**mod** 386537523017258344 695351890931987344298927329706434998657235251451519142289560424626786245033

850017266508831324033343508204367865614099502786767768214042806
71468710289717).

А так как 8123412425215154359032004312451233436749517375 16 < 386453752301725834469535189093198734429892732970643499865723525145151914228956042462678624503308500172665088313240333435082043678656140995027867677682140428067146871028971 7, то банкир делает вывод, что 8123412425215154359032004312451233436749517375 16 и есть распоряжение вкладчика. ♦

А теперь рассмотрим цифровую подпись на базе алгоритма Эль-Гамаля. Основные положения алгоритма таковы.

Пусть имеются два простых числа – p и $2p+1$, $p>2$.Тогда v и w – образующие мультипликативных групп Z^*_p и Z^*_{2p+1} (т.е. групп обратимых элементов в Z_p и Z^*_{2p+1}). Далее вычисляем $v_0=(p+(p+1)\cdot v)(\mathrm{mod}\ 2p)$, которая будет являться образующей в Z^*_{2p}. Затем выбираем секретный ключ x из Z^*_p. Далее вычисляем открытый ключ y. Он определяется следующим образом: $z=v_0^x(\mathrm{mod}\ 2p)$; $y=w^z(\mathrm{mod}\ 2p)$. Сообщение s, к которому надо прикрепить цифровую подпись, принадлежит кольцу Z_{2p}, т.е. $s\in Z_{2p}$. Для вычисления электронной подписи выбираем случайное число $r\in Z^*_{2p}$ и в качестве подписи передаем пару чисел (a,b), где $a=a(r,s)=z^{-1}\cdot r\cdot s(\mathrm{mod}\ 2p)$, $b=b(r,s)=w^r(\mathrm{mod}\ 2p+1)$. Для проверки подлинности подписи необходимо воспользоваться равенством $y^a=b^s(\mathrm{mod}\ 2p+1)$.

Пример 79. Пусть имеются два простых числа – $p=1013$ и $2p+1=2027$. Образующие мультипликативных групп Z^*_{1013} и Z^*_{2027} соответственно равны $v=958$ и $w=1352$. Далее вычисляем $v_0=(p+(p+1)\cdot v)(\mathrm{mod}\ 2p)=(1013+(1013+1)\cdot 958)(\mathrm{mod}\ 2026)=1971$. Выбираем секретный ключ x из Z^*_p, $x=835$. Далее вычисляем открытый ключ y: $z=v_0^x(\mathrm{mod}\ 2p)=1971^{835}(\mathrm{mod}\ 2026)=855$, $y=w^z(\mathrm{mod}\ 2p)=1352^{855}(\mathrm{mod}\ 2026)=1758$. Создаем сообщение $s=1143$, к которому надо прикрепить цифровую подпись. Для этого выбираем случайное число $r\in Z^*_{2p}$: $r=1983$. Вычисляем пару (a,b): $a=z^{-1}\cdot r\cdot s(\mathrm{mod}\ 2p)=855^{-1}\cdot 1983\cdot 1143(\mathrm{mod}\ 2026)=1917\cdot 1983\cdot 1143(\mathrm{mod}\ 2026)=497$; $b=w^r(\mathrm{mod}\ 2p+1)=1352^{1983}(\mathrm{mod}\ 2027)=920$. Посылаем вычисленную пару (a,b) в открытый канал. Проверяем подлинность подписи: $y^a=1758^{497}(\mathrm{mod}\ 2027)=1269=b^s=920^{1143}(\mathrm{mod}\ 2027)$. ♦

8. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В последнее время защита информации перестала быть задачей только для государственных структур. С нею приходится сталкиваться и многим обычным пользователям персональных компьютеров (ПК). Идя навстречу их пожеланиям, многие производители программного обеспечения ст али включать свои продукты функции защиты данных. Однако в большинстве случаев разработчики не ставят своей целью использовать в них сколько-нибудь стойкие алгоритмы. Они считают своей основной задачей предоставить пользователю возможность защитить информацию либо от случайного несанкционированного доступа, либо от неквалифицированного взломщика. Они, скорее, маскируют информацию, чем реализуют алгоритмы надежного криптографического закрытия. Продемонстрируем данное утверждение на двух программных продуктах.

Многие пользователи используют в работе Microsoft Word. Эта система предоставляет пользователю большой спектр возможностей для работы с документами, в том числе и шифрования информации. Но выбранная в начальных версиях Microsoft Word схема шифрования информации останавливала лишь начинающего взломщика. Рассмотрим ее подробнее.

Из пароля пользователя Word вырабатывает массив длиной 16 байт, называемый гаммой (gamma[0…15]). далее, каждый байт открытого текста (open_text[i]) последовательно складывается побитно (XOR) с байтом гаммы. В результате получается шифрованный текст (cripto_text[i]), который мы можем видеть в файле с паролем, т.е. шифрование производится согласно формуле:

cripto_text[i]=open_text[i] XOR gamma[i mod 16],

где mod 16 – операция получения остатка от целочисленного деления на 16.

Таким образом, перед нами типичный пример криптографической схемы гаммирования короткой гаммой. Так как каждый шестнадцатый символ шифрованного текста получается прибавлением к символу открытого текста одного и того же значения гаммы, можно считать, что мы имеем дело с 16-ю простыми заменами. Для каждой из шестнадцати позиций символа в тексте подсчитаем таблицу частот его значений, после чего выберем в каждой из них значения символа, встретившегося чаще других.

Самый частый символ в документе Word – это пробел (его значение в кодировке ASCII есть 0x20). Следовательно, самым частым символам в таблице частот соответствуют зашифрованные пробелы. Складывая побитно значения этих символов с 0x20, мы получим все 16 знаков гаммы. Далее, зная гамму, расшифровываем весь текст.

На эту очевидную слабость многие обратили внимание. Поэтому фирма Microsoft для версий текстового процессора Microsoft Word, начиная с Word 97, полностью изменила алгоритм шифрования файлов, встроив в него алгоритмы шифрования RC4 и хеширования VD5.

Теперь посмотрим, как защищаются пароли пользователя в операционных системах (ОС) Microsoft Windows 95 первых версий (до OSR 2).

ОС Microsoft Windows 95 не является многопользовательской и не предоставляет возможность пользователям разделять свои ресурсы. Тем не менее, она запрашивает у пользователя при входе в систему его имя и пароль. Но если он ничего не ответит (нажмет кнопку Esc), ОС все равно разрешит ему работать дальше. Но для того, что бы работать в локальной вычислительной сети (ЛВС), где ПК доступны ресурсы или серверы, необходимы соответствующие пароли, причем, возможно, различные. Чтобы пользователю не нужно было их все запоминать, ОС Microsoft Windows 95 записывает пароли для доступа к ресурсам ЛВС в специальный файл с именем "имя_пользователя.pwl". В этом файле данные шифруются на том самом пароле, который система запрашивает у пользователя при его входе в систему. Если пароль введен правильно, то в дальнейшем ОС сама подставляет соответствующий пароль при запросе пользователя на доступ к ресурсам или серверам ЛВС.

Данные в *.pwl файлах шифруются следующим образом. Из пароля пользователя по алгоритму шифрования RC4 вырабатывается гамма. Каждый пароль на доступ к соответствующему ресурсу вместе с некоторой служебной информацией суммируется побитно с полученной гаммой. То есть каждый раз при шифровании используется одна и та же гамма. Если учесть, что *.pwl файл содержит зашифрованную запись, начинающегося с имени пользователя, дополненного до 20 символов пробелами, то задача вскрытия пароля становится элементарной. Получив первые 20 знаков гаммы, мы можем прочитать любой сохраненный в файле пароль (учитывая то обстоятельство, что редко когда используют пароли длиной более 10 символов).

Следует отметить, что сам по себе алгоритм RC4 довольно сложный, и в данном случае использовались слабости не самого алгоритма, а схемы его применения, а именно многократное использование одной и той же гаммы.

ЗАКЛЮЧЕНИЕ

Известно, что не существует единого шифра, подходящего для всех случаев жизни. Выбор способа шифрования зависит от особенностей информации, ее ценности и возможностей владельцев по защите своей информации. Прежде всего подчеркнем большое разнообразие видов защищаемой информации: документальная, телефонная, телевизионная, компьютерная и т.д. и т.п. Каждый вид информации имеет свои специфические особенности, и эти особенности сильно влияют на выбор методов шифрования информации. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации.

Выбор вида шифра и его параметров существенно зависит от характера защищаемых секретов или тайны. Некоторые тайны (например, государственные, военные и др.) должны сохраняться десятилетиями, а некоторые (например, биржевые) — уже через несколько часов можно разгласить. Необходимо учитывать так же и возможности того противника, от которого защищается данная информация. Одно дело — противостоять одиночке или даже банде уголовников, а другое дело — мощной государственной структуре.

Для профессионального понимания криптографических алгоритмов и умения оценивать их сильные и слабые стороны, необходима соответствующая математическая подготовка. Это объясняется тем, что современная криптография основана на глубоких результатах таких разделов математики, как теория сложности вычислений, теория чисел, алгебра и т.д. Представленный материал содержит основные сведения теории чисел, алгебры, необходимые для понимания основ современной криптографии. Желающие более глубоко ознакомиться с этими математическими дисциплинами, могут обращаться к рекомендуемой литературе.

Кроме того, за рамками данной работы остались многие вопросы, такие как генерация случайной последовательности, построение больших простых чисел, распознавание простоты наугад взятого числа, содержащего 250 и более цифр в десятичной записи, генерация ключей и т.д и т.п. Всех интересующихся данными вопросами можно порекомендовать обратиться к соответствующей литературе, часть из которой приведена в списке.

ЛИТЕРАТУРА

1. *Аграновский А.В., Балакин А.В, Хади Р.А.* "Классические шифры и методы их криптоанализа", М: Машиностроение, Информационные технологии, № 10, 2001.
2. *Ван дер Ваден Б.Л.* Алгебра, пер. с нем. 2–изд.– М.:Наука, 1979. – 352 с.
3. *Воеводин В.В.* Линейная алгебра. – М.:Наука, 1980. – 348 с.
4. *Гантмахер Ф.Р.* Теория матриц. – М.:Наука, 1966. – 576 с.
5. *Гельфанд И.М., Райков Д.А., Шилов Г.Е.* Коммутативные нормированные кольца. – М.:Физматгиз, 1959. – 356 с.
6. *Ибрагимов Н.Х.* Группы преобразований в математической физике. М.:Наука, 1983. – 280 с.
7. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.
8. *Кон П.* Универсальная алгебра. - М.:Мир. - 1968. – 351 с.
9. *Коробейников А. Г.* Математические основы криптографии. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002. – 41 с.
10. *Гатчин Ю. А., Коробейников А. Г.* Основы криптографических алгоритмов. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002. – 29 с.
11. *Левин М.* Криптография. Руководство пользователя. - М.: Познавательная книга плюс, 2001. – 320 с.
12. *Молдовян А.А., Молдовян Н.А., Советов Б.Я.* Криптография. – СПб.: Издательство "Лань", 2001. – 224 с.
13. *Смирнов В.И.* Курс высшей математики, том III, часть I – М:. Наука, Главная редакция физико-математической литературы, 1974. – 324 с.
14. *Фрид Э.* Элементарное введение в абстрактную алгебру. Пер. с венгер.–М.:Мир, 1979. – 260 с.
15. *Чмора А.Л.* Современная прикладная криптография. 2-е изд. – М.: Гелиос, АРВ, 2002. – 256 с. ил.
16. *Шеннон К.Э.* Теория связи в секретных системах. В кн. Шеннона К.Э. “Работы по теории информации и кибернетике”. – М.: ИЛ, 1963. – с. 333 – 402.
17. Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО, ”ЧеРо”, 1998. – 272 с.

оглавление

ИСТОРИЯ КАФЕДРЫ

1945-1966 РЛПУ (кафедра радиолокационных приборов и устройств). Решением Советского правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения. Приказом по институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д.т.н., профессор С. И. Зилитинкевич (до 1951 г.). Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. – радиоинженер (специальность 0705).

В разные годы кафедрой заведовали доцент Б.С. Мишин, доцент И.П. Захаров, доцент А.Н. Иванов.

1966–1970 КиПРЭА (кафедра конструирования и производства радиоэлектронной аппаратуры). Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско–технологической направленностью. Оканчивающим институт по этой специальности присваивалась квалификация инженер–конструктор–технолог РЭА.

Заведовал кафедрой доцент А.Н. Иванов.

1970–1988 КиПЭВА (кафедра конструирования и производства электронной вычислительной аппаратуры). Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых ответственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям– автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой д.т.н., проф. В.В. Новиков (до 1976 г.), затем проф. Г.А. Петухов.

1988–1997 МАИ (кафедра микроэлектроники и автоматизации проектирования). Кафедра выпускала инженеров–конструкторов–технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность **2205).** Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям–разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. С.А. Арустамов, за-

тем снова проф. Г.А. Петухов.

С **1997 ПКС** (кафедра проектирования компьютерных систем). Кафедра выпускает инженеров по специальности "Проектирование и технология электронно-вычислительных средств". Область профессиональной деятельности выпускников включает в себя проектирование, конструирование и технологию электронных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации. Кроме того, кафедра готовит специалистов по защите информации, специальность 075400 ”Комплексная защита объектов информатизации”. Объектами профессиональной деятельности специалиста по защите информации являются методы, средства и системы обеспечения защиты информации на объектах информатизации.

С 1996 г. кафедрой заведует д.т.н., профессор Ю.А. Гатчин.

За время своего существования кафедра выпустила 4069 инженеров, из них по специальности 0705 – 2472 чел. и по специальности 0648 (2205) – 1597 чел. На кафедре защищено 56 кандидатских и 7 докторских диссертаций.

Анатолий Григорьевич Коробейников, Юрий Арменакович Гатчин

Математические основы криптологии

Учебное пособие

Компьютерный набор и верстка А. Г. Коробейников
Дизайн А. Г. Коробейников

Зав. редакционно-издательским отделом Н.Ф.Гусарова

Лицензия ИД № 00408 от 05.11.99
Подписано к печати 28.06.04 Отпечатано на ризографе
Тираж 100 экз. Заказ № ___