Федеральное государственное казенное образовательное учреждение
высшего профессионального образования
«Дальневосточный юридический институт
Министерства внутренних дел Российской Федерации»

В.Т. Гиль

КЛАССИЧЕСКИЕ АЛГОРИТМЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ИНФОРМАЦИИ

Учебное пособие

Хабаровск, 2013

73
Г-474

Одобрено редакционно-издательским советом
Дальневосточного юридического института МВД РФ

Рецензенты:
начальник филиала ВНИИ МВД России
по Дальневосточному федеральному округу
канд. юрид. наук, доцент И.В. Никитенко;
заместитель начальника отдела ЦИТСиЗИ УМВД России
по Хабаровскому краю А.Л. Рассоха

Гиль, В.Т.

Г-474 Классические алгоритмы криптографических преобразований информации : учебное пособие / В.Т. Гиль ; Дальневосточный юрид. ин-т МВД РФ. – Хабаровск : РИО ДВЮИ МВД РФ, 2013. – 80с.

В учебном пособии рассмотрены основные понятия, технология и особенности применения классических алгоритмов криптографических преобразований информации.

Материал учебного пособия может быть использован при изучении дисциплин «Информатика и информационные технологии в профессиональной деятельности» и «Основы информационной безопасности в органах внутренних дел», предназначен для курсантов и слушателей вузов системы МВД России, практических работников ОВД.

Введение

История развития человеческого общества – это история расцвета и упадка цивилизаций, история мирного и военного соперничества людей за лучшие условия для жизни. В периоды стабильности общество развивалось и процветало за счет труда, знаний и опыта, накопленных членами этого общества. Люди, не способные к созидательному труду, но желающие жить также хорошо, как их одаренные и талантливые соседи, обычно решали свои проблемы за чужой счет, занимаясь воровством, грабежом, организуя военные походы. Нормальный человек в таких условиях был вынужден учиться защищать свою семью, свой дом и свое государство от внутренних и внешних врагов. Важным элементом защиты была защита знаний, обеспечивающих стабильность и развитие общества. Например, сведения о временных проблемах и трудностях не должны были попадать в руки врагов. Поэтому для передачи таких сведений друзьям люди сначала использовали стеганографию (сокрытие факта передачи информации), а затем стали применять криптографические методы, обеспечивающие преобразование информации к виду, исключающему ее прочтение лицами, не владеющими секретом преобразования.

Стеганография в переводе с греческого означает «секретная запись» (*steganos* – секрет и *graphy* – запись), а криптография – «тайнопись» (*kryptos* – тайный и *grapho* – пишу). Для вскрытия зашифрованных текстов и получения доступа к чужим секретам уже в древности стали применять методы криптоанализа. Криптография и криптоанализ составляют основу науки, которая называется криптологией. Она занимает значительное место среди других наук. Причем знание основ этой науки сейчас требуется всем пользователям информационных технологий, так как из существующих способов защиты информации криптографические способы наиболее доступны и надежны.

1. Основные понятия

Чтобы яснее представлять себе область знаний, занимающуюся шифрованием, дешифрованием и криптоанализом, сначала рассмотрим терминологию.

Шифрование (зашифрование) – процесс применения шифра к защищаемой информации, то есть преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифротекст, криптограмму) с помощью определенных правил, содержащихся в шифре.

Дешифрование (расшифрование) – процесс, обратный шифрованию, то есть преобразование шифрованного сообщения в исходную защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Вскрытием (или взломом) шифров называется процесс поиска способов получения доступа к зашифрованной информации без знания ключа.

Криптология (от греч. *kryptos* – тайный, *logos* – наука) – наука, которая занимается проблемами защиты информации путем ее преобразования. Криптология разделяется на два направления – криптографию и криптоанализ.

Криптография – наука, которая занимается поиском и исследованием математических методов преобразования (шифрования) информации в целях ее защиты от незаконных пользователей. Она также используется для исключения возможности искажения информации или подтверждения ее происхождения.

Криптоанализ – наука, занимающаяся поиском и исследованием математических методов вскрытия шифров без знания ключей, проверкой и доказательством устойчивости шифров к взлому как теоретически, так и практически.

Криптографический алгоритм, или шифр представляет собой семейство обратимых преобразований T открытого текста в шифрованный. Каждому члену этого семейства можно взаимно однозначно поставить в соответствие элемент k, называемый ключом, из набора возможных ключей K. Конкретный вариант преобразования T_k определяется соответствующим криптографическим алгоритмом, а также значением ключа k.

Ключ – определенное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного варианта преобразования из совокупности возможных для данного алгоритма вариантов.

Открытый текст, или клер в криптографии – исходное сообщение.

Криптограмма, шифротекст или шифрограмма – зашифрованное сообщение.

Преобразуемая информация представляет собой тексты (сообщения) в виде упорядоченных наборов элементов некоторого алфавита.

Алфавит – это конечное множество используемых для кодирования информации знаков. Примерами алфавитов являются двоичный алфавит, состоящий из двух элементов (0 и 1), шестнадцатеричный алфавит, содержащий набор из 16 символов (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F), латинский и русский алфавиты.

Обычно ключ представляет собой секретную последовательность символов алфавита. Следует отличать понятия «ключ» и «пароль». Пароль также является секретной последовательностью символов алфавита, однако используется не для шифрования, как ключ, а для аутентификации субъектов.

Необходимо также разделять термины «кодирование» и «шифрование», так как под кодированием обычно понимают представление информации в виде символов алфавита, а шифрование – это преобразование информационных кодов к виду, не позволяющему использовать информацию без знания алгоритма криптографического преобразования и ключа. То есть шифр характеризуется двумя элементами: алгоритмом и ключом.

2. История развития криптологии

Криптология используется людьми на протяжении нескольких тысячелетий, что говорит о ее значимости. За этот период она выросла до размера науки, сведения о которой долгие годы были засекречены, и только в последнее время становятся доступными пользователям открытых систем шифрования. Знакомству пользователей с основами этой науки может способствовать последовательное хронологическое рассмотрение фактов из истории криптологии. Без истории невозможно понять концептуальную схему данной науки, модель постановки проблем и их решения, методы исследования и их эволюцию.

Значительная часть древней истории криптологии не нашла отражение в письменных источниках и потеряна для потомков. До настоящего времени не удалось прочитать и многие источники, поскольку первоначально письменность сама по себе была своеобразной тайнописью, в древних обществах ею владели только избранные. Примером может служить египетское иероглифическое письмо, секрет которого был утерян в IV в. н.э., когда официальной религией Римской империи стало христианство. В 391 г. император Феодосий I закрыл все языческие храмы, в результате чего исчезли египетские жрецы, владевшие тайной древнеегипетского письма, и к VI в. уже никто не мог прочесть надписи на стенах гробниц и древние папирусы. Ключом к разгадке тайны иероглифов стал Розеттский камень, обнаруженный в 1799 г. офицером наполеоновской армии в дельте Нила при раскопках средневековой арабской крепости Розетта (рис. 1).

На плите из черного базальта высотой 1,5 метра трижды был высечен указ мемфисских жрецов в честь коронования фараона Птолемея V Епифана (205 – 180 гг. до н.э.): в верхней части камня – иероглифами, в средней – демотическим письмом, которым в то время пользовались египтяне, а в нижней – на греческом языке. Иероглифы были идентифицированы только в 1822 г. французским египтологом Жаном-Франсуа Шампольоном. Ключом к распознаванию стало имя Птолемея, выделенное картушем среди других иероглифов.

Шифрование появилось примерно четыре тысячи лет тому назад. Первым известным письменным источником, в котором содержались элементы шифро-

вания, считается египетский текст, датированный примерно 1900 г. до н.э. Вместо обычных (для египтян) иероглифов там были умышленно использованы не совпадающие с ними знаки. По мере совершенствования древнеегипетской письменности преобразования текстов, которые вырезались на каменных гробницах, продолжились. Постепенно многие надписи стали засекречивать, вероятно, для усиления колдовской силы поминальных текстов, а добавление элементов секретности породило криптографию. Иероглифы Древнего Египта действительно включали, хотя и в несовершенной форме, два элемента – секретность и преобразование письма, которые составляют основные атрибуты криптографии.

Рис. 1. Розеттский камень

В глубокой древности тайнопись считалась искусством. Сведения о способах шифрованного письма обнаружены в документах древних цивилизаций Индии, Египта, Месопотамии и Греции. Среди самых простых – иероглифическое письмо, написание знаков не по порядку, а вразброс по некоторому правилу. Например, в IV в. н.э. брахман Ватсьяяна – автор индийского трактата «Камасутра» – рекомендовал заменять буквы при шифровании по таблице, устанавливающей соответствие между буквами алфавита открытого текста и буквами криптограммы, выбираемыми произвольно. Этот метод шифрования сейчас называют алфавитной подстановкой.

Примеры использования криптографии можно встретить в священных иудейских книгах, в том числе в книге пророка Иеремии (VI в. до н.э.), где ис-

пользовался простой шифр подстановки для иврита под названием «атбаш». При шифровании этим шифром алфавит разбивается на две половины, буквы второй половины пишутся под буквами первой половины в обратном порядке. Буквы текста заменяют теми, которые стоят с ними в паре.

Одним из древнейших криптографических устройств, которое использовали древние греки в V–VI вв. до н.э., является скитала.

Скитала (от греч. *сцитала,* жезл), известный также как шифр Древней Спарты, представляет собой прибор, используемый для осуществления шифрования перестановкой. Он состоит из цилиндра и узкой полоски пергамента, обматывавшейся вокруг него по спирали, на которой писалось сообщение (рис. 2). Античные греки и спартанцы, в частности, использовали этот шифр для связи во время военных кампаний.

Рис. 2. Скитала

Шифруемый текст писался на пергаментной ленте по длине палочки. После того, как длина палочки оказывалась исчерпанной, она поворачивалась, и текст писался далее, пока либо не заканчивался текст, либо не исписывалась вся пергаментная лента. В последнем случае использовался очередной кусок пергаментной ленты. Дешифровка выполнялась с использованием палочки такого же диаметра.

Таким образом, размер шифруемого текста определялся длиной и диаметром палочки, а само шифрование заключалось в перестановке символов исходного текста. Например, используя палочку, по длине окружности которой помещается 4 символа, а длина палочки позволяет записать 5 символов, исходный текст – «это шифр Древней Спарты» – превратится в шифрограмму: «эфвп трна одер шрйт иесы». Схематически это изображено на рис. 3.

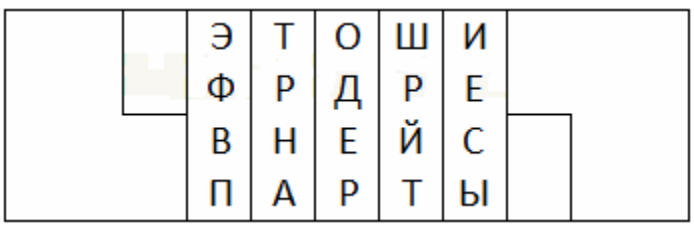

Рис. 3. Пример шифрования скиталой

С именем Энея Тактики – полководца IV в. до н.э. – связывают несколько техник шифрования и тайнописи. Диск Энея (рис. 4) был диаметром 10 - 15 см с отверстиями по числу букв алфавита.

Для записи сообщения нитка протягивалась через отверстия в диске, соответствующие буквам сообщения. При чтении получатель вытягивал нитку и получал буквы, правда, в обратном порядке. Чтобы недоброжелатель не смог прочитать сообщение, если перехватит диск, Эней предусмотрел способ быстрого уничтожения сообщения: для этого было достаточно выдернуть нить, закрепленную на катушке в центре диска.

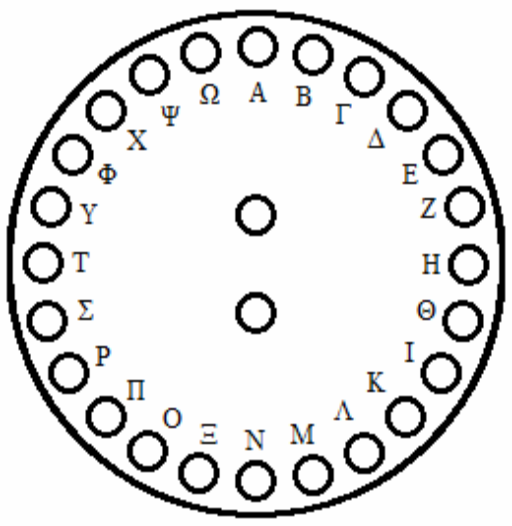

Рис. 4. Диск Энея

Первым действительно криптографическим инструментом можно назвать линейку Энея, реализующую шифр замены. Вместо диска использовалась линейка с отверстиями по числу букв алфавита, катушкой и прорезью. Для шифрования нить протягивалась через прорезь в отверстие, после чего на нити завязывался очередной узел. Для дешифрования необходимо было иметь саму нить и линейку с аналогичным расположением отверстий. Не владея ключом (линейкой), прочитать сообщение было невозможно.

В своем сочинении «Об обороне укрепленных мест» Эней описывает еще одну технику тайнописи, позже получившую название «книжный шифр». Он предложил при составлении тайного письма делать малозаметные проколы рядом с буквами в книге. Много позже аналогичные шифры нашли широкое применение.

Одним из первых шифров простой замены считается так называемый полибианский квадрат. За два века до нашей эры греческий писатель и историк Полибий предложил использовать для целей шифрования квадратную таблицу размером 5×5, заполненную 24 буквами греческого алфавита и пробелом в случайном порядке (рис. 5.).

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	κ
χ	ν		φ	ι

Рис. 5. Полибианский квадрат с греческим алфавитом

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифротекст букву, расположенную ниже нее в том же столбце. Если буква текста оказывалась нижней в строке таблицы, то для шифротекста брали самую верхнюю букву из того же столбца. Например, для слова ταυροσ получается шифротекст κφδμτξ.

В литературе полибианскими называют также квадраты другого типа, имеющие цифровые идентификаторы строк и столбцов, которые использовались при передаче сообщений с помощью оптического телеграфа. Каждая буква передавалась с помощью факелов ночью или флажков днем. Для указания позиции буквы в квадрате Полибия сначала числом факелов задавался номер строки, а затем – номер столбца.

Раньше квадрат такого типа назывался доской Полибия. На рис. 6 приведен вариант такого полибианского квадрата для латинского алфавита.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Рис. 6. Полибианский квадрат с латинским алфавитом

Изобретение Полибия оказалась плодотворным и нашло применение в криптосистемах последующего времени. Для шифрования, например, использовались квадраты Полибия с заполнением таблицы по лозунговому ключу.

Классическим примером древнего шифра является шифр Цезаря, который шифровал свои послания, заменяя каждую букву A на D, каждую B – на E, и так далее, то есть со смещением на 3 позиции по алфавиту.

С ослаблением античной цивилизации и образованием в Европе варварских государств криптография пришла в упадок. В условиях, когда грамотность была крайне низка, зашифровывать сообщения не было необходимости, да и самих письменных сообщений практически не существовало, поэтому в Средние века криптография в странах Западной Европы практически не применялась. Кроме того, шифрование и дешифрование рассматривались инквизицией как колдовство, которым заниматься было небезопасно. Даже церковные системы шифрования пребывали в зачаточном виде, хотя тогда Церковь пользовалась наибольшим влиянием в обществе. Только в период позднего Средне-

вековья криптография начинает постепенно возрождаться, становясь одним из важнейших инструментов политики, дипломатии и военного дела.

С VIII в. н.э. основной вклад в развитие криптологии внесли арабские ученые. Используются и до настоящего времени понятия «алгоритм», «шифр» и «цифра» арабского происхождения. В 855 г. арабский ученый по имени Абу Бакр тамед бен-Али бен-Вахшия ан-Набати в своей «Книге о большом стремлении человека разгадать загадки древней письменности» описал несколько шифров, в том числе полиалфавитный шифр. В это же время выходит в свет книга арабского филолога Халиль аль-Фарахиди «Китаб аль-Маумма» («Книга тайного языка»), в которой он описал метод вскрытия зашифрованного текста на основе использования стандартных фраз. Используя данный метод, филолог расшифровал письмо византийскому императору на греческом языке, предположив, что первыми в нем будут слова: «Во имя Аллаха».

В IX в. Ал-Кинди в книге «Манускрипт о дешифровке криптографических сообщений» привел сведения о частотном криптоанализе. Позже, в 1412 г., Шехабом ал-Калкашанди была написана 14-томная энциклопедия «Шауба ал-Аша», один из разделов которой под названием «Относительно сокрытия в буквах тайных сообщений» содержал описание семи шифров замены и перестановки и методику криптоанализа шифротекста, основанную на частотных характеристиках букв арабского языка, полученных при изучении текста Корана.

Излагая методику анализа, Калкашанди, в частности, писал: «Если вы хотите прочесть сообщение, которое вы получили в зашифрованном виде, то, прежде всего, начните подсчет букв, а затем сосчитайте, сколько раз повторяется каждый знак, и подведите итог в каждом отдельном случае. Если изобретатель шифра был очень внимателен и скрыл в сообщении все границы между словами, то первая задача, которая должна быть решена, заключается в нахождении знака, разделяющего слова. Это делается так: вы берете букву и работаете, исходя из предположения, что следующая буква является знаком, делящим слова. И таким образом вы изучаете все сообщение с учетом различных комбинаций букв, из которых могут быть составлены слова... Если получается, тогда все в порядке; если нет, то вы берете следующую по счету букву и так далее, пока вы не сможете установить знак раздела между словами.

Далее нужно найти, какие буквы чаще всего встречаются в сообщении, и сравнить их с образцом частоты встречаемости букв, о котором упоминалось прежде. Когда вы увидите, что одна буква попадается чаще других в данном сообщении, вы предполагаете, что это буква "Алиф". Потом вы предполагаете, что следующей по частоте встречаемости будет буква «Лам». Точность вашего предположения должна подтверждаться тем фактом, что в большинстве контекстов буква «Лам» следует за буквой "Алиф"... Затем первые слова, которые вы попытаетесь разгадать в сообщении, должны состоять из двух букв. Это делается путем оценки наиболее вероятных комбинаций букв до тех пор, пока вы не убедитесь в том, что стоите на правильном пути. Тогда вы глядите на их знаки и выписываете их эквиваленты всякий раз, когда они попадаются в сообщении. Нужно применять точно такой же принцип по отношению к трехбуквен-

ным словам этого сообщения, пока не убедитесь, что вы на что-то напали. Выписывайте эквиваленты из всего сообщения.

Этот же принцип применяется по отношению к словам, состоящим из четырех и пяти букв, причем метод работы прежний. Всякий раз, когда возникает какое-либо сомнение, нужно высказать два-три предположения или еще больше и выписать каждое из них, пока оно не подтвердится на основании другого слова». В данном разделе Калкашанди приводит также пример вскрытия шифра по приведенной методике.

В эпоху позднего Средневековья криптография в Европе начинает возрождаться, прежде всего, в среде интеллектуальной элиты того времени. Многие ученые средневекового периода стремились скрыть сделанные ими изобретения и открытия. Так, современные исследователи установили, что состав черного пороха был открыт известным английским ученым середины XIII в. Роджером Бэконом почти за сто лет до «официальной» даты создания пороха Бертольдом Шварцем. В одном из своих трудов он привел незашифрованное описание свойств этого вещества, но сам состав был зашифрован шифром перестановки, который удалось вскрыть лишь в наши дни.

Развитие криптологии в позднее Средневековье связано также с нуждами дипломатии. В это время лидерство в области криптографии принадлежало папской курии, имевшей активные дипломатические связи и привлекавшей к своей работе образованнейших людей того времени. Появление постоянных дипломатических представительств и обострение политической борьбы стимулировало послов зашифровывать свои донесения, опасаясь, что они будут перехвачены противником. Во многих европейских государствах появляется должность «секретаря по шифрам», единственным занятием которого было создание шифров для «своих» дипломатических служб и взлом «чужих» сообщений.

В эпоху Возрождения первой европейской книгой, описывающей использование криптографии, считается труд Роджера Бэкона (XIII в. н.э.) «Послание брата Рогериса Бакониса о тайных действиях искусства и природы и ничтожестве магии», описывающий, в числе прочего, применение 7 методов скрытия текста.

Надо сказать, что к началу XV в. криптология в Европе достигла значительных успехов и сравнялась с арабским уровнем (возможно и обогнала его). Так, в 1401 г. в герцогстве Мантуя секретарь герцога Симеоне де Крема создал первый дошедший до нас шифр многозначной замены. Он ввел в шифр гомофоны (возможность замены символа исходного текста одним из нескольких возможных знаков шифра) для сокрытия гласных букв при помощи более чем одного эквивалента, что может свидетельствовать о знакомстве составителя шифра с методами криптоанализа, основанными на частоте встречающихся в тексте гласных букв.

В XIV в. сотрудник канцелярии папской курии Чикко Симонетти написал книгу о системах тайнописи. В ней описаны шифры замены, в которых гласным буквам ставятся в соответствие несколько знаков с целью выравнивания частот букв в шифротексте. Дано понятие лозунгового шифра, в котором замена букв

определяется так: под алфавитом пишутся различные буквы лозунга в порядке появления, а затем буквы, не появившиеся в лозунге. Почти век спустя появляется книга «Трактат о шифрах», ее автор Габриэль де Лавинд, секретарь папы Клементия XII, дает описание нового типа шифра, предполагающего замену букв несколькими символами, количество которых пропорционально встречаемости букв в открытом тексте. Имена, должности, географические названия рекомендуется заменять специальными знаками. Это был самый ранний образец номенклатора – гибридной системы шифрования, которой в последующие 450 лет суждено было распространиться по всей Европе. В этот период в Милане применяется шифр под названием «миланский ключ», представляющий собой значковый шифр пропорциональной замены.

Отцом западной криптографии называют ученого эпохи Возрождения Леона Альберти. В 1466 г. он представил в папскую канцелярию трактат о шифрах, где описал способ маскировки сообщения в некотором безобидном вспомогательном тексте. Здесь же Альберти предложил свой собственный шифр с нескромным названием «шифр королей». По сути, Альберти придумал полиалфавитную замену – новый вид шифрования, используемый в большинстве современных шифрсистем.

По идее Альберти, первую букву сообщения следовало заменять по одному признаку (алфавиту замены). Например, a = p, b = m, c = f, ..., вторую – по второму, например, a = l, b = t, c = a, ..., третью – по третьему, например, a = f, b = x, c = p, ... и так далее. Порядок шифралфавитов устанавливался в соответствии с известным ключом. Многоалфавитные шифры явились большим шагом вперед, но на практике не использовались в течение более четырех столетий. Многоалфавитная замена, по сравнению с номенклатором, отнимала слишком много времени, а «незначительная» ошибка при письме, например, пропуск буквы, приводила к таким искажениям, что получателю сообщения было не суждено расшифровать его даже при наличии верного ключа. Несколькими годами позже, значительно опередив свое время, Альберти изобрел код с перешифровкой, который стал широко применяться в странах Европы лишь 400 лет спустя.

В 1518 г. в развитии криптографии был сделан новый шаг благодаря появлению в Германии первой печатной книги по криптографии. Аббат Иоганнес Тритемий – настоятель монастыря в Вюрцбурге – написал книгу «Полиграфия», в которой говорится о ряде шифров. Один из них развивает идею многоалфавитной замены. Шифрование осуществляется так: заготавливается таблица замены, в которой первая строка есть алфавит, вторая строка – алфавит, сдвинутый на один шаг и т.д. При шифровании первая буква открытого текста заменяется буквой, стоящей в первой строке, вторая буква – буквой во второй строке и т.д.

Несмотря на то, что тайнопись использовалась уже в XII - XIII вв., в России официальной датой появления криптографической службы считается 1549 г. (царствование Ивана IV), а именно образование «посольского приказа», при котором имелось «цифирное отделение». Шифры использовались такие же,

как на западе: значковые, замены, перестановки. Петр I позднее полностью реорганизовал криптографическую службу, создав Посольскую канцелярию. В это время появляются специальные коды для шифрования – «цифирные азбуки».

В 1550 г. была издана книга состоящего на службе у Папы Римского итальянского математика Джероламо Кардано «О тонкостях», в которой он описал шифр, называемый ныне «Решетка Кардано», и предложил использовать открытый текст в качестве ключа. Решетку Кардано считают первым транспозиционным шифром, или геометрическим шифром, основанным на положении букв в шифротексте.

Три года спустя в Италии вышла книга «Шифр синьора Белазо», в которой автор предложил использовать слово или группу слов, назвав это «паролем», выписывая его над открытым текстом. Буква пароля означает номер применяемой замены к букве открытого текста.

В начале XVI в. Маттео Арженти, криптограф папской канцелярии, изобрел код, представляющий собой шифр замены, в котором заменяются буквы, слоги, слова и целые фразы. Необходимым количеством словарных величин в коде считалось 1200. В это же время появляется и числовой код.

Следующим этапом развития криптографии можно считать 1563 г., когда в своей книге «О тайной переписке» итальянец Джованни Порта описал полиалфавитный табличный шифр и биграммный шифр, в котором осуществляется замена не одной буквы, а пары букв. Там же Джованни Порта приводит примеры списков вероятных слов из различных областей знания, существенно предвосхитив то, что впоследствии криптологи назовут «методом вероятного слова».

Фрэнсис Бэкон в 1580 г. предложил двоичный способ кодирования латинского алфавита по принципу, аналогичному тому, который сейчас применяется в компьютерах. Используя этот принцип, а также имея два разных способа начертания для каждой из букв, отправитель мог «спрятать» в тексте одного длинного сообщения короткое секретное. Данный способ тайнописи получил название «шифр Бэкона», хотя, по сути, относится к стеганографии.

В том же XVI в. был сделан еще один существенный шаг в развитии криптографии. Блез Виженер, французский посол в Риме, познакомился там с трудами по криптографии, после чего в 1585 г. вышла книга «Трактат о шифрах». В ней он описал основы криптографии и предложил табличный шифр полиалфавитной замены, который сейчас называют шифром Виженера. В качестве ключа он рекомендовал использовать открытый или шифрованный текст. Этот шифр с коротким ключевым словом получил широкое распространение и до 1863 г., когда в печати была опубликована методика вскрытия этого шифра, считался криптостойким.

К концу XVII в. криптография окончательно сложилась как научная дисциплина. Появились профессиональные криптоаналитики, соответствующие службы практически в каждой европейской стране, в состав которых входила научная элита того времени: Франсуа Виет во Франции, Джероламо Кардано

в Риме, Джон Валлис и Фрэнсис Бэкон в Англии, Лейбниц в Германии. Возникло значительное количество работ по криптографии и криптоанализу. Несмотря на то, что в это время господствовали номенклаторы, которые не являлись шифрами в чистом виде, появление многоалфавитной замены, использование решеток, биграмм и цифровых обозначений стало огромным шагом вперед, по сравнению с древнейшим периодом.

XVIII век для криптологии был веком застоя. Большой скачок, который эта наука сделала в предшествующий период, позволил в течение почти 150 лет не вводить никаких нововведений в способы шифрования и дешифровки сообщений. Криптографические системы, разработанные ранее, успешно применялись на практике, а трактаты XVI - XVII вв. служили учебными пособиями для криптоаналитиков. Почти повсеместно к криптографической деятельности привлекались видные ученые, в основном математики. Однако ни один из них в XVIII в. не оставил сколь-нибудь значимого труда по криптологии, не разработал новой шифрсистемы, не придумал более эффективного способа криптоанализа. Существовавшие шифры замены были довольно устойчивы, но и квалификация криптоаналитиков была настолько высокой, что большинство значимых сообщений расшифровывалось. Это время стало периодом расцвета номенклаторов. Данный тип криптографической системы, постепенно усложнявшийся на протяжении трех предшествующих веков, достиг в XVIII в. пика своего развития. Стандартным был размер номенклатора в 400-500 символов, но были и такие, которые достигали 5-6 тыс., заменяя особыми символами практически все значимые понятия, имена, названия и целые предложения. В этот период номенклаторы стали походить больше не на шифр, а на форму иероглифического письма. И, несмотря на это, их все же взламывали.

В 1790 г. криптография, будучи в состоянии застоя, все-таки обогатилась замечательным изобретением. Его автор – государственный деятель, первый государственный секретарь, а затем и президент США – Томас Джефферсон. Свою систему шифрования он назвал «дисковым шифром». Этот шифр реализовывался с помощью специального устройства, которое впоследствии назвали шифратором Джефферсона (рис. 7).

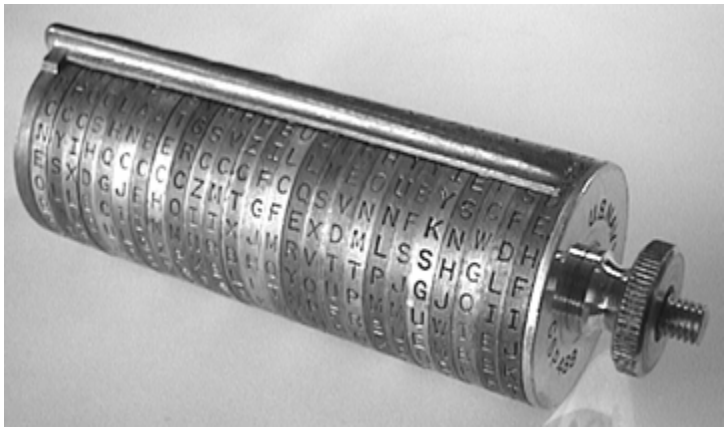

Рис. 7. Американский шифратор M-94 (CSP-488), аналог шифратора Джефферсона

Конструкция шифратора может быть вкратце описана следующим образом. Деревянный цилиндр разрезался на 36 дисков (в принципе, общее количество дисков могло быть и иным). Эти диски насаживались на одну общую ось таким образом, чтобы они могли независимо вращаться на ней. На боковых поверхностях каждого из дисков выписывались все буквы английского алфавита в произвольном порядке. Стоит отметить, что порядок следования букв на различных дисках – различный. На поверхности цилиндра выделялась линия, параллельная его оси. При шифровании открытый текст разбивался на группы по 36 знаков, затем первая буква группы фиксировалась положением первого диска по выделенной линии, вторая – положением второго диска и так далее. Шифрованный текст образовывался путем считывания последовательности букв с любой линии, параллельной выделенной. Обратный процесс осуществлялся на аналогичном шифраторе: полученный шифротекст выписывался путем поворота дисков по выделенной линии, а открытый текст отыскивался среди параллельных ей линий путем прочтения осмысленного возможного варианта. Это изобретение стало предвестником появления так называемых дисковых шифраторов, нашедших широкое распространение в развитых странах в XX в. Шифратор, совершенно аналогичный шифратору Джефферсона, использовался в армии США с 1922 г. и до окончания Второй мировой войны, но при жизни Джефферсона его шифратор не нашел применения.

Изобретение Джефферсона в 1891 г. повторил француз Этьен Базери. Его устройство – «цилиндр Базери» – было отвергнуто из-за «чрезвычайной сложности» как в изготовлении, так и в применении. Следует отметить, что подобное устройство – «прибор Вави» – в 1916 г. изобрел также наш соотечественник подпоручик Попазов. В XX в. криптоаналитики США признали высокую стойкость шифра Джефферсона. Они даже назвали его автора «отцом американского шифровального дела».

В начале XIX в. криптология оставалась на прежнем уровне, несмотря на бурные события, происходившие в Европе. Ситуация изменилась только в середине XIX в. Сначала, в 1844 г., был изобретен телеграф, а затем, в 1895 г., – радио. Возросшие скорости передачи информации требовали увеличения скорости шифрования, а средства ручного шифрования обеспечить этого уже не могли, хотя продолжали совершенствоваться и широко использоваться. Так, в 1854 г. англичанин Чарльз Уитстон изобрел новую криптографическую систему, значительно повысившую устойчивость шифров к взлому. Она получила название «шифр Плейфера». Друг Уитстона Лорд Плейфер способствовал использованию шифра английскими военными. Чарльзу Уитстону приписывается также изобретение шифра «двойной квадрат Уитстона», но который он не изобретал. Эту модификацию шифра предложили немцы, называли этот шифр «два квадрата» и использовали накануне и во время Второй мировой войны.

В 1863 г. в Берлине вышла в свет небольшая книга Фридриха Касиски «Искусство тайнописи и дешифрования», ознаменовавшая начало новой эпохи в криптоанализе. В ней он описал метод вскрытия полиалфавитных шифров,

с помощью которого можно было вскрывать практически любые шифры того времени. Метод состоял из двух частей: определения периода шифра и дешифровки текста с использованием частотного криптоанализа.

В 1883 г. Огюст Керкгоффс опубликовал работу под названием «Военная криптография», где были сформулированы принципы криптоанализа. Он доказал, что криптоанализ – единственное верное средство испытания надежности шифров и что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Иными словами, согласно Керкгоффсу, криптоаналитику противника известно все об алгоритме шифрования, кроме значения секретного ключа. Стоит отметить, что криптоаналитик имеет в своем распоряжении шифротексты сообщений. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации. Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и средств, тогда как ключ является легко изменяемым объектом. Именно поэтому стойкость криптосистемы определяется только секретностью ключа.

Кроме этого, он разработал криптоаналитические методы, играющие важную роль в современной теории дешифрования. Один из них называется наложением, или перекрытием, и представляет собой способ дешифрования многоалфавитных систем замены. Для криптоанализа данным методом нужно иметь несколько сообщений, зашифрованных одним и тем же ключом. Криптоаналитик выписывает эти сообщения одно под другим так, чтобы буквы, зашифрованные одной и той же буквой ключа, образовывали единую колонку. Каждую такую колонку можно потом дешифровать как обыкновенную одноалфавитную замену.

В 1917 г. сотрудник американской компании «Американ телефон энд телеграф» («AT&T») Гилберт Вернам разработал шифр для телеграфных аппаратов, который был запатентован в 1919 г. В телеграфных аппаратах для кодирования букв использовался пятиразрядный код Бодо. В этом коде буква «A», например, кодируется комбинацией «1 1 0 0 0», а буква «N» – комбинацией «0 0 1 1 0». Вернам предложил при передаче производить сложение по модулю 2 (обозначается □) пятиразрядных кодов букв открытого текста с пятиразрядными кодами букв псевдослучайной последовательности, которая получила название «гамма». На рис. 8 приведен пример такого сложения. Результат сложения по модулю 2 равен 0, если складываются разряды, имеющие одинаковое значение (0□0 или 1□1), и равен 1, если складываются разряды, имеющие различное значение (0□1 или 1□0). При дешифровании коды букв криптограммы складывались с последовательностью букв гаммы, использованной при шифровании, в результате чего восстанавливался открытый текст.

Коды букв открытого текста	□	0 0 1 0 10 1 1 1 11 0 1 0 10 1 1 1 01 1 0 0 0
Коды букв гаммы		1 1 0 0 10 1 0 1 01 1 0 1 11 0 0 1 10 0 1 0 1
Коды букв криптограммы	=	1 1 1 0 00 0 1 0 10 1 1 1 01 1 1 0 11 1 1 0 1

Рис. 8. Пример сложения 5 символов в коде Бодо с гаммой

При использовании шифра Вернама шифрование и дешифрование выполнялось в процессе передачи по каналу связи в автоматическом режиме. Такое шифрование впоследствии стали называть линейным. До появления шифра Вернама информация первым делом шифровалась и только после этого передавалась по каналу связи.

Сначала для формирования гаммы использовали склеенную в кольцо перфоленту с набитыми на нее кодами гаммы. Для короткой перфоленты период гаммы был небольшим, поэтому и защита не отличалась высокой стойкостью. Использовать длинные перфоленты с гаммой было неудобно, поэтому поступило предложение длинную гамму формировать путем сложения по модулю двух коротких гамм, имеющих различную длину и взаимно простые периоды. В этом случае общий период равняется произведению периодов исходных гамм. Если, например, одна такая гамма содержала 100 букв, а вторая – 99, то при их суммировании результирующая гамма начинала повторяться только через 9900 знаков.

Несмотря на то, что шифр Вернама при соблюдении определенных условий является единственным невскрываемым шифром, он не получил широкого распространения. Абсолютная криптостойкость этого шифра реализуется только при условии однократного использования истинно случайной гаммы, размер которой должен быть не меньше шифруемого сообщения. Другими словами, случайный ключ шифрования в шифре Вернама должен иметь такой же размер, как и открытый текст, причем при шифровании следующего открытого текста требуется новый случайный ключ соответствующего размера. При интенсивном обмене зашифрованной информацией, особенно в условиях военного времени, организовать изготовление, учет и передачу по секретным каналам ключевых последовательностей, равных по размеру шифруемым текстам, весьма проблематично (если есть секретный канал для передачи ключевой информации, то проще использовать его для передачи открытых текстов). Поэтому шифр Вернама в виде одноразового шифровального блокнота используется для передачи только совершенно секретной информации небольшого объема. В 1947 г. Клод Шеннон в статье «Теория связи в секретных системах» доказал, что полный перебор ключей, которые могли быть использованы при шифровании одноразовым шифроблокнотом, позволит извлечь из криптограммы всевозможные осмысленные тексты одинаковой длины, причем какой из них был в действительности зашифрован – выявить невозможно.

В 1918 г. были опубликованы труды американского криптолога и криптоаналитика российского происхождения Уильяма Фридмана «Ривербэнкские Записки» (цикл из 8 лекций) и «Индекс совпадения и его применение в криптографии». В этой работе, которая считается одной из самых важных

в истории криптологии, Фридман ввел понятие «индекс совпадения» и методику расчета совпадения. Фридман также предложил метод определения периода гаммы (длины лозунга) в шифре Виженера и бесключевой метод дешифрования при использовании неравновероятной гаммы (так называемый тест Фридмана, 1925 г.). Он впервые продемонстрировал успешное применение вероятностно-статистических методов в криптографии, которые стали серьезным вкладом в теоретическую криптографию и по сегодняшний день не утратили своей актуальности.

В первой половине XX в. было разработано несколько различных электромеханических шифровальных устройств, позволяющих получить преимущество в скорости и точности шифрования, которых недоставало ручным системам, и одновременно достигнуть желаемого уровня сложности. В период с 1917 г. по 1919 г. патенты на такие устройства получили: американец Э.Х. Хепберн, голландец Х.Ф. Кох, немец А. Шербиус и швед А.Г. Дамм.

Шифровальное устройство Эдварда Хепберна на основе шифрующего диска, запатентованное им в 1917 г., представлено на рис. 9. Шифрующий диск, или ротор изготавливался из изоляционного материала, например, твердой резины. По окружностям каждой из его сторон были вмонтированы на равном расстоянии друг от друга 26 электрических контактов. Каждый контакт был соединен внутри корпуса с некоторым контактом на другой стороне. Контакты на входной стороне представляли буквы открытого текста, контакты на выходной стороне – буквы шифротекста.

Рис. 9. Одноторный шифратор Эдварда Хепберна

Ротор устанавливался на оси между двумя неподвижными пластинами (розетками), каждая из которых также была изготовлена из изолятора и имела 26 контактов, соответствующих расположению контактов на диске. Контакты входной розетки соединялись с клавиатурой пишущей машинки, печатающей буквы открытого текста. Контакты выходной розетки соединялись с выходным устройством, указывающим буквы шифротекста, например, с помощью лампочек. При фиксированном угловом положении ротора электрические цепи, соединяющие входные и выходные контакты, реализовывали моноалфавит-

ную замену, но ротор в устройстве поворачивался на один шаг после шифрования каждой буквы, реализуя полиалфавитную замену с использованием 26 алфавитов.

После того, как первые 26 букв были зашифрованы, ротор снова приходил в исходное положение и последовательность алфавитов повторялась. С криптографической точки зрения, такое повторение является недостатком, так как оно наступает после зашифровывания слишком небольшого количества букв исходного текста. Чтобы усложнить процесс шифрования, стали соединять в ряд несколько роторов. Если, например, использовать 3 ротора, то электрический импульс проходит при шифровании по очереди через каждый из них. Поскольку на каждый ротор приходится по 26 возможных позиций, трехроторное устройство было способно породить 26×26×26 = 17 576 различных шифровальных алфавитов. После зашифровывания каждой буквы открытого текста можно было выбрать новый алфавит путем передвижения одного или более имеющихся роторов так, чтобы изменить переплетение проводов, через которые проходит ток. Хепберн построил машины с четырьмя и пятью роторами. Роторы поворачивались не одновременно. Один из роторов вступал в работу при шифровании каждой буквы; он считался «быстрым». Другой ротор вступал в работу только один раз в течение каждого оборота быстрого ротора и назывался «средним» ротором. «Медленный» же ротор вступал в работу один раз за период обращения среднего ротора. Таким образом, машина Хепберна могла порождать огромное множество шифровальных алфавитов, причем для шифрования каждой новой буквы открытого текста использовался полностью новый алфавит. Более того, роторы в машине Хепберна могли, при желании, выниматься и переставляться в произвольном порядке. Еще одной переменной величиной при шифровании того или иного сообщения этой машиной являлось исходное положение роторов.

В Европе наиболее известная роторная шифровальная машина под названием «Энигма» (в переводе с латыни – «Загадка») была разработана Артуром Шербиусом. От машины Хепберна Энигма отличалась тем, что в ней ток проходил через роторы дважды различными путями. Достигнув последнего ротора, ток разворачивался с помощью рефлектора и направлялся в обратном направлении. В результате в криптограмме Энигмы ни одна буква открытого текста не могла соответствовать самой себе в шифровке, и наоборот. Более того, шифровальные алфавиты, порождаемые этой машиной, все были взаимообратными. Это означает, что если, например, буква E при определенной исходной установке машины зашифровывалась как W, то и буква W при этой установке зашифровывалась как E. Общий вид Энигмы представлен на рис. 10, а комплект роторов для нее – на рис. 11.

Рис. 10. Энигма

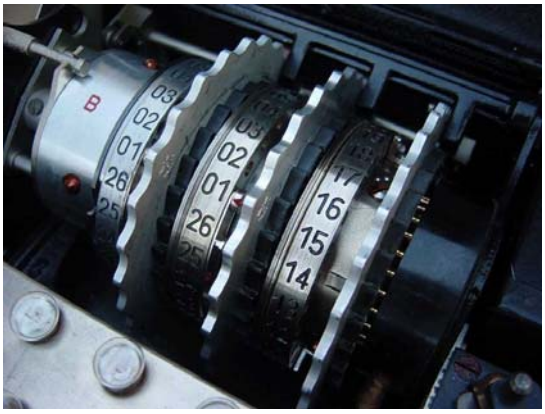

Рис. 11. Роторы Энигмы

А. Шербиус организовал фирму и занимался производством Энигмы в 1923 – 1934 гг., когда фирма была ликвидирована из-за того, что шифровальные машины не пользовались спросом. После прихода к власти в Германии Гитлера началось серьезное перевооружение армии. Немецкие криптографы модернизировали Энигму, добавив в нее коммутационную панель, позволяющую изменять схему коммутации рефлектора, и она стала широко использоваться в германской армии, ВМС и ВВС. Энигма была надежной и портативной (размером с пишущую машинку), работала от батареи, имела деревянный футляр. Ее серьезный недостаток состоял в том, что она не печатала зашифрованный текст, а показывала буквы шифротекста с помощью загорающихся лампочек. Поэтому для ее обслуживания требовалось три человека: для чтения и набора на клавиатуре текста сообщения, диктовки высвечивающихся букв шифротекста и их записи.

До 1939 г. взломом зашифрованных Энигмой криптограмм успешно занимались польские криптоаналитики, в распоряжении которых был экземпляр немецкой машины. За два месяца до захвата Польши Германскими войсками, в июле 1939 г., польские специалисты встретились со своими британскими и французскими коллегами и передали им Энигму, а также результаты своей криптоаналитической работы. Это помогло английским криптоаналитикам под руководством Алана Тьюринга спроектировать и построить первую вычислительную машину для взлома шифровок, полученных с помощью Энигмы. Эту машину назвали «Бомба» и ее несколько экземпляров до конца Второй мировой войны успешно подбирали ключи к немецким шифровкам.

Японцы для шифрования использовали машины собственной конструкции. В 1935 г. американские криптоаналитики столкнулись с японским машинным шифром, названным ими «RED». В 1936 г. Фрэнк Роулетт и Соломон Калбэк, криптоаналитики армии США, взломали шифры RED и раскрыли принцип действия японского устройства.

В 1939 г. машина RED была заменена японцами на Angooki Taipu B, или PURPLE, как ее называли американцы. Американским специалистам удалось взломать шифры этой машины и воссоздать ее устройство. PURPLE была первой из целой серии японских шифровальных машин, в конструкции которых вместо роторов применялись телефонные коммутаторы. Вслед за машинами RED и PURPLE криптоаналитики раскрыли устройство японских шифровальных машин JADE и CORAL.

В Швеции производством шифромашин занималась фирма, организованная А.Г. Даммом. Сложную и ненадежную шифромашину Дамма в 1925 г. модернизировал Борис Хагелин, который снабдил ее клавиатурой и индикаторными лампочками, как у Энигмы. Машина, получившая обозначение B-21, была роторной. Но роторы использовались для управления матричным коммутатором, в котором электрически изменялось соединение строк и столбцов для преобразования буквы открытого текста в букву шифротекста. В 1926 г. Б. Хагелин предложил B-21 Шведской армии, которая сделала на нее большой заказ. В 1927 г. Б. Хагелин выкупил у Дамма его фирму и возглавил ее. Свою следующую машину B-211 он снабдил печатающим устройством, работавшим со скоростью около 200 знаков в минуту. Она была самой портативной печатающей шифромашиной в 1934 г.

В 1927 г. французский генштаб заказал Б. Хагелину портативную шифровальную машину, которая могла бы обслуживаться одним человеком. Через некоторое время такая машина на цевочных дисках (рис. 12), получившая обозначение C-36, была изготовлена.

Рис. 12. Шифровальная машина С-36

По размерам она была меньше телефонного аппарата, весила вместе с футляром около двух с половиной килограммов. Французы сразу же сделали заказ на 5 машин. Позднее машина была существенно усовершенствована и в 1939 г. взята на вооружение Американской армии. У американцев она называлась М-209 (рис. 13) и использовалась на протяжении всей Второй мировой войны. Всего было произведено около 140 тыс. таких машин. Позже фирма Хагелина стала производить широко известные машины С-48, С-52, Т-55 и многие другие.

Рис. 13. Шифровальная машина М-209

В СССР серийное производство шифровальных машин началось в 1938 г. Первой была шифровальная машина В-4, разработанная под руководством И.П. Волоска. Модернизированный вариант назывался М-100 и производился с 1940 г. параллельно с В-4. Общий вес одного комплекта В-4 достигал 141 килограмма, тем не менее эта техника успешно использовалась во время боевых действий в Испании, на Хасане и Халхин-Голе. В 1939 г. произведена закупка 100 американских автобусов «Студебеккер», которые были переоборудованы для перевозки тяжелой шифровальной техники. В результате повысились конспирация органов шифрования и их мобильность при передислокации войск.

В 1939 г. запущена в производство малогабаритная дисковая шифровальная машина К-37 («Кристалл»), разработанная под руководством В.Н. Рытова и предназначенная для замены ручных шифров в оперативном звене управления (армия - корпус - дивизия). Это было достаточно компактное устройство весом 19 килограммов, выпуск которого продолжался до 1946 г.

Таким образом, перед Второй мировой войной все ведущие страны имели на вооружении электромеханические шифровальные системы, обладающие высокой скоростью обработки информации и высокой стойкостью. Считалось, что применяемые системы недешифруемы, но, как уже было отмечено выше, криптоаналитики их успешно взламывали.

Отечественные шифровальные машины, созданные в послевоенное время, не уступали зарубежным аналогам. В качестве примера на рис. 14 представлена шифровальная машина «Фиалка» со снятым кожухом, в которой использовалось 10 роторов.

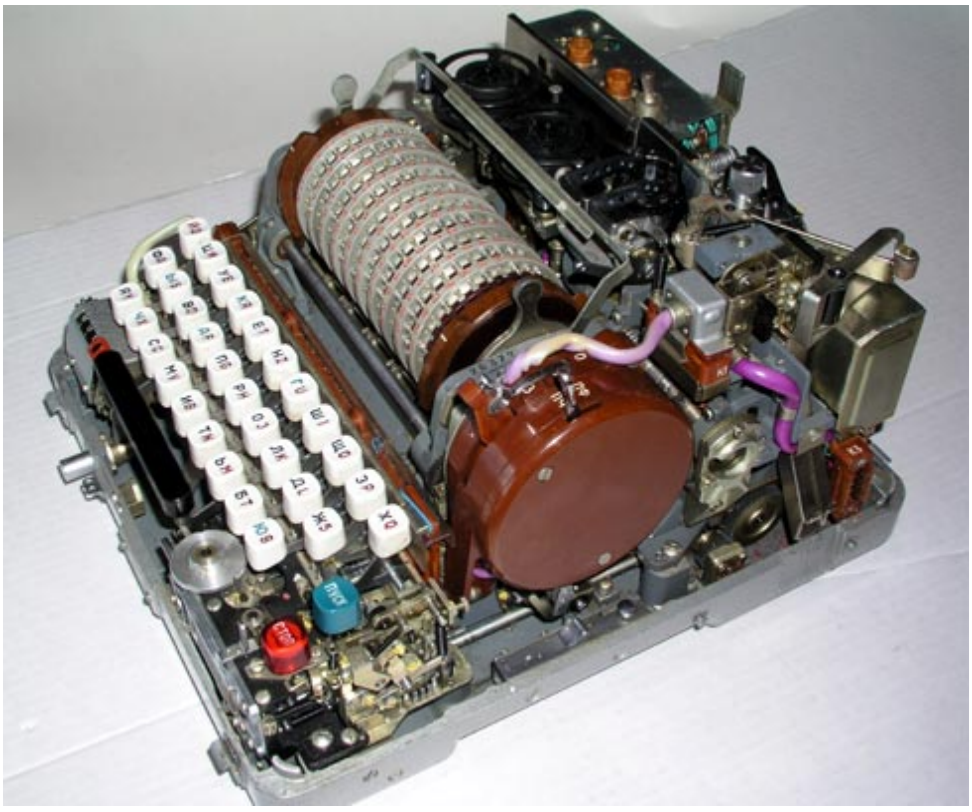

Рис. 14. Шифровальная машина «Фиалка»

3. Классификация криптографических алгоритмов

При использовании эффективного криптографического алгоритма и соблюдении условий секретности и целостности ключа криптографические преобразования позволяют защитить информацию от лиц, не владеющих ключом, и обеспечить с требуемой надежностью обнаружение несанкционированных искажений информации. Некриптографические средства защиты, такие, как системы доступа, охрана, сигнализация, сейфы и так далее, не в состоянии обеспечить такую же степень защиты информации и требуют больших затрат.

Криптографические алгоритмы подразделяются на симметричные алгоритмы с одним секретным ключом и на асимметричные алгоритмы с секретным и открытым ключами, которые математически связаны друг с другом.

В симметричных криптосистемах информация зашифровывается и расшифровывается с помощью одного и того же секретного ключа. Что касается асимметричных криптосистем, то в них информация зашифровывается с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

В настоящее время известно большое число криптографических алгоритмов. Их классификация (рис. 15) может быть осуществлена по следующим признакам:

- по типу ключей;
- по размеру блока информации;
- по характеру преобразований, производимых над данными.

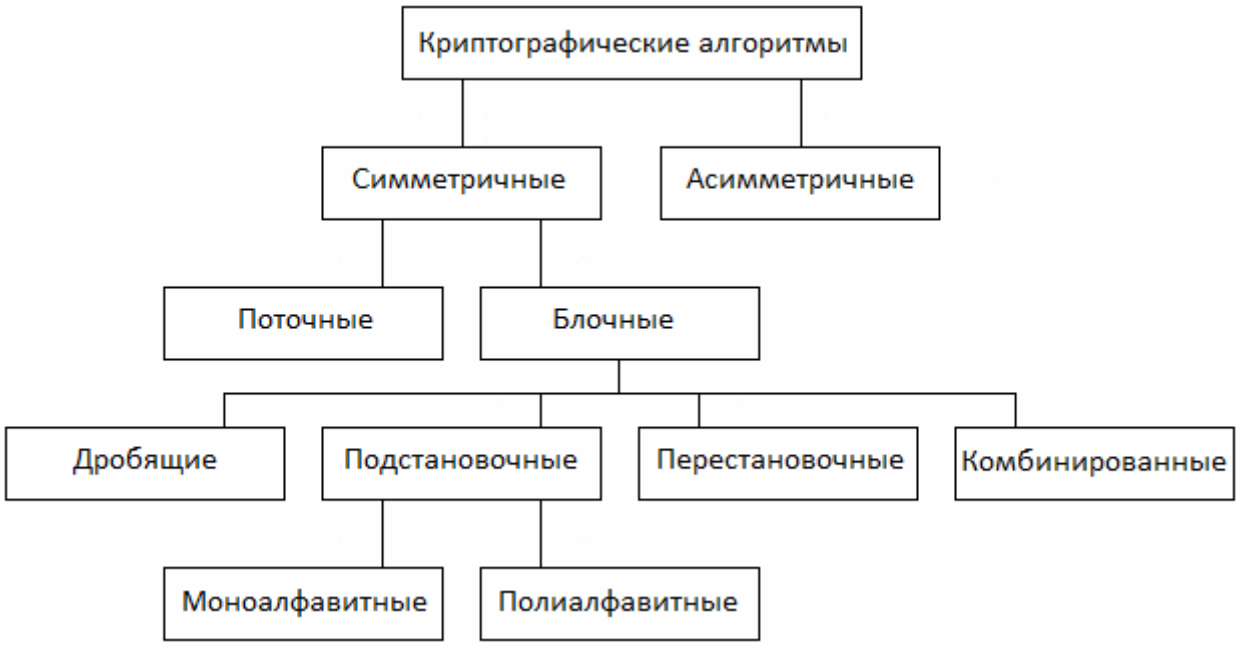

Рис. 15. Общая классификация криптографических алгоритмов

В общем случае при организации канала связи между отправителем и получателем секретной информации может использоваться секретный алгоритм криптографического преобразования информации, не требующий защищенного канала для передачи ключей, так как в этом случае ключом может быть сам алгоритм. Современная криптография секретные алгоритмы не применяет, она использует только алгоритмы с секретными ключами, основываясь на принципах Огюста Керкгоффса (Голландия), который сформулировал их в книге «Военная криптография» в 80-х гг. XIX в.

Согласно одному из принципов Керкгоффса, противник, пытающийся вскрыть перехваченное зашифрованное сообщение, знает шифр, использованный при его шифровании, то есть алгоритм криптографического преобразования сообщения. Поэтому защита должна основываться только на секретном, неизвестном противнику ключе шифра. Это обусловлено тем, что защищенность системы не должна зависеть от секретности чего-либо, что невозможно быстро изменить в случае утечки секретной информации. А изменить ключ шифрования на практике гораздо проще, чем весь используемый в системе алгоритм.

Криптографические алгоритмы с секретными ключами делятся на симметричные (с одним секретным ключом, по которому производится шифрование и дешифрование информации) и асимметричные (с открытым и секретным ключами). Модель симметричной системы шифрования представлена на рис. 16.

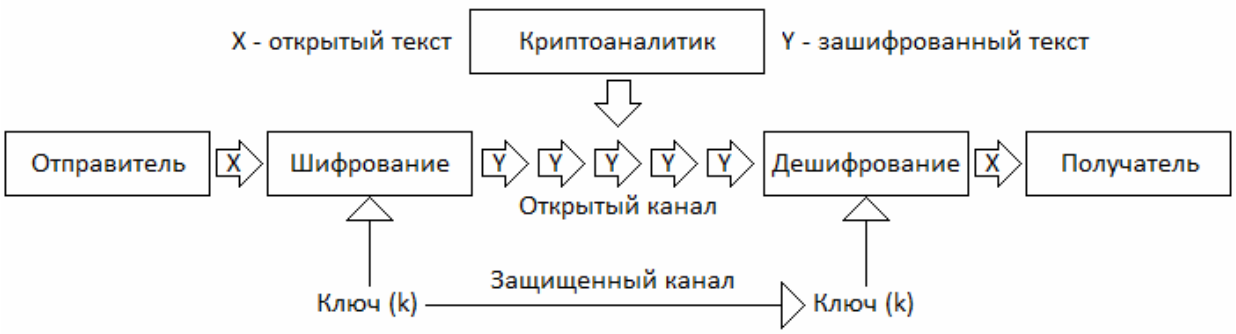

Рис. 16. Обобщенная модель симметричной системы шифрования

Отличительной чертой симметричных алгоритмов шифрования является наличие одного ключа шифрования (k на рис. 16), который должен быть известен только отправителю и получателю сообщения. Отправитель с помощью ключа k шифрует сообщение, получатель дешифрует полученную криптограмму ключом k. Криптоаналитик может перехватить зашифрованный текст Y, передаваемый по открытому каналу связи, но, так как он не знает ключа, задача вскрытия зашифрованного текста является очень трудоемкой. Принципиальным моментом является необходимость наличия секретного канала связи между получателем и отправителем для передачи ключа шифрования, исключающего возможность его перехвата криптоаналитиком.

Модель асимметричной системы шифрования представлена на рис. 17.

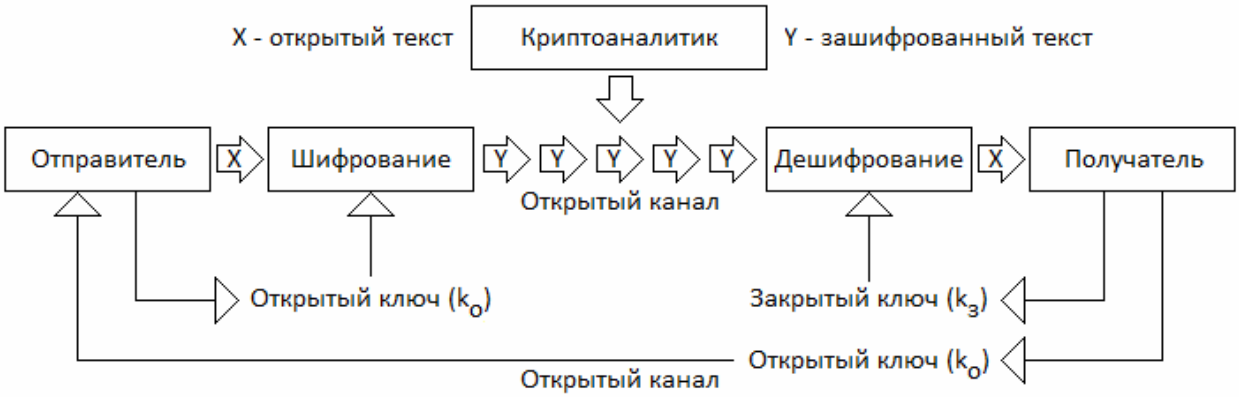

Рис. 17. Обобщенная модель асимметричной системы шифрования

Отличительной особенностью асимметричных алгоритмов является наличие пары ключей шифрования: открытого k_o, который передается второй стороне по незащищенному каналу связи и поэтому может быть известен криптоаналитику, а также закрытого $k_з$, который известен лишь одному человеку (получателю сообщения) и держится в секрете. Пара ключей обладает тем свойством, что сообщение, зашифрованное с помощью открытого ключа, может быть дешифровано только с помощью закрытого ключа.

В зависимости от размера блока шифруемой информации алгоритмы шифрования делятся на блочные и поточные. Поточный шифр – это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. При блочном шифровании открытый текст разбивается на блоки равной длины, наряду с этим совпадающие блоки при данном ключе всегда шифруются одинаково.

Еще одним критерием классификации криптоалгоритмов является тип выполняемых преобразований над блоками открытого текста. По данному критерию криптоалгоритмы разделяют на подстановочные и перестановочные. Подстановочные шифры (шифры замены) изменяют буквы текста или блоки информации по определенным законам. В перестановочных шифрах буквы текста или блоки информации не изменяются сами по себе, но изменяется их порядок следования.

Деление криптоалгоритмов на моноалфавитные и полиалфавитные характерно для подстановочных шифров. Моноалфавитные криптоалгоритмы заменяют блок входного текста (символ входного алфавита) на один и тот же блок шифротекта (символ выходного алфавита). В полиалфавитных шифрах одному и тому же блоку входного текста могут соответствовать разные блоки шифротекста, что существенно затрудняет криптоанализ.

По степени секретности криптоалгоритмы делятся на абсолютно стойкие и практически стойкие. Абсолютно стойкие шифры невозможно вскрыть. На практике этого можно добиться, только если размер используемого ключа шифрования превышает размер кодируемого сообщения и при этом ключ ис-

пользуется однократно. Практически стойким называется шифр, для которого не существует более эффективного способа взлома, кроме как полным перебором всех возможных ключей шифрования.

Современные алгоритмы шифрования возникли на базе развития и совершенствования простейших шифров путем устранения имеющихся у них недостатков. Большинство современных шифров можно рассматривать как усиление и модернизацию разработанных ранее шифров простой замены и перестановки. Известно, что недостатком шифров простой замены является возможность их взлома, если велико соотношение между объемом зашифрованного материала и размером алфавита открытого и шифрованного текстов. Но шифр простой замены сложно вскрыть, если это соотношение мало. Поэтому при модернизации таких шифров нужно минимизировать указанный параметр. Делают это двумя способами: увеличивают алфавит либо уменьшают объем сообщения, шифруемого с помощью одной и той же замены. Первый путь (увеличение алфавита) реализован в шифрах многозначной замены, в кодах и в современных блочных шифрах. По второму пути (уменьшение числа знаков, шифруемых по одной замене) пошли при создании поточных шифров замены.

Поскольку за многовековую историю развития криптологии было разработано множество различных шифров, которые невозможно рассмотреть в рамках данного пособия, далее будут представлены только наиболее значимые классические алгоритмы криптографического преобразования информации.

4. Шифры подстановки (замены)

Наиболее часто используемыми шифрами являются шифры подстановки, или замены. Они характеризуются тем, что отдельные части сообщения, например, символы заменяются на какие-либо другие символы. При этом замена осуществляется так, чтобы потом по шифрованному сообщению можно было однозначно восстановить передаваемое сообщение.

При шифровании применяют 5 типов подстановок:

1. Моноалфавитные подстановки. Используется один алфавит замены (одинаковые буквы исходного текста заменяются одним и тем же символом из алфавита замены).

2. Гомофонические подстановки. Такие подстановки также являются моноалфавитными, но при этом для замены одной буквы исходного алфавита используется несколько различных символов алфавита замены.

3. Полиграммные подстановки (символы исходного текста заменяются не по одному, а группами, например, «ЛА» на «ПР», «ВЕ» на «КО» и т.д.).

4. Полиалфавитные подстановки (одна и та же буква может быть заменена на символы из нескольких различных алфавитов замены. Например, в зависимости от порядкового номера символа в исходном тексте алфавиты замены

могут выбираться последовательно, без ключа, или в соответствии с ключом, циклически).

5. Многопетлевые полиалфавитные подстановки. В многопетлевых шифрах используется не один, а несколько ключей, называемых петлевыми, или первичными, и позволяющих существенно увеличить число вариантов замены при шифровании.

Рассмотрим принципы шифрования с помощью подстановочных шифров. Пусть, например, зашифровывается сообщение на русском языке и при этом замене подлежит каждая буква сообщения. Формально в данном случае шифр замены можно описать следующим образом. Для каждого i-го символа исходного алфавита (i изменяется от 1 до n, где n – число символов или мощность алфавита) строится некоторое множество символов M_i так, что множества M_1, M_2,…, M_i, M_{i+1},…, M_n попарно не пересекаются, то есть любые два таких множества не содержат одинаковых элементов. Множество M называется множеством шифрообозначений для i-го символа.

Представленная на рис. 18 таблица является ключом шифра замены. Зная таблицу, можно осуществить как шифрование, так и дешифрование.

А	*Б*	*В*	*Г*	. . .	*Я*
$M_а$	$M_б$	$M_в$	$M_г$		$M_я$

Рис. 18. Общий вид табличного ключа замены

При шифровании все буквы *А* открытого сообщения, начиная с первой, заменяются любыми символами из множества $M_а$. Если в сообщении содержится несколько букв *А*, то при их замене следует в любом порядке перебирать заменяющие символы из $M_а$. За счет этого, с помощью одного ключа (рис. 18) можно получить различные варианты зашифрованного сообщения для одного и того же открытого сообщения. Например, если ключом шифра замены является таблица на рис. 19,

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	Ъ	Ы	Ь	Э	Ю	Я
23	33	13	18	45	31	19	11	27	40	32	30	14	25	17	83	51	66	93	73	10	60	99	82	74	28	21	54	57	29	88	28
44	12	98	39	15	34	85	70	35	05	42	24	16	84	20	48	36	77	91	81	71	61	56	95	63	76	67	55	94	68	92	72
37	38	41	43	46	47	49	50	52	80	07	53	58	59	62	64	65	69	79	75	78	86	87	89	90	96	97	98	25	22	26	27

,

Рис. 19. Пример ключа замены

то сообщение «ПОТЕРЯЛ УПРАВЛЕНИЕ» может быть зашифровано любым из трех способов, представленных на рис. 20.

48	17	79	31	65	27	30	75	83	51	23	41	53	47	25	52	31
64	20	91	34	36	72	24	81	48	36	44	98	30	31	84	27	47
83	62	93	47	51	28	53	73	64	65	37	13	24	34	59	35	34

Рис. 20. Три варианта криптограмм для использованного в примере ключа

Так как множества $M_а$, $M_б$, $M_в$, ..., $M_я$ попарно не пересекаются, то по каждому символу шифрованного сообщения можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому дешифрование возможно, и открытое сообщение определяется единственным образом.

Рассмотрим наиболее характерные примеры шифров замены и соответствующие им криптографические алгоритмы.

4.1. Моноалфавитные подстановки

4.1.1. Шифры равнозначной замены

В шифрах равнозначной замены при шифровании один символ исходного текста заменяется на один символ алфавита шифрования. К таким шифрам относятся некоторые древние шифры, а также шифры, известные из художественной литературы. Например, шифр, описанный в рассказе «Пляшущие человечки» А. Конан Дойла.

Пусть каждое множество M_i состоит из одной буквы, как на рис. 21.

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

Рис. 21. Шифр простой однобуквенной замены

Такой шифр называется шифром простой однобуквенной замены, или алфавитной подстановкой. При зашифровании каждая буква открытого текста заменяется на соответствующую букву из второй строки (А на Л, Б на Ф и т.д.). При расшифровании, наоборот, Л заменяется на А и т.д. В данном случае ключ представляет собой произвольный порядок букв алфавита, который запомнить достаточно сложно. Поэтому всегда пытались придумать какое-либо правило, облегчающее запоминание ключа.

Некоторые фрагменты библейских текстов зашифрованы с помощью шифра под названием «атбаш». Правило зашифрования состояло в замене i-й буквы алфавита буквой с номером n−i+ 1, где n – число букв в алфавите. Происхождение слова «атбаш» объясняется принципом замены букв. Это слово составлено из букв «Алеф», «Тав», «Бет», «Шин», то есть первой и последней, второй и предпоследней букв древнесемитского алфавита. Для русского алфавита такой шифр может быть представлен следующей ключевой таблицей (рис. 22).

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

Рис. 22. Шифр атбаш для русского алфавита

Другим примером шифра с легко запоминаемым ключом может служить шифр Цезаря. Для него вторая строка ключевой таблицы является последовательностью, записанной в алфавитном порядке, но сдвинутой по алфавиту циклически вправо на 3 буквы. Ключевая таблица этого шифра для русского алфавита приведена ниже на рис. 23.

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

Рис. 23. Шифр Цезаря для русского алфавита

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

$$y = (x + k) \bmod n;$$
$$x = (y - k) \bmod n,$$

где:
x – символ открытого текста,
y – символ шифрованного текста,
n – мощность алфавита (количество символов),
k – ключ.

Для шифра Цезаря ключ равен 3, а в общем случае он может принимать любые значения от 1 до n - 1. Зашифруем, например, слово «криптография» шифром Цезаря с ключом $k = 4$. Для проверки правильности шифрования ниже приведена таблица с числовыми эквивалентами букв русского алфавита (рис. 24).

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	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Рис. 24. Числовые эквиваленты букв русского алфавита

Результат шифрования содержится в таблице на рис. 25.

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
x_i	10	16	8	15	18	14	3	16	0	20	8	31
$(x_i + k) \bmod 32$	14	20	12	19	22	18	7	20	4	24	12	3
Результат	О	Ф	М	У	Ц	Т	З	Ф	Д	Ш	М	Г

Рис. 25. Пример шифрования с помощью шифра Цезаря с ключом 4

Часто для получения ключевого алфавита используется так называемый лозунг – легко запоминаемое слово или фраза. Ключевой алфавит формируют из последовательности неповторяющихся букв лозунга и букв алфавита, не входящих в лозунг. Например, выберем слово-лозунг «БУЛОЧНАЯ» и заполним вторую строку таблицы по следующему правилу: сначала заносим в нее

слово-лозунг, удаляя из него повторяющиеся буквы, а затем записываем в алфавитном порядке буквы алфавита, не вошедшие в слово-лозунг. Ключевая таблица для рассматриваемого шифра в результате примет следующий вид (рис. 26).

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

Рис. 26. Пример лозунгового шифра

В лозунговом шифре, в отличие, например, от шифра Цезаря, число вариантов ключа существенно больше числа букв алфавита.

Общим недостатком моноалфавитных шифров равнозначной замены, в которых один символ исходного текста заменяется одним символом шифрованного текста, является их раскрываемость с помощью частотного анализа. Шифр Цезаря, кроме этого, характеризуется небольшим количеством возможных ключей, их всего 31 для русского алфавита из 32 символов. То есть взломать шифр можно максимум за 31 шаг перебором возможных ключей.

В XVI в. криптограф Папы Римского Маттео Ардженти для затруднения вскрытия шифрованных текстов с помощью частотного анализа предложил скрывать истинную частоту букв в этих текстах путем замены букв либо на цифры (от 0 до 9), либо на числа (от 00 до 99). Чтобы однозначно отличать цифры и двузначные числа в шифрованных текстах при их дешифровании, цифры, входящие в алфавит замены, не должны входить в двузначные числа алфавита замены. При этом можно было использовать лишь часть цифр. Чтобы скрыть их малую частоту появления в шифротексте, Ардженти рекомендовал обозначать цифрами буквы, наиболее часто встречающиеся в открытых текстах. Таким образом, Ардженти предложил один из способов изменения частотных характеристик букв – использование разнозначной замены, когда каждой букве исходного текста ставится в соответствие один или два символа при шифровании. Ключевая таблица простейшего шифра разнозначной замены для русского алфавита приведена ниже на рис. 27. В ней используется только 4 цифры (6, 7, 8 и 9), причем они не входят в двузначные числа этой таблицы.

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	Ъ	Ы	Ь	Э	Ю	Я
6	12	14	32	45	7	43	54	52	22	31	24	53	42	9	35	23	44	11	41	30	8	20	13	50	34	40	55	21	51	25	33

Рис. 27. Шифр разнозначной замены

Текст, шифрованный с помощью такого шифра и записанный без пробелов, сложно разбить на отдельные символы, что затрудняет его вскрытие противником. При этом шифрованный текст однозначно дешифруется с помощью ключа. Расшифруем, например, следующую криптограмму: 11923357455223914642427118945 6. Для этого выделим в ней отдельные символы с помощью ключевой таблицы. Криптограмма однозначно может быть разделена на 19 символов – 11 9 23 35 7 45 52 23 9 14 6 42 42 7 11 8 9 45 6, что соответствует зашифрованному тексту – ТОРПЕДИРОВАН НЕТ ХОДА.

При вскрытии шифра противник может разбить эту же криптограмму на 15 символов следующим образом – 11 92 33 57 45 52 23 91 46 42 42 71 18 94 56, предположив, что каждому символу в криптограмме соответствует двузначное число. Это не позволит прочесть зашифрованный текст с помощью частотного анализа.

4.1.2. Шифры пропорциональной замены (гомофонические подстановки)

Шифры пропорциональной замены обеспечивают простейшую защиту от криптоаналитических атак, основанных на подсчете частот появления букв в шифротексте. Данные шифры являются моноалфавитными, но количество символов, входящих в алфавит замены, существенно превышает число символов исходного алфавита. Это позволяет использовать для замены одной буквы исходного алфавита более одного символа алфавита замены. Число заменяющих символов для конкретной буквы выбирается пропорционально вероятности появления этой буквы в открытых текстах.

Данные о распределениях вероятностей букв в русском и английском текстах приведены в таблицах на рис. 28 и 29 соответственно. Буквы в таблицах указаны в порядке убывания вероятности их появления в тексте. Например, русская буква Е встречается в 36 раз чаще, чем буква Ф, а английская буква Е встречается в 123 раза чаще, чем буква Z.

Шифруя букву исходного сообщения, случайным образом выбирают один из символов, предназначенных для замены данной буквы. Заменяющие символы, называемые омофонами, могут быть представлены числами от 00 до 99 или числами от 000 до 999. Например, округлив в английском алфавите вероятности букв до двух знаков после запятой, можно установить, что букве Е следует выделить 12 омофонов из диапазона 00 – 99, буквам В и G по 2 омофона, а буквам V, K, Q, X, J и Z по 1 омофону и т.д. Возможное распределение омофонов представлено на рис. 30.

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
␣	0,175	Р	0,040	Я	0,018	Х	0,009
О	0,090	В	0,038	Ы	0,016	Ж	0,007
Е	0,072	Л	0,035	З	0,016	Ю	0,006
А	0,062	К	0,028	Ъ	0,014	Ш	0,006
И	0,062	М	0,026	Б	0,014	Ц	0,004
Н	0,053	Д	0,025	Г	0,013	Щ	0,003
Т	0,053	П	0,023	Ч	0,012	Э	0,003
С	0,045	У	0,021	Й	0,010	Ф	0,002

Рис. 28. Таблица распределения вероятностей русских букв

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
E	0,123	L	0,040	B	0,016
T	0,096	D	0,036	G	0,016
A	0,081	C	0,032	V	0,009
O	0,079	U	0,031	K	0,005
N	0,072	P	0,023	Q	0,002
I	0,071	F	0,023	X	0,002
S	0,066	M	0,022	J	0,001
R	0,060	W	0,020	Z	0,001
H	0,051	Y	0,019		

Рис. 29. Таблица распределения вероятностей латинских букв

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55				93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Рис. 30. Пример распределения омофонов для латинских букв

Если омофоны выделяются случайным образом и для замены букв в тексте омофоны также выбираются случайно, тогда каждый омофон появляется в шифротексте с одинаковой вероятностью. Взломать такой шифр с помощью частотного анализа невозможно. Вместе с тем, стойкость шифра пропорциональной замены к частотному анализу может быть повышена путем увеличения количества омофонов, используемых при шифровании, например, выбирая их из диапазона 000 – 999. Однако это приводит к усложнению процедур шифрования и дешифрования.

4.2. Шифры многозначной замены

Шифры многозначной замены также позволяют изменить частотные свойства криптограмм. Но для данных шифров число заменяющих символов для конкретной буквы не пропорционально вероятности появления этой буквы в открытых текстах. Примером шифра многозначной замены является книжный шифр, в котором в качестве ключа используется страница одной и той же книги. При шифровании буквы открытого сообщения находят на заданной странице и обозначают парой чисел – номером строки и номером буквы в строке, а при дешифровании по этим обозначениям восстанавливают исходный текст. Поскольку на странице расположено множество одинаковых букв, то одна и та

же буква в криптограмме будет иметь различные обозначения и частотный анализ не позволит восстановить исходный текст.

Книжные шифры обладали значительно большей криптографической стойкостью по сравнению с шифрами простой замены. Но наличие книги-ключа является недостатком книжного шифра, поскольку ключевую книгу можно определить по наличию ее у всех корреспондентов, например, при обнаружении сети связи. Поэтому часто вместо книжного шифра использовался шифр «по слову», который является упрощенным аналогом книжного шифра.

В шифре «по слову» ключом является заранее оговоренное слово, словосочетание или фраза. По нему строится таблица замены. Пусть, например, этим словом является слово «ПРЕКРАСНАЯ». Поскольку в заданном слове 10 букв, то по нему строится таблица шифрования, содержащая 10 строк и 10 столбцов пронумерованных цифрами от 0 до 9. В первый столбец этой таблицы записывают буквы выбранного слова, каждая буква построчно разворачивается в последовательность букв русского алфавита (циклически). В результате получается таблица (рис. 31), которая при шифровании и дешифровании используется в качестве страницы книги-ключа.

	0	1	2	3	4	5	6	7	8	9
0	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
1	Р	С	Т	У	Ф	Х	Ц	Ш	Ь	Э
2	Е	Ж	З	И	К	Л	М	Н	О	П
3	К	Л	М	Н	О	П	Р	С	Т	У
4	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Ь
5	А	Б	В	Г	Д	Е	Ж	З	И	К
6	С	Т	У	Ф	Х	Ц	Ш	Ь	Э	Ю
7	Н	О	П	Р	С	Т	У	Ф	Х	Ц
8	А	Б	В	Г	Д	Е	Ж	З	И	К
9	Я	А	Б	В	Г	Д	Е	Ж	З	И

Рис. 31. Пример шифра «по слову»

По такой таблице производилась замена букв открытого текста на их координаты (первая цифра – номер строки, вторая – номер столбца), причем число обозначений для одной и той же буквы определялось числом таких букв в таблице, например, буква П могла быть зашифрована числами 00, 29, 35 или 72. В результате одинаковые слова открытого сообщения также шифровались различным образом. Так, слово «агент» в криптограмме могло быть представлено как: «80 53 20 27 38» или «91 83 96 70 03» и т.д.

4.3. Полиграммные шифры

Изменить частотные свойства, характерные для открытых текстов, можно путем шифрования не отдельных символов, а групп символов – полиграмм (биграмм, триграмм и т.д.). Например, при использовании латинского алфавита количество биграмм равно 26×26=676, то есть при проведении частотного ана-

лиза требуется определять частоту не 26 букв, как в шифрах равнозначной замены, а 676 биграмм. Это значительно труднее и требует намного большего объема зашифрованного текста. Рассмотрим в качестве примера наиболее известный биграммный шифр замены – шифр Плейфера. Как уже было отмечено ранее, он изобретен в 1854 г. Чарльзом Уитстоном, но назван именем Лорда Лайона Плейфера, который способствовал внедрению и использованию данного шифра в Великобритании.

Основой шифра Плейфера является таблица со случайно расположенными символами алфавита, которая является ключом шифра. В целях удобства запоминания таблицы шифрования обычно для ее формирования используется лозунг (ключевое слово или фраза), символами которого заполняют начальные строки таблицы без повторения. Оставшаяся часть таблицы заполняется символами, не входящими в лозунг. Для русского языка шифрующая таблица с ключевым словом «КОМАНДИР» может быть задана следующим образом (рис. 32).

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

Рис. 32. Пример заполнения таблицы шифрования для шифра Плейфера

Рассмотрим процесс шифрования исходного текста «СИЛОВАЯ УСТАНОВКА ПОВРЕЖДЕНА» с помощью шифра Плейфера. При шифровании исходный текст разбивается на пары символов X_i и X_i+1, которые называют биграммами. При этом биграммы не должны содержать одинаковых символов. При появлении таких биграмм следует изменить исходный текст, например, вставкой какого-либо разделяющего символа между повторяющимися буквами в тексте (ПР | ОГ | РА | МЪ | МА). Вставка дополнительного символа, например, перед шифруемым текстом или после него, используется также при нечетном числе символов в тексте (ЫТОРПЕДА, ТОРПЕДАЫ).

Для рассматриваемого примера разбивка на биграммы выполняется без проблем:

СИ | ЛО | ВА | ЯУ | СТ | АН | ОВ | КА | ПО | ВР | ЕЖ | ДЕ | НА.

Шифрование биграмм производится по следующим правилам:

- если буквы биграммы находятся в одной строке таблицы шифрования, то каждую из них следует заменить буквой, расположенной справа от нее (последняя буква в строке заменяется первой);
- если буквы биграммы находятся в одном столбце, то каждую из них следует заменить буквой, расположенной под ней в столбце (нижняя буква в столбце заменяется верхней);
- если буквы биграммы находятся в разных строках и столбцах, то каждую из них следует заменить буквой, расположенной на пересечении строки, содержащей эту букву, и столбца, содержащего другую букву.

Применение этих правил для рассматриваемого примера позволяет получить следующий шифротекст:

ЦО | ВР | ЕО | ЫЧ | ТУ | НД | ВС | ОН | СК | ЛО | ЖЗ | АЗ | ДН.

Рассмотрим, каким образом выполняется замена букв первой биграммы, которые выделены в приведенной на рис. 33 таблице шифрования волнистой рамкой (буквы этой биграммы расположены в разных строках и столбцах таблицы). Первая буква этой биграммы (С) находится в строке 3, а вторая (И) – в столбце 7. На пересечении строки 3 и столбца 7 расположена буква Ц, на которую заменяется буква С первой биграммы. Вторая буква первой биграммы (И) находится в строке 1, а первая (С) – в столбце 2. На пересечении строки 1 и столбца 2 расположена буква О, на которую заменяется буква И первой биграммы.

	1	2	3	4	5	6	7	8
1	К	О	М	А	Н	Д	И	Р
2	Б	В	Г	Е	Ж	З	Й	Л
3	П	С	Т	У	Ф	Х	Ц	Ч
4	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Рис. 33. Пример шифрования для шифра Плейфера

Дешифрование криптограммы, полученной с помощью шифра Плейфера, выполняется аналогично шифрованию.

В 1914 г. шифр Плейфера был взломан лейтенантом Джозефом О. Моуборном, который опубликовал алгоритм взлома. Впоследствии немцы модернизировали этот шифр, добавив в него вторую таблицу шифрования. В результате был получен достаточно надежный и удобный в применении шифр для ручного шифрования, который они называли «Два квадрата», а сейчас его называют «Двойной квадрат Уитстона». Немецкая армия, ВВС и полиция использовали шифр «Два квадрата» во время Второй мировой войны в тактических целях для шифрования распоряжений, донесений и приказов, например, во время ведения боя, когда зашифрованная информация быстро устаревала, и к моменту взлома противником была уже бесполезна.

Рассмотрим далее шифр «Двойной квадрат Уитстона» для русского алфавита. Две шифровальные таблицы могут быть расположены по вертикали или по горизонтали и должны иметь различное заполнение символами алфавита. Выберем горизонтальное расположение таблиц, а в качестве ключа для формирования второй таблицы используем слово «ГЕРМАНИЯ». В результате получим систему, представленную на рис. 34.

Алгоритм шифрования с помощью двух таблиц рассмотрим на примере шифрования текста из предыдущего примера – «СИЛОВАЯ УСТАНОВКА ПОВРЕЖДЕНА». Для этого текста разбивка на биграммы выполнена ранее и имеет вид:

СИ | ЛО | ВА | ЯУ | СТ | АН | ОВ | КА | ПО | ВР | ЕЖ | ДЕ | НА.

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

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

Рис. 34. Пример таблиц шифрования для шифра «Двойной квадрат Уитстона»

Причем, в отличие от шифра Плейфера, биграммы для рассматриваемого шифра могут содержать одинаковые символы.

Шифрование биграмм производится по следующим правилам:

- при горизонтальном расположении таблиц шифрования первую букву биграммы находят в левой таблице, а вторую букву в правой таблице;
- если буквы биграммы находятся в разных строках, то мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника будут содержать буквы биграммы шифротекста. Причем первая буква биграммы, расположенная в левой таблице, заменяется на букву из левой таблицы, а вторая буква биграммы, расположенная в правой таблице, заменяется на букву из правой таблицы;
- если буквы биграммы исходного текста находятся в одной строке, то буквы биграммы шифротекста берут в этой же строке. Первую букву биграммы шифротекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая же буква биграммы шифротекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения;
- если буквы биграммы исходного текста находятся в одной строке и в одинаковых столбцах, то буквы биграммы шифротекста будут совпадать с буквами биграммы исходного текста.

В результате шифрования по двум таблицам получим криптограмму:

ОХ | ЧБ | ОЗ | ТУ | ЧЫ | УП | ДМ | ВЕ | НГ | ПО | ОД | ЕЖ | ОН | НА.

В нашем примере буквы трех биграмм (ПО, ЕЖ и НА) оказались расположенными в одной строке и в одинаковых столбцах и при шифровании не изменились. Рассмотрим, каким образом выполняется замена букв первой биграммы, которые выделены в приведенных на рис. 35 таблицах волнистой рамкой (буквы этой биграммы расположены в разных строках и столбцах таблицы). Первая буква этой биграммы (С) заменяется на букву О из левой таблицы, а вторая (И) – заменяется на букву Х из правой таблицы. Эти буквы расположены в углах прямоугольника, образованного строками и столбцами букв первой биграммы.

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

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

Рис. 35. Пример шифрования для шифра «Двойной квадрат Уитстона»

Далее рассмотрим, каким образом выполняется замена букв пятой биграммы (СТ), буквы которой расположены в строке 3 и выделены в таблицах шифрования на рис. 36 волнистой рамкой. Первая буква этой биграммы (С) заменяется на букву У из левой таблицы (4 столбец), так как вторая буква (Т) первой биграммы расположена в 4 столбце. Вторая буква этой биграммы (Т) заменяется на букву П из правой таблицы (2 столбец), так как первая буква (С) первой биграммы расположена во 2 столбце.

1	2	3	4	5	6	7	8	
К	О	М	А	Н	Д	И	Р	1
Б	В	Г	Е	Ж	З	Й	Л	2
П	С	Т	У	Ф	Х	Ц	Ч	3
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	4

1	2	3	4	5	6	7	8
Г	Е	Р	М	А	Н	И	Я
Б	В	Д	Ж	З	Й	К	Л
О	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Рис. 36. Замена букв, расположенных в одной строке таблиц шифрования

Дешифрование криптограммы, полученной с помощью шифра «Двойной квадрат Уитстона», выполняется аналогично шифрованию.

Для упрощения процедур шифрования и дешифрования, а также в целях исключения совпадения биграмм в исходном тексте и в криптограмме, была предложена модификация рассмотренного шифра, в которой используются четыре шифрующие таблицы. Принцип шифрования с помощью четырех таблиц поясняет рисунок (рис. 37), на котором показано, как буквы биграммы СИ исходного текста (выделены волнистой рамкой) преобразуются в буквы биграммы ХЕ криптограммы. Первая буква биграммы СИ выбирается в первой таблице, а вторая – в четвертой. Первая буква биграммы ХЕ выбирается из второй таблицы, а вторая – из третьей. Эти буквы расположены на пересечении строк и столбцов, в которых находятся буквы исходной биграммы.

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

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

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

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

Рис. 37. *Принцип шифрования шифром Уитстона с использованием 4 таблиц*

Следует отметить, что при использовании ключевого слова шифровальные таблицы имеют различное, но не случайное заполнение (последние строки у таблиц 1 и 4, а также у таблиц 2 и 3 совпадают). Уитстону принадлежит идея получения более хаотичного заполнения таблицы шифрования. В шифре Уитстона (Плейфера) требовалось заполнить латинскими буквами таблицу размером 5×5 (буквы I и J не различались).

Проиллюстрируем процесс заполнения таблицы шифрования, используя ключевое слово «MAGNETIC». По этому слову составлялась таблица размером 4×8. Буквы алфавита, не вошедшие в указанное слово, вписывались в таблицу в алфавитном порядке после ключевого слова. В нашем примере эта таблица примет следующий вид (рис. 38).

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

Рис. 38. Принцип заполнения таблицы шифрования по ключевому слову

Далее буквы выписывались по столбцам: MBQZADRGFSNHUEKVTLWI OXCPY, а затем заносились в таблицу шифрования.

В нашем примере получим следующую таблицу шифрования (рис. 39).

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

Рис. 39. Пример заполнения таблицы шифрования по вспомогательной таблице

Если бы ключевое слово сразу записывалось в шифрующую таблицу, то она бы имела менее хаотичное заполнение (рис.40).

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

Рис. 40. Пример обычного заполнения таблицы шифрования по ключевому слову

В приведенной выше таблице последняя строка оказалась заполненной алфавитом в обычной последовательности, что облегчает взлом шифра.

4.4. Полиалфавитные подстановки

В рассмотренных выше шифрах используется только один алфавит шифрования, что обуславливает их низкую стойкость к частотному анализу. Существуют шифры, в которых для шифрования применяется несколько алфавитов. Такие шифры называются полиалфавитными. Они позволяют, в отличие от простых моноалфавитных подстановок, скрыть естественную частоту появления символов в тексте, хотя сейчас известны алгоритмы взлома и таких шифров.

Первый шифр полиалфавитной подстановки был предложен в 1466 г. итальянским архитектором Леоном Баттистой Альберти (рис. 41).

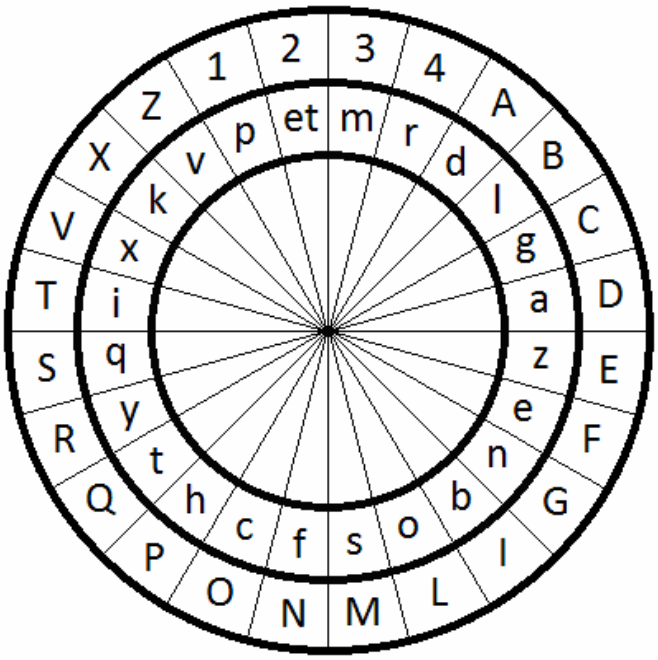

Рис. 41. Диск Альберти

Итальянский архитектор изобрел шифровальное устройство, состоящее из двух дисков различного диаметра, закрепленных на одной оси. Оба диска были разделены на 24 сектора. В сектора большого неподвижного диска были вписаны 20 букв латинского алфавита в их естественном порядке и 4 цифры (от 1 до 4). При этом из алфавита были удалены 4 буквы, которые не использовались при шифровании. В сектора малого подвижного диска были вписаны 24 буквы латинского алфавита в случайной последовательности, которая являлась первой частью составного ключа данного шифра. Вторая часть ключа – начальное положение малого диска относительно большого. Процесс шифрования заключался в нахождении буквы открытого текста на большом диске и замене ее на расположенную напротив букву малого диска. После шифрования нескольких букв, количество которых определялось заранее, малый диск поворачивался на 1 сектор относительно большого диска, при этом происходила смена алфавита шифрования. Общее число используемых алфавитов равнялось количеству символов большого диска – 24.

В своем шифровальном устройстве Альберти предложил использовать также буквенно-цифровой код, для чего на большом диске размещались 4 цифры, которые шифровались так же, как и буквы. Цифры использовались для составления двузначных, трехзначных и четырехзначных кодов, общее число которых равнялось 336, для обозначения законченных фраз. Когда такая фраза встречалась в открытом сообщении, она заменялась соответствующим кодовым обозначением, а с помощью диска цифры зашифровывались как обычные знаки открытого текста, превращаясь в буквы.

Таким образом, шифровальный диск позволял использовать так называемые коды с перешифрованием, которые получили широкое распространение лишь в конце XIX в., спустя четыре столетия после изобретения Альберти.

В 1518 г. немецкий аббат Иоганнес Тритемий предложил другой полиалфавитный шифр на основе использования специальной таблицы, которая получила название «Таблица Тритемия». Эквивалент этой таблицы для русского языка приведен на рис. 42. Она представляет собой набор расположенных друг под другом алфавитов, причем каждый последующий алфавит циклически смещен на одну букву влево, по сравнению с предыдущим. При шифровании по таблице Тритемия ключ не использовался, шифрующие алфавиты выбирались в таблице последовательно и циклически. То есть после крайнего алфавита возвращались к первому. Буквы открытого текста задавались в первой строке таблицы. Буквы криптограммы выбирались на пересечении столбца, содержащего букву открытого текста, и строки с алфавитом шифрования, соответствующей порядковому номеру буквы в тексте. Например, в слове «КУКУШКА» буква Ш стоит на пятой позиции, значит, для ее шифрования будет использован пятый алфавит шифрования. На пересечении пятой строки и столбца, начинающегося с буквы Ш, находится соответствующая буква криптограммы – Ь.

Рассмотрим процесс шифрования слова «АББАТ» с помощью данной таблицы. Первая буква открытого текста (А) задается и шифруется по первой строке, поэтому она не изменяется, и первой буквой криптограммы будет А. Вторую букву открытого текста (Б) находим также в первой строке, а соответствующую ей букву криптограммы (В) – под ней во второй строке. Третья буква открытого текста (Б) зашифровывается по третьей строке в букву Г. Четвертая буква открытого текста (А) зашифровывается по четвертой строке в букву Г, а пятая буква открытого текста (Т) зашифровывается по пятой строке в букву Ц.

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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	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	Ъ	Ы	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
Ц	Ч	Ш	Щ	Ъ	Ы	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
Ч	Ш	Щ	Ъ	Ы	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
Ш	Щ	Ъ	Ы	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
Щ	Ъ	Ы	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
Ъ	Ы	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
Ы	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	Ъ
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	Ъ	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	Ъ	Ы	Ь
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	Ъ	Ы	Ь	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	Ъ	Ы	Ь	Э	Ю

Рис. 42. Таблица Тритемия для русского алфавита

В результате получим – АВГГЦ. Одинаковые буквы открытого текста в криптограмме имеют различное обозначение, так как зашифрованы с помощью различных алфавитов.

Недостатком данного шифра является отсутствие ключа, поскольку секретность шифра обеспечивается секретностью ключа шифрования. В 1553 г. итальянец Джованни Белазо предложил использовать для шифра на основе таблицы Тритемия легко запоминающийся ключ, который он назвал паролем. Над буквами открытого текста записывались буквы пароля, по которым выбирались строки в таблице шифрования. Впоследствии идею Тритемия использовали при разработке более надежных полиалфавитных табличных шифров, среди которых следует отметить шифры Порта, Виженера и Бофора. Первый из этих шифров изобрел Джованни де ла Порта в 1563 г. На рис. 43 приведена таблица Порта для русского алфавита.

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

Рис. 43. Таблица Порта для русского языка

Таблица состоит из 16 (для русского языка) секций, каждая из которых содержит строку с первой половиной алфавита (эти строки в таблице пронумерованы) и строку со второй половиной алфавита, буквы которой расположены в алфавитном порядке только в первой секции, а в остальных сдвинуты циклически влево на одну букву, по сравнению с предыдущей. Прописные буквы в начале строк образуют столбец для выбора алфавита шифрования. Шифрование осуществляется при помощи ключа, который записывают над открытым текстом, циклически повторяя. По букве ключа в столбце с прописными буквами определяется секция с алфавитом шифрования (каждой секции соответст-

вуют две буквы ключа). Расположенная под буквой ключа буква открытого текста ищется в верхнем или нижнем полуалфавите секции и заменяется соответствующей ей буквой второго полуалфавита.

Зашифруем, например, сообщение «снаряды закончились» с помощью таблицы Порта, используя ключ «крепость» (рис. 44). Первой букве ключа (К) соответствует 6 секция таблицы, шифруемая буква С расположена в нижнем полуалфавите секции, над буквой С в верхнем полуалфавите находится первая буква криптограммы – М. Второй букве ключа (Р) соответствует секция 9, в которой букве сообщения Н (верхний полуалфавит) соответствует вторая буква криптограммы – Х (нижний полуалфавит). Третьей букве ключа (Е) соответствует секция 3, в которой букве сообщения А (верхний полуалфавит) соответствует третья буква криптограммы – Т (нижний полуалфавит).

Ключ	К	Р	Е	П	О	С	Т	Ь	К	Р	Е	П	О	С	Т	Ь	К	Р
Сообщение	С	Н	А	Р	Я	Д	Ы	З	А	К	О	Н	Ч	И	Л	И	С	Ь
Криптограмма	М	Х	Т	Й	И	Ь	В	Х	Х	Т	Р	Ф	А	Р	Ф	Ц	М	Д

Рис. 44. Пример шифрования по таблице Порта

Оставшуюся часть сообщения шифруем аналогично, в результате получаем криптограмму: МХТЙИЬВХХТРФАРФЦМД.

Алгоритм дешифрования криптограммы по таблице Порта совпадает с алгоритмом шифрования открытого сообщения.

За этот шифр Джованни де ла Порта позднее стали называть отцом криптографии, хотя изобретенная им система шифрования редко использовалась современниками, которые считали ее слишком сложной. Здесь следует упомянуть историю с биграммным шифром Уитстона, который в Министерстве иностранных дел Великобритании также посчитали слишком сложным и не захотели использовать. Причем когда Уитстон предложил за 15 минут научить трех мальчиков из соседней школы применять этот шифр, заместитель министра иностранных дел ответил: «Это очень возможно, но вы никогда не научили бы этому атташе».

Но не все дипломаты были узкими специалистами. Так, наиболее известным полиалфавитным шифром является шифр французского дипломата Виженера, описание которого содержится в его книге «Трактат о шифрах», изданной в 1586 г. Таблица Тритемия в предложенном шифре модернизировалась, над таблицей размещалась дополнительная строка, а слева – дополнительный столбец, которые содержали алфавиты в их естественном порядке (рис. 45).

Такая таблица впоследствии стала называться таблицей Виженера. Виженер предложил использовать в качестве ключа для таблицы текст самого сообщения или же шифрованный текст. Такой ключ позже стали называть автоключом. Первая строка использовалась для задания букв открытого текста, а первый столбец – для выбора алфавита шифрования по букве ключа. В настоящее время под шифром Виженера понимают его простейший вариант с коротким ключом. При шифровании ключ, циклически повторяя, записывают над шифруемым текстом. Буква открытого текста в первой строке задает столбец

таблицы шифрования, а расположенная над ней буква ключа в первом столбце задает строку таблицы шифрования, на пересечении которых располагается соответствующая буква криптограммы.

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

Рис. 45. Таблица Виженера для русского алфавита

При применении в качестве ключа открытого сообщения Виженер предлагал в качестве первой буквы ключа использовать букву, известную отправителю и получателю, эта буква позволяла получателю начать дешифрование криптограммы, не зная открытого текста, то есть ключа. Зашифруем по таблице Виженера, например, сообщение «снаряды закончились», используя его в качестве ключа, а букву Ф – в качестве первой буквы ключа. Процесс шифрования иллюстрирует таблица на рис. 46.

Ключ	Ф	С	Н	А	Р	Я	Д	Ы	З	А	К	О	Н	Ч	И	Л	И	С
Сообщение	С	Н	А	Р	Я	Д	Ы	З	А	К	О	Н	Ч	И	Л	И	С	Ь
Криптограмма	Е	Ю	Н	Р	П	Ь	Г	В	З	К	Ш	Ы	Д	Я	Ф	У	Щ	Д

Рис. 46. Пример шифрования по таблице Виженера с автоключом

Получим следующую криптограмму: ЕЮНРПЬГВЗКШЫДЯФУЩД. Расшифруем ее с помощью автоключа с начальной буквой Ф (рис. 47).

Ключ	Ф	С	Н	А														
Криптограмма	Е	Ю	Н	Р	П	Ь	Г	В	З	К	Ш	Ы	Д	Я	Ф	У	Щ	Д
Сообщение	С	Н	А															

Рис. 47. Пример дешифрования по таблице Виженера с автоключом

На первом шаге в строке Ф таблицы Виженера находим букву Е криптограммы, ей соответствует буква С в первой строке (первая буква открытого текста). Подставляем ее в качестве второй буквы ключа. На втором шаге в строке С находим букву Ю криптограммы, ей соответствует буква Н в первой строке (вторая буква открытого текста), подставляем ее в качестве третьей буквы ключа. На третьем шаге в строке Н находим букву Н криптограммы, ей соответствует буква А в первой строке (третья буква открытого текста), подставляем ее в качестве четвертой буквы ключа. Действуя далее по этому алгоритму, получим открытый текст.

Поскольку таблица симметрична относительно диагонали проходящей из левого верхнего угла в правый нижний, то дешифровать криптограмму можно, выполняя следующий алгоритм. На первом шаге в столбце Ф находим букву Е криптограммы, ей соответствует буква С в первом столбце (первая буква открытого текста). Подставляем ее в качестве второй буквы ключа. На втором шаге в столбце С находим букву Ю криптограммы, ей соответствует буква Н в первом столбце (вторая буква открытого текста). Подставляем ее в качестве третьей буквы ключа. На третьем шаге в столбце Н находим букву Н криптограммы, ей соответствует буква А в первом столбце (третья буква открытого текста). Подставляем ее в качестве четвертой буквы ключа. Таким образом, на очередном шаге при дешифрации получаем очередную букву открытого текста, подставляя которую в качестве следующей буквы ключа получаем следующую букву открытого текста. Это позволяет в результате получить весь открытый текст.

В XIX в. английский адмирал Фрэнсис Бофорт модернизировал шифр Виженера, изменив порядок расположения букв в строках таблицы шифрования (рис. 48). В шифре Бофора они записываются в обратном порядке. Это привело к тому, что правила шифрования и дешифрования стали совпадать. В шифре Бофорта для задания букв открытого текста при шифровании и букв криптограммы при дешифровании используется первая строка таблицы шифрования.

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

Рис. 48. Таблица Бофорта для русского алфавита

При шифровании букву сообщения задают в верхней строке, а соответствующую ей букву ключа – в левом столбце. На пересечении столбца с буквой сообщения и строки с буквой ключа располагается буква криптограммы. При дешифровании букву шифра задают в верхней строке, а соответствующую ей букву ключа – в левом столбце. На пересечении столбца с буквой криптограммы и строки с буквой ключа располагается буква сообщения.

Пример шифрования сообщения «БЕРИТЕ» с ключом «КОТ» представлен на рис. 49. В таблице Бофорта показано, как первая буква сообщения (Б), заданная в верхней строке таблицы, преобразуется в букву И при шифровании и как первая буква криптограммы (И), заданная также в верхней строке таблицы, преобразуется в букву Б при дешифровании. В обоих случаях результат получают в строке, выбранной по первой букве ключа (К).

Ключ	К	О	Т	К	О	Т
Сообщение	Б	Е	Р	И	Т	Е
Криптограмма	И	Я	А	В	Т	Л

Рис. 49. Пример шифрования и дешифрования по таблице Бофорта

Начальник первого дешифровального отделения Германии граф Гронсфельд создал усовершенствованный вариант шифра Виженера, не требующий применения таблицы шифрования. Вместо буквенного лозунга Гронсфельд использовал цифровой, состоявший из нескольких цифр в интервале от 1 до 9. То есть, в шифре Гронсфельда число используемых при шифровании алфавитов сокращено до 9. При шифровании цифры лозунга циклически выписывали под буквами открытого текста, затем очередную букву открытого текста заменяли на букву алфавита, расположенную справа от нее на шаг, соответствующий цифре лозунга. Замены производили по алфавиту с правильным расположением букв. Поясним идею Гронсфельда на примере шифрования слова «ГРОНСФЕЛЬД» с помощью алфавита, представленного на рис. 50, и легко запоминаемого лозунга: 13579. Для этого под буквами открытого текста выпишем циклически цифры лозунга (рис. 51).

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	Ъ	Ы	Ь	Э	Ю	Я

Рис. 50. Алфавит шифра

Г	Р	О	Н	С	Ф	Е	Л	Ь	Д
1	3	5	7	9	1	3	5	7	9
Д	У	У	Ф	Ъ	Х	И	Р	В	Н

Рис. 51. Пример шифрования с помощью шифра Гронсфельда

Первую букву Г заменяем на букву, следующую за ней в указанном алфавите на расстоянии 1 (то есть на букву Д); вторая буква заменяется на букву на расстоянии 3 (на У) и т.д. Получим шифротекст: ДУУФЪХИРВН.

С развитием математики отпала необходимость применения громоздких таблиц шифрования. Используя числовые эквиваленты букв, процессы шифрования и дешифрования можно описать математическими формулами. Например, подстановку Цезаря можно описать выражением:

$$E_i = (M_i + S_i) \; mod \; L,$$

где: E_i , M_i – числовые эквиваленты символов криптограммы и открытого текста соответственно, S_i – коэффициент сдвига, L – число символов алфавита шифрования.

Полиалфавитный шифр Виженера описывается выражением:

$$E_i = (M_i + K_i(modU)) \; mod \; L,$$

где: E_i , M_i – числовые эквиваленты символов криптограммы и открытого текста соответственно, U – длина ключа или период шифра, $K_i(mod\ U)$ – числовой эквивалент буквы ключа, L – число символов алфавита шифрования.

Буквы ключа определяют величину смещения символов криптограммы относительно символов открытого текста. Зашифруем, например, текст «ПОЛИАЛФАВИТНАЯ ПОДСТАНОВКА» ключом КРАБ, используя алфавит, приведенный на рис. 24. Процесс шифрования продемонстрирован на рис. 52.

П	15	К	10	(15+10) mod 32	25	Щ
О	14	Р	16	(14+16) mod 32	30	Ю
Л	11	А	0	(11+0) mod 32	11	Л
И	8	Б	1	(8+1) mod 32	9	Й
А	0	К	10	(0+10) mod 32	10	К
Л	11	Р	16	(11+16) mod 32	27	Ы
Ф	20	А	0	(20+0) mod 32	20	Ф
А	0	Б	1	(0+1) mod 32	1	Б
В	2	К	10	(2+10) mod 32	12	М
И	8	Р	16	(8+16) mod 32	24	Ш
Т	18	А	0	(18+0) mod 32	18	Т
Н	13	Б	1	(13+1) mod 32	14	О
А	0	К	10	(0+10) mod 32	10	К
Я	31	Р	16	(31+16) mod 32	15	П
П	15	А	0	(15+0) mod 32	15	П
О	14	Б	1	(14+1) mod 32	15	П
Д	4	К	10	(4+10) mod 32	14	О
С	17	Р	16	(17+16) mod 32	1	Б
Т	18	А	0	(18+0) mod 32	18	Т
А	0	Б	1	(0+1) mod 32	1	Б
Н	13	К	10	(13+10) mod 32	23	Ч
О	14	Р	16	(14+16) mod 32	30	Ю
В	2	А	0	(2+0) mod 32	2	В
К	10	Б	1	(10+1) mod 32	11	Л
А	0	К	10	(0+10) mod 32	10	К

Рис. 52. Пример шифрования шифром Виженера по формуле

4.5. Многопетлевые полиалфавитные подстановки

Многопетлевая полиалфавитная подстановка является наиболее интересным подстановочным шифром. В шифре Виженера при шифровании используется только один ключ. В многопетлевом шифре используется не один, а несколько ключей шифрования. Их называют петлевыми, или первичными ключами.

Многопетлевой шифр описывается формулой:

$$E_i = (M_i + K_{1i} \bmod U_1 + \ldots + K_{ji} \bmod U_j + \ldots + K_{Gi} \bmod U_G) \bmod L,$$

где: *Ei* – *i*-ый символ криптограммы, *Mi* – *i*-ый символ открытого текста, *L* – мощность исходного алфавита, *G* – число петель шифра, *Uj* – длина *j*-ого первичного ключа, *N* – число символов в криптограмме, $1 \geq i \geq N$;$1 \geq j \geq G$.

В качестве первичных ключей используются осмысленные слова русского языка. Составной ключ равен сумме первичных ключей. Поэтому он не является осмысленным словом и имеет гораздо больший период. Многопетлевые подстановки, благодаря этому, надежнее всех уже рассмотренных нами шифров. Одновременное, последовательное и циклическое применение первичных ключей дает в итоге составной ключ.

Период составного ключа равен наименьшему общему кратному длин всех первичных ключей. Если длины первичных ключей являются взаимно простыми числами, то длина составного ключа равна их произведению и будет наибольшей.

Зашифруем, например, текст «МНОГОПЕТЛЕВАЯ ПОДСТАНОВКА», а в качестве первичных ключей будем использовать слова «КРАБ» и «БУКВА». В ходе шифрования цифровые эквиваленты этих ключей складываются. В результате формируется составной ключ длиной 20 символов (рис. 53), который суммируется по mod 32 с частью открытого текста (рис. 54)

11	3	10	3	10	17	19	11	12	16	1	20	20	18	0	2	29	26	2	1
Л	Г	К	Г	К	С	У	Л	М	П	Б	Ф	Ф	Т	А	В	Э	Ъ	В	Б

Рис. 53. Составной ключ, формируемый из первичных ключей КРАБ и БУКВА

12	13	14	3	14	15	5	18	11	5	2	0	31	15	14	4	17	18	0	13
М	Н	О	Г	О	П	Е	Т	Л	Е	В	А	Я	П	О	Д	С	Т	А	Н

Рис. 54. Часть открытого текста, соответствующая составному ключу

На рис. 55 приведен процесс шифрования многопетлевым шифром.

В результате шифрования получаем зашифрованный текст:

ЧРШЖШАШЭЧХГФУБОЖОМВОЩЕФГ.

Для нашего примера *L*=32, *N* = 24, *G*=2, U_1 = 4, U_2 = 5. Длина составного ключа – 20 символов, а длина шифруемого текста – 24 символа. Это значит, что при шифровании последних 4 символов текста ключ повторяется. Чтобы этого не происходило, длины первичных ключей следует выбирать таким образом, чтобы составной ключ имел большую длину, чем шифруемый текст. Например, при выборе в качестве первого первичного ключа слово «СИНИЦА» длиной 6 символов, составной ключ имел бы длину 30 символов.

Шифры Виженера и Цезаря являются частными случаями многопетлевой подстановки. Поэтому формулу для многопетлевой подстановки можно использовать для описания указанных шифров.

В настоящее время разработаны криптоаналитические методы для вскрытия моноалфавитных и полиалфавитных шифров, причем криптостойкость полиалфавитных шифров резко убывает с уменьшением длины ключа. Тем не менее, такие системы, как шифр Виженера, шифр Бофорта и так далее, допускают

несложную аппаратную или программную реализацию и при достаточно большой длине ключа могут быть использованы в современных информационных системах.

М	12	К	10	Б	1	(12+10+1) mod 32	26	Ч
Н	13	Р	16	У	19	(13+16+19) mod 32	16	Р
О	14	А	0	К	10	(14+0+10) mod 32	24	Ш
Г	3	Б	1	В	2	(3+1+2) mod 32	6	Ж
О	14	К	10	А	0	(14+10+0) mod 32	24	Ш
П	15	Р	16	Б	1	(15+16+1) mod 32	0	А
Е	5	А	0	У	19	(5+0+19) mod 32	24	Ш
Т	18	Б	1	К	10	(18+1+10) mod 32	29	Э
Л	11	К	10	В	2	(11+10+2) mod 32	23	Ч
Е	5	Р	16	А	0	(5+16+0) mod 32	21	Х
В	2	А	0	Б	1	(2+0+1) mod 32	3	Г
А	0	Б	1	У	19	(0+1+19) mod 32	20	Ф
Я	31	К	10	К	10	(31+10+10) mod 32	19	У
П	15	Р	16	В	2	(15+16+2) mod 32	1	Б
О	14	А	0	А	0	(14+0+0) mod 32	14	О
Д	4	Б	1	Б	1	(4+1+1) mod 32	6	Ж
С	17	К	10	У	19	(17+10+19) mod 32	14	О
Т	18	Р	16	К	10	(18+16+10) mod 32	12	М
А	0	А	0	В	2	(0+0+2) mod 32	2	В
Н	13	Б	1	А	0	(13+1+0) mod 32	14	О
О	14	К	10	Б	1	(14+10+1) mod 32	25	Щ
В	2	Р	16	У	19	(2+16+19) mod 32	5	Е
К	10	А	0	К	10	(10+0+10) mod 32	20	Ф
А	0	Б	1	В	2	0+1+2) mod 32	3	Г

Рис. 55. Пример шифрования многопетлевым шифром

4.6. Аналитические методы шифрования

Для шифрования информации могут применяться некоторые аналитические преобразования. Наибольшее распространение получили методы шифрования, основанные на использовании математического аппарата алгебры матриц.

Впервые полиграммный шифр, основанный на аналитических преобразованиях, заключающихся в умножении матриц на векторы, был предложен Лестером Хиллом в 1929 г. Это был первый шифр, который позволял одновременно шифровать более двух символов.

В шифре Хилла в качестве ключа используется квадратная матрица A размерностью $n \times n$ (размерность называют также порядком матрицы). Исходный текст разбивается на блоки длиной n символов. То есть для шифрования биграмм ключевая матрица должна иметь размерность 2×2, для шифрования

триграмм – 3×3 и т.д. Каждый блок рассматривается как *n*-мерный вектор. Процесс шифрования блока заключается в умножении ключевой матрицы *A* на *n*-мерный вектор шифруемого блока, в результате чего получается *n*-мерный вектор зашифрованного блока.

Дешифрование текста происходит с помощью такого же преобразования, только в качестве ключа используется матрица, обратная ключевой, которая обозначается A^{-1}.

Работа с шифром Хилла предполагает, что шифровальщик знает основы алгебры матриц. Поэтому далее будут приведены сведения, необходимые для выполнения используемых в шифре операций над матрицами.

Рассмотрим сначала правила умножения матриц.

Умножением матриц $A \times B$ называется операция вычисления матрицы *C*, элементы которой равны сумме произведений элементов из соответствующей строки матрицы *A* и столбца матрицы *B*.

В матрице *A* должно быть столько же столбцов, сколько строк в матрице *B*. На рис. 56 приведены примеры, иллюстрирующие процесс формирования элементов матрицы произведения *C*. Слева представлен пример умножения квадратных матриц, а справа показано, как квадратная матрица *A* умножается на вектор *B*. Умножение на трехэлементный вектор (столбец из трех элементов) используется в шифре Хилла при шифровании триграмм открытого текста и при дешифровании триграмм зашифрованного текста.

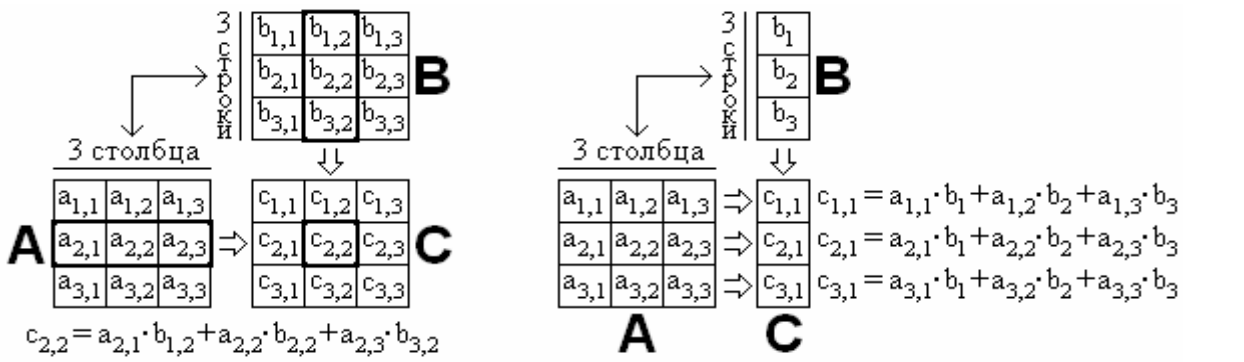

Рис. 56. Схемы умножения матриц

Как отмечено выше, в шифре Хилла используются квадратные ключевые матрицы. Квадратной называют матрицу, количество строк в которой равно количеству столбцов. Причем для применяемой в качестве ключа шифрования матрицы *A* должна существовать обратная матрица A^{-1}, которая является ключом для дешифрования, а обратные матрицы есть только у некоторых квадратных матриц. Обратной называют матрицу A^{-1}, при умножении на которую исходной матрицы *A* получается единичная матрица *E,* то есть $AA^{-1}=E$. Единичная матрица – это аналог единицы для операции умножения чисел. Если квадратную матрицу умножить на единичную матрицу такого же порядка, получится исходная матрица. На рис. 57 приведена единичная матрица *E* размерностью 3×3, у нее единицы стоят только по главной диагонали, остальные элементы равны нулю.

$$E = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}.$$

Рис. 57. Единичная матрица размерности 3×3

Матрицы, для которых существует обратная матрица, называются невырожденными, а остальные – вырожденными. У любой квадратной матрицы A существует определитель $\det A$, по значению которого можно определить тип матрицы. Матрица является невырожденной и имеет обратную матрицу, если ее определитель не равен нулю.

Определитель матрицы равен

$$\det A = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} M_{1j},$$

где: M_{1j} – дополнительный минор к элементу a_{1j} .

Таким образом, определитель матрицы – это число, вычисляемое на основе значений элементов матрицы, стоящих в первой строке, и дополнительных миноров к этим элементам. Каждый элемент квадратной матрицы имеет свой дополнительный минор. Дополнительным минором элемента матрицы a_{1j} называется определитель матрицы, полученной вычеркиванием i-той строки и j-того столбца. Иногда дополнительным минором называют не определитель, а матрицу, полученную из исходной матрицы вышеуказанным способом.

На рис. 58 приведен пример вычисления дополнительного минора M_{23} для элемента a_{23} матрицы A, состоящей из трех строк и трех столбцов, приведенной на этом же рисунке слева.

$$A = \begin{vmatrix} 1 & -1 & 2 \\ 5 & 8 & 9 \\ 3 & 12 & 4 \end{vmatrix}, \qquad M_{23} = \begin{vmatrix} 1 & -1 & \square \\ \square & \square & \square \\ 3 & 12 & \square \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 3 & 12 \end{vmatrix} = (1 \cdot 12 - 3 \cdot (-1)) = 16 .$$

Рис. 58. Пример вычисления дополнительного минора

Рассмотрим далее, как вычисляется определитель для матрицы A, представленной на рис. 59, на котором представлены также дополнительные миноры для элементов A_1, A_2 и A_3 этой матрицы:

$$A = \begin{vmatrix} A_1 & A_2 & A_3 \\ B_1 & B_2 & B_3 \\ C_1 & C_2 & C_3 \end{vmatrix},$$

$$M_{11} = \begin{vmatrix} \square & \square & \square \\ \square & B_2 & B_3 \\ \square & C_2 & C_3 \end{vmatrix} = \begin{vmatrix} B_2 & B_3 \\ C_2 & C_3 \end{vmatrix} = (B_2 \cdot C_3 - B_3 \cdot C_2),$$

$$M_{12} = \begin{vmatrix} \square & \square & \square \\ B_1 & \square & B_3 \\ C_1 & \square & C_3 \end{vmatrix} = \begin{vmatrix} B_1 & B_3 \\ C_1 & C_3 \end{vmatrix} = (B_1 \cdot C_3 - B_3 \cdot C_1),$$

$$M_{12} = \begin{vmatrix} \square & \square & \square \\ B_1 & B_2 & \square \\ C_1 & C_2 & \square \end{vmatrix} = \begin{vmatrix} B_1 & B_2 \\ C_1 & C_2 \end{vmatrix} = (B_1 \cdot C_2 - B_2 \cdot C_1)$$

Рис. 59. Примеры расчета дополнительных миноров для матрицы размерностью 3×3

Используя полученные результаты и приведенную выше формулу для det A, найдем определитель матрицы A (рис. 59):

$$\det A = A_1 \cdot (B_2 \cdot C_3 - B_3 \cdot C_2) - A_2 \cdot (B_1 \cdot C_3 - B_3 \cdot C_1) + A_3 \cdot (B_1 \cdot C_2 - B_2 \cdot C_1).$$

Следует обратить внимание на то, что второе слагаемое получилось со знаком минус, так как в формуле при $j = 2$ сомножитель $(-1)^{1+j}$ получается со знаком минус (-1 возводится в степень 3).

Затем рассмотрим, каким образом из исходной матрицы (ключа шифрования) можно получить обратную матрицу (ключ дешифрования).

Известно несколько способов нахождения обратной матрицы, отличающихся сложностью выполняемых вычислений. В данной работе будем использовать сравнительно простой способ получения обратной матрицы с помощью матрицы алгебраических дополнений (по следующей формуле):

$$A^{-1} = \frac{1}{\det A} \cdot C^T,$$

где: C^T – транспонированная матрица алгебраических дополнений элементов исходной матрицы, а det A – определитель исходной матрицы.

Алгебраическим дополнением элемента a_{ij} матрицы A называется число:

$$A_{ij} = (-1)^{i+j} M_{ij},$$

где: M_{ij} – дополнительный минор или определитель матрицы, получающейся из исходной матрицы A путем вычеркивания i-й строки и j-го столбца.

Из приведенных формул следует, что для нахождения обратной матрицы нужно выполнить следующие действия:

1) вычислить определитель исходной матрицы – det A;
2) если значение детерминанта не равно нулю, то из исходной матрицы сформировать матрицу алгебраических дополнений, заменив каждый элемент исходной матрицы на его алгебраическое дополнение – A_{ij};
3) транспонировать матрицу алгебраических дополнений с целью получения союзной матрицы;
4) сформировать обратную матрицу, разделив каждый элемент союзной матрицы на определитель исходной матрицы.

Далее рассмотрим пример получения обратной матрицы для матрицы-ключа, приведенной на рис. 60 слева.

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}, \qquad A = \begin{vmatrix} A_1 & A_2 & A_3 \\ B_1 & B_2 & B_3 \\ C_1 & C_2 & C_3 \end{vmatrix}.$$

Рис. 60. Матрица-ключ размерности 3×3

Сначала вычислим определитель матрицы-ключа, чтобы узнать есть ли у нее обратная матрица. Для вычисления определителя воспользуемся полученной выше формулой для матрицы размерностью 3×3. В формуле использованы обозначения элементов из этой матрицы, поэтому для удобства подстановки в формулу элементов ключевой матрицы рядом с ключевой матрицей на рис. 60 размещена матрица с соответствующими обозначениями.

$$\det A = A_1 \cdot (B_2 \cdot C_3 - B_3 \cdot C_2) - A_2 \cdot (B_1 \cdot C_3 - B_3 \cdot C_1) + A_3 \cdot (B_1 \cdot C_2 - B_2 \cdot C_1);$$

$$\det A = 1 \cdot (7 \cdot 5 - 2 \cdot 9) - 4 \cdot (3 \cdot 5 - 2 \cdot 6) + 8 \cdot (3 \cdot 9 - 7 \cdot 6) = 17 - 12 - 120 = -115.$$

Определитель ключевой матрицы не равен нулю, поэтому для нее существует обратная матрица.

Сформируем обратную матрицу по приведенному выше алгоритму.

Первый пункт этого алгоритма уже выполнен – произведено вычисление детерминанта ключевой матрицы.

Поскольку детерминант ключевой матрицы не равен нулю, сформируем матрицу алгебраических дополнений для исходной ключевой матрицы (рис. 60). Чтобы рассчитать алгебраические дополнения для всех элементов a_{ij}, получим сначала матрицы для вычисления дополнительных миноров вычеркиванием *i*-й строки и *j*-го столбца исходной матрицы. Полученные матрицы приведены на рис. 61.

$$M_{11} = \begin{vmatrix} 7 & 2 \\ 9 & 5 \end{vmatrix}, M_{12} = \begin{vmatrix} 3 & 2 \\ 6 & 5 \end{vmatrix}, M_{13} = \begin{vmatrix} 3 & 7 \\ 6 & 9 \end{vmatrix},$$

$$M_{21} = \begin{vmatrix} 4 & 8 \\ 9 & 5 \end{vmatrix}, M_{22} = \begin{vmatrix} 1 & 8 \\ 6 & 5 \end{vmatrix}, M_{23} = \begin{vmatrix} 1 & 4 \\ 6 & 9 \end{vmatrix},$$

$$M_{31} = \begin{vmatrix} 4 & 8 \\ 7 & 2 \end{vmatrix}, M_{32} = \begin{vmatrix} 1 & 8 \\ 3 & 2 \end{vmatrix}, M_{33} = \begin{vmatrix} 1 & 4 \\ 3 & 7 \end{vmatrix}.$$

Рис. 61. Матрицы для вычисления дополнительных миноров

Используя эти матрицы, вычислим алгебраические дополнения для элементов ключевой матрицы *A*:

$$A_{11}^* = (-1^{1+1}) \cdot (7 \cdot 5 - 2 \cdot 9) = 35 - 18 = 17;$$

$$A_{12}^* = (-1^{1+2}) \cdot (3 \cdot 5 - 6 \cdot 2) = -(15 - 12) = -3;$$

$$A_{13}^* = (-1^{1+3}) \cdot (3 \cdot 9 - 6 \cdot 7) = 27 - 42 = -15;$$

$$A_{21}^* = (-1^{2+1}) \cdot (4 \cdot 5 - 9 \cdot 8) = -(20 - 72) = 52;$$

$$A_{22}^* = (-1^{2+2}) \cdot (1 \cdot 5 - 6 \cdot 8) = 5 - 48 = -43;$$

$$A_{23}^* = (-1^{2+3}) \cdot (1 \cdot 9 - 6 \cdot 4) = -(9 - 24 = 15;$$

$$A_{31}^* = (-1^{3+1}) \cdot (4 \cdot 2 - 7 \cdot 8) = 8 - 56 = -48;$$

$$A^*_{32} = (-1^{3+2}) \cdot (1 \cdot 2 - 3 \cdot 8) = -(2 - 24) = 22;$$

$$A_133^1 *= ([-1]^{1}(3+3)) \cdot (1 \cdot 7 - 3 \cdot 4) = 7 - 12) = -5.$$

Матрица алгебраических дополнений из полученных элементов приведена на рис. 62.

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}.$$

Рис. 62. Матрица алгебраических дополнений

Далее получим союзную матрицу путем транспонирования матрицы алгебраических дополнений. Транспонирование матрицы – это операция, при которой исходная матрица отражается относительно главной диагонали, то есть $a^T_{ij} = a_{ji}$. Полученная в результате транспонирования союзная матрица СТ приведена на рис. 63.

$$C^T = \begin{vmatrix} 17 & 52 & -48 \\ 3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}.$$

Рис. 63. Союзная матрица

Разделим каждый элемент союзной матрицы на определитель исходной матрицы, равный 115, и получим обратную матрицу, которая представлена на рис. 64.

$$A^{-1} = \begin{vmatrix} -\frac{17}{115} & -\frac{52}{115} & \frac{48}{115} \\ \frac{3}{115} & \frac{43}{115} & -\frac{22}{115} \\ \frac{15}{115} & -\frac{15}{115} & \frac{5}{115} \end{vmatrix}.$$

Рис. 64. Обратная матрица

Получив набор ключей, рассмотрим пример шифрования шифром Хилла триграмм открытого текста, а также дешифрования криптограммы, состоящей из зашифрованных триграмм. В данном примере будем шифровать открытый текст «ЗАБАВА» с помощью матрицы-ключа, приведенной на рис. 60, а расшифровывать полученную криптограмму будем с помощью сформированной обратной матрицы (рис. 64).

Для шифрования открытого текста заменим входящие в него буквы числовыми эквивалентами в соответствии с таблицей, представленной на рис. 65.

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	Ъ	Ы	Ь	Э	Ю	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	151	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Рис. 65. Числовые эквиваленты букв русского алфавита

В результате получим – 8 1 2 1 3 1.

Разделим полученный код на триграммы, из которых сформируем векторы открытого текста, то есть матрицы, содержащие по одному столбцу из трех элементов (рис. 66).

$$B_1 = \begin{bmatrix} 8 \\ 1 \\ 2 \end{bmatrix}, \qquad B_2 = \begin{bmatrix} 1 \\ 3 \\ 1 \end{bmatrix}.$$

Рис. 66. Векторы открытого текста

Зашифруем полученные векторы путем их умножения на ключевую матрицу и получим векторы криптограммы C_1 и C_2 (рис. 67).

$$C_1 = \begin{bmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 28 \\ 35 \\ 67 \end{bmatrix}, C_2 = \begin{bmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 3 \\ 1 \end{bmatrix} = \begin{bmatrix} 21 \\ 26 \\ 38 \end{bmatrix}.$$

Рис. 67. Получение векторов шифрованного текста

Для получения криптограммы следует выписать числа из матриц C_1 и C_2 в строку – 28 35 67 21 26 38.

При дешифровании криптограмма разбивается на триграммы, из которых формируются векторы криптограммы, то есть матрицы, содержащие по одному столбцу из трех элементов (рис. 68).

$$C_1 = \begin{bmatrix} 28 \\ 35 \\ 67 \end{bmatrix}, \qquad C_2 = \begin{bmatrix} 21 \\ 26 \\ 38 \end{bmatrix}.$$

Рис. 68. Векторы криптограммы

Дешифрование криптограммы выполняется по следующим формулам: $B_1 = A^{-1} \times C_1$; $B_2 = A^{-1} \times C_2$. То есть для получения триграмм открытого текста нужно умножить соответствующие векторы криптограммы на обратную матрицу. Рис. 69 иллюстрирует процесс дешифрования.

$$\frac{-476 - 1820 + 3216}{115} @ \frac{84 + 1505 - 1474}{115} @ \frac{420 - 525 + 335}{1}$$

$$\frac{-357 - 1352 + 1824}{115} @ \frac{63 + 1118 - 836}{115} @ \frac{315 - 390 + 190}{11}$$

Рис. 69. Примеры дешифрования векторов криптограммы

В результате дешифрования получены векторы открытого текста в виде числовых эквивалентов букв – 8 1 2 1 3 1. Для восстановления открытого текста используется таблица кодирования (рис. 65), с помощью которой получим «ЗАБАВА».

Наиболее просто с помощью шифра Хилла шифровать биграммы открытого текста, в этом случае ключевые таблицы имеют размерность 2×2. При этом никаких преимуществ, по сравнению с шифром Плейфера, он не имеет и даже уступает ему по простоте использования. Его основным достоинством, по сравнению с другими шифрами, является возможность шифрования полиграмм, содержащих более двух символов. Однако при увеличении числа одновременно шифруемых символов увеличивается размерность ключевых таблиц, и шифр становится недоступным для ручного шифрования.

Таким образом, можно сделать вывод о том, что шифр Лестера Хилла является самым сложным шифром из рассмотренных в данном пособии ручных шифров. Шифр интересен тем, что, в отличие от остальных симметричных шифров, в нем используются не один ключ для шифрования и дешифрования, а два различных ключа, причем ключ для дешифрования может быть получен из ключа шифрования с помощью сложных аналитических преобразований. По этому признаку шифр выпадает из классификации симметричных шифров. Шифр интересен еще и тем, что при шифровании данным шифром имеет место разнозначная замена. Так, в рассмотренном примере код открытого текста (812131) не совпадает по размеру с кодом шифрованного текста (283567212638), что существенно усложняет криптоанализ криптограмм.

В шифре Хилла ключи для дешифрования могут быть сформированы заранее, в этом случае шифрование и дешифрование шифром Хилла выполняется сравнительно просто. Однако при интенсивном обмене криптограммами необходимость частой смены ключа, например, через определенный интервал времени, требует от шифровальщика значительных усилий и временных затрат, особенно при большой размерности ключевой матрицы. Поэтому шифры на основе аналитических преобразований больше подходят для машинной и программной реализации. Понимая это, Лестер Хилл создал механический шифратор и получил патент на свое устройство, выполняющее умножение матриц размерности 6×6. Однако в его шифраторе использовался только один ключ, который задавался расположением шестеренок в механическом блоке. Для использования другого ключа нужно было изменить расположение шестеренок в шифраторе, то есть изменить конструкцию устройства. Это было недостатком механического шифратора Хилла, который не получил широкого распространения. Хотя для 1929 г. шифр Хилла, даже в реализации с одним ключом большой размерности, обладал высокой криптостойкостью, поскольку в то время статистики использования триграмм, а тем более шестиграмм не существовало. Такая статистика для полиграмм с числом символов более трех отсутствует и в настоящее время.

5. Шифры перестановки

Шифр, который в результате преобразования исходного текста изменяет только порядок следования символов исходного текста, но не изменяет их самих, называется шифром перестановки.

Шифры перестановки бывают двух типов:

- шифры одинарной перестановки. При шифровании символы только один раз перемещаются с исходных мест на новые позиции;
- шифры множественной перестановки. При шифровании символы несколько раз перемещаются с исходных мест на новые позиции.

5.1. Шифры одинарной перестановки

5.1.1. Шифр простой одинарной перестановки

В общем случае для данного класса шифров при шифровании и дешифровании используется таблица перестановок, представленная на рис. 70. В первой строке данной таблицы числа от 1 до *n* расположены по порядку и указывают позицию символов в исходном сообщении длиной *n*, а во второй – те же числа расположены в порядке, задающем расположение символов в криптограмме. Такая таблица является ключом шифра. Максимальное количество ключей для такого шифра перестановки равно *n*!.

1	2	3	4	. . .	n
i_1	i_2	i_3	i_4	. . .	i_n

Рис. 70. Таблица одинарных перестановок

К	Р	Е	Й	С	Е	Р
1	2	3	4	5	6	7
2	3	7	1	6	4	5
Р	Е	Р	К	Е	Й	С

Рис. 71. Пример таблицы перестановок

Зная подстановку, задающую преобразование, можно осуществить как шифрование открытых сообщений, так и дешифрование криптограмм. Например, если для шифрования используется перестановка, заданная таблицей на рис. 71, то при шифровании сообщения «КРЕЙСЕР» получим криптограмму «РЕРКЕЙС».

Для использования на практике такой шифр не совсем удобен, так как при больших значениях n приходится работать с длинными таблицами и для сообщений разной длины необходимо иметь свою таблицу перестановок.

5.1.2. Шифр блочной одинарной перестановки

При использовании этого шифра задается таблица перестановки блока символов, которая последовательно применяется до тех пор, пока исходное сообщение не закончится. Если исходное сообщение не кратно размеру блока, тогда оно при шифровании дополняется произвольными символами. На рис. 72 слева представлена таблица для блочной одинарной перестановки, а справа – пример использования этой таблицы для шифрования сообщения «ХОЗЯИН ПРИБЫЛ» длиной 12 символов. В данном примере размер блока равен 4, поэтому перестановка 3142 последовательно выполняется 3 раза для разных участков сообщения. В результате шифрования получим «ОЯХЗНРИПБЛИЫ».

1	2	3	4
3	1	4	2

Х	О	З	Я	И	Н	П	Р	И	Б	Ы	Л
3	1	4	2	3	1	4	2	3	1	4	2

Рис. 72. Блочная одинарная перестановка

Количество ключей для данного шифра равно $m!$, где: m – размер блока. В рассмотренном примере их всего 24 ($4! = 1 \times 2 \times 3 \times 4 = 24$).

5.2. Шифры маршрутной перестановки

5.2.1. Шифры простой маршрутной перестановки

На практике широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру (плоскую или объемную). Преобразования состоят в том, что в фигуру исходный текст записывается в последовательности, заданной одним маршрутом, а извлекается по другому маршруту.

Одним из самых простых шифров маршрутной перестановки является табличный шифр простой перестановки. Ключ такого шифра – размер используемой прямоугольной таблицы, в которую сообщение записывается по строкам слева направо, а буквы криптограммы извлекаются из столбцов сверху вниз последовательно, начиная с первого столбца. Например, при шифровании по таблице размером 6х6 (рис. 73) сообщение «МАРШРУТ ТРАНСПОРТА ИЗВЕСТЕН ПРОТИВНИКАМ» будет преобразовано в криптограмму: МТПЗНВАТОВПНРРРЕРИШАТСОКРНАТТАУСИЕИМ.

М	А	Р	Ш	Р	У
Т	Т	Р	А	Н	С
П	О	Р	Т	А	И
З	В	Е	С	Т	Е
Н	П	Р	О	Т	И
В	Н	И	К	А	М

Рис. 73. Шифр простой табличной перестановки

Шифр маршрутной перестановки с ключом для выбора столбцов называется шифром вертикальной перестановки. В нем используется прямоугольная таблица, в которую сообщение записывается по строкам слева направо. Буквы криптограммы извлекаются из столбцов таблицы по вертикали, а столбцы при этом выбираются в порядке, определяемом ключом. В качестве примера рассмотрим таблицу размером 6×6 с ключом – 3 5 2 6 1 4. Зашифруем с помощью такой таблицы сообщение:

«МАРШРУТ ТРАНСПОРТА ИЗВЕСТЕН ПРОТИВНИКАМ».

Запишем сообщение в строки таблицы последовательно, начиная с первой (рис. 74). Для получения зашифрованного текста следует извлечь буквы из столбцов таблицы сверху вниз, выбирая столбцы в порядке, заданном ключом. Получим следующую криптограмму:

РНАТТАРРРЕРИМТПЗНВУСИЕИМАТОВПНШАТСОК.

3	5	2	6	1	4
М	А	Р	Ш	Р	У
Т	Т	Р	А	Н	С
П	О	Р	Т	А	И
З	В	Е	С	Т	Е
Н	П	Р	О	Т	И
В	Н	И	К	А	М

Рис. 74. Шифр вертикальной перестановки

Ключом для шифров табличной перестановки являются маршруты занесения открытого сообщения и извлечения букв криптограммы, а также размеры таблицы. Для заданного в примере размера и порядка заполнения таблицы число ключей вертикальной перестановки равно m!, где m – число столбцов таблицы. Ключом шифра вертикальной перестановки может быть слово или фраза, тогда порядок выбора столбцов будет определяться алфавитным порядком букв в ключе. Например, при использовании в качестве ключа к таблице размером 6×6 слова «КУРИЦА», порядок выбора столбцов при шифровании будет следующим – 354261.

5.2.2. Шифры маршрутной перестановки на основе магических квадратов

Магические квадраты появились несколько тысячелетий назад в Индии и Китае. Глиняные пластинки с магическими квадратами, найденные при археологических раскопках в Китае, имели отверстие. Вероятно, их носили на шее в качестве амулетов, считая, что они обладают магической силой.

Магическими квадратами называются квадратные таблицы, заполненные последовательностью различных натуральных чисел, начиная с 1, которые в сумме по каждому столбцу, каждой строке и каждой диагонали дают одина-

ковое число. Подобные квадраты широко применялись для шифрования текста, который записывался в квадрат в порядке нумерации его ячеек, результат шифрования перестановкой получался путем извлечения букв из квадрата по строкам. Число магических квадратов зависит от размера квадрата. Так, существует лишь один магический квадрат размером 3×3, если не принимать во внимание его повороты. Магических квадратов 4×4 насчитывается уже 880, а число магических квадратов размером 5×5 составляет около 250 тыс. Магические квадраты больших размеров могли быть хорошей основой для системы шифрования перестановкой в прежние века, потому что ручной перебор всех вариантов ключа для этого шифра требовал много времени.

Рассмотрим магический квадрат размером 4×4, обнаруженный в Индии и датируемый XI – XII вв. до н.э. (рис. 75). Числа от 1 до 16 заполняют его таким образом, что их сумма по строкам, столбцам и полным диагоналям равняется одному и тому же числу – 34. Этот квадрат обладает интересной особенностью: при циклическом перемещении его строк по вертикали и столбцов по горизонтали он остается магическим. Вероятно, такой квадрат не только защищал владельца, но и помогал уничтожать его врагов.

7	12	1	14
2	13	8	11
16	3	10	5
9	6	15	4

Рис. 75. Магический квадрат 4×4

Зашифруем с помощью этого магического квадрата сообщение «ШИФР ПЕРЕСТАНОВКИ». Заполним квадрат буквами сообщения в порядке нумерации ячеек (рис. 76) и извлечем буквы построчно, начиная с первой строки. В результате получим криптограмму: РНШВИОЕАИФТПСЕКР. При дешифрации криптограмма записывается в квадрат построчно, а буквы сообщения извлекаются в порядке нумерации ячеек.

7(Р)	12(Н)	1(Ш)	14(В)
2(И)	13(О)	8(Е)	11(А)
16(И)	3(Ф)	10(Т)	5(П)
9(С)	6(Е)	15(К)	4(Р)

Рис. 76. Пример шифрования с помощью магического квадрата

5.2.3. Шифры маршрутной перестановки на основе решеток

Шифр «Поворотная решетка» изобрел в 1550 г. итальянский математик Джероламо Кардано. Этот шифр является первым геометрическим шифром. Он основан на использовании квадратной таблицы, некоторые ячейки которой имеют отверстия, образующие геометрическую фигуру для заполнения шифруемым текстом. Отверстия в таблице вырезаются таким образом, чтобы при наложении полученного трафарета на таблицу такого же размера четырьмя возможными способами отверстия полностью покрывали все ячейки таблицы ровно по одному разу. При шифровании шифруемый текст разбивается на блоки по числу отверстий в трафарете. Трафарет накладывается на лист бумаги и первый блок текста через отверстия записывается на бумагу слева направо и сверху вниз. Затем трафарет поворачивается на 90 градусов, записывается следующий блок и так далее для четырех возможных положений решетки. Криптограмму извлекают из итоговой таблицы по определенному маршруту.

Таким образом, ключом при шифровании является трафарет, а также порядок его поворотов и маршрут извлечения букв криптограммы.

При создании трафарета квадратная таблица с четным количеством строк и столбцов делится на 4 четверти, в каждой из которых ячейки нумеруются так, чтобы при вращении таблицы ячейки с одинаковыми номерами совпадали. Пример таблицы размером 6×6 с требуемой нумерацией ячеек представлен на рис. 77. Если в такой таблице сделать отверстие, например, в ячейке, имеющей номер 1 в третьей четверти, то при первом повороте на 90 градусов по часовой стрелке отверстие совпадет с ячейкой, обозначенной 1 в четвертой четверти. При втором повороте отверстие совпадет с ячейкой, обозначенной 1 в первой четверти, а при третьем повороте – с аналогичной ячейкой во второй четверти. Таким образом, одно отверстие, сделанное в ячейке с номером 1 в любой четверти, после серии поворотов обойдет все ячейки с номерами 1. Одно отверстие, сделанное в ячейке с номером 2 в любой четверти, после серии поворотов обойдет все ячейки с номерами 2 и т.д. Для получения решетки для шифрования в данной таблице нужно сделать 9 отверстий: по одному в группах с одинаковыми номерами, например, как на рис. 77. Из приведенного примера следует, что после серии из 3 поворотов отверстия перекроют все ячейки таблицы.

0 градусов					
1	2	3	4	5	1
5	6	7	8	6	2
4	8	9	9	7	3
3	7	9	9	8	4
2	6	8	7	6	5
1	5	4	3	2	1

90 градусов					
1	2	3	4	5	1
5	6	7	8	6	2
4	8	9	9	7	3
3	7	9	9	8	4
2	6	8	7	6	5
1	5	4	3	2	1

180 градусов					
1	2	3	4	5	1
5	6	7	8	6	2
4	8	9	9	7	3
3	7	9	9	8	4
2	6	8	7	6	5
1	5	4	3	2	1

270 градусов					
1	2	3	4	5	1
5	6	7	8	6	2
4	8	9	9	7	3
3	7	9	9	8	4
2	6	8	7	6	5
1	5	4	3	2	1

Рис. 77. Пример использования шифра «Поворотная решетка»

В шифре «Поворотная решетка» может использоваться и неквадратная таблица, если изменить порядок ее наложения на лист чистой бумаги при шифровании. Например, если решетку накладывать на лист различными сторонами и поворачивать только на 180 градусов, то такая решетка может быть изготовлена из таблицы размером $2m \times 2k$ ячеек. В таблице должно быть вырезано $m \times k$ ячеек так, чтобы при наложении решетки на чистый лист бумаги того же размера четырьмя возможными способами ее вырезы полностью покрывали всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Поясним процесс шифрования на примере. Пусть в качестве ключа используется решетка 6×10, представленная на рис. 78. Число возможных решеток при таком размере решетки, то есть количество ключей такого шифра, составляет 1073741824.

1	2	3	4	5	6	7	8	9	10
11	12	12	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Рис. 78. Пример прямоугольной решетки в шифре «Поворотная решетка»

Зашифруем с ее помощью текст:

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ.

1	Ш	3	4	5	6	7	8	9	10
И	12	13	14	Ф	16	Р	Р	19	20
21	Е	23	24	25	Ш	27	28	29	Е
31	32	33	Т	35	36	37	К	39	40
41	А	43	44	45	46	47	48	49	50
51	52	Я	54	55	В	Л	58	59	Я

Рис. 79. Пример начального заполнения решетки

Наложив решетку на лист бумаги, вписываем первые 15 (по числу вырезов) букв сообщения: ШИФРРЕШЕТКАЯВЛЯ (рис. 79). Поворачиваем решетку на 180 градусов. В отверстиях появятся новые, еще не заполненные клетки. Вписываем в них следующие 15 букв – ЕТСЯЧАСТНЫМСЛУЧ. Получится запись, приведенная на рис. 80.

Е	59	58	Т	С	55	54	Я	52	51
50	49	48	47	46	45	44	43	Ч	41
40	39	А	37	36	35	С	33	32	31
Т	29	28	27	Н	25	24	23	Ы	21
20	19	М	С	16	Л	14	13	12	Ч
10	9	8	7	6	5	4	3	А	1

Рис. 80. Пример заполнения решетки после поворота на 180 градусов

Затем переворачиваем решетку на другую сторону и вписываем остаток текста (АЕМШИФРАМАРШРУТ и НОЙПЕРЕСТАНОВКИ) аналогичным образом (рис. 81 и 82).

10	9	8	7	6	5	4	3	А	1
20	19	Е	М	16	Ш	14	13	12	И
Ф	29	28	27	Р	25	24	23	А	21
40	39	М	37	36	35	А	33	32	31
50	49	48	47	46	45	44	43	Р	41
Ш	59	58	Р	У	55	54	Т	52	51

Рис. 81. Пример заполнения решетки после поворота на другую сторону

51	52	Н	54	55	О	Й	58	59	П
41	Е	43	44	45	46	47	48	49	50
31	32	33	Р	35	36	37	Е	39	40
21	С	23	24	25	Т	27	28	29	А
Н	12	13	14	О	16	В	К	19	20
1	И	3	4	5	6	7	8	9	10

Рис. 82. Пример заполнения решетки после поворота на 180 градусов

Итоговая перестановка букв на листе бумаги после снятия решетки представлена на рис. 83. Для дешифрации этой криптограммы следует наложить на нее решетку по порядку четырьмя указанными выше способами.

Е	Ш	Н	Т	С	О	Й	Я	А	П
И	Е	Е	М	Ф	Ш	Р	Р	Ч	И
Ф	Е	А	Р	Р	Ш	С	Е	А	Е
21	С	М	Т	Н	Т	А	К	Ы	А
Н	А	М	С	О	16	В	К	Р	Ч
Ш	И	Я	Р	У	В	Л	Т	А	Я

Рис. 83. Итоговая перестановка букв на листе бумаги после снятия решетки

5.2.4. Шифры множественной перестановки

В данном подклассе шифров используется идея повторного шифрования уже зашифрованного сообщения.

Шифр маршрутной перестановки с ключами для перестановки столбцов и строк называется шифром двойной перестановки. В нем используется прямоугольная таблица, в которую сообщение записывается, например, по строкам слева направо. После этого выполняется перестановка столбцов по первому ключу. Столбец, обозначенный в ключевой строке цифрой 1, становится первым, столбец, обозначенный цифрой 2, становится вторым и т.д. После этого выполняется перестановка строк таблицы по второму ключу, строка, обозначенная в ключевом столбце цифрой 1, становится первой, строка, обозначенная цифрой 2, становится второй и т.д. Буквы криптограммы могут извлекаться из таблицы по различным маршрутам, например, по строкам.

В качестве примера рассмотрим таблицу размером 6х6. Для перестановки столбцов используем ключ 3 5 2 6 1 4, а для перестановки строк – ключ 2 5 4 1 6 3. Зашифруем с помощью такой таблицы сообщение:

МАРШРУТ ТРАНСПОРТА ИЗВЕСТЕН ПРОТИВНИКАМ.

Запишем сообщение в строки таблицы последовательно, начиная с первой. Результат представлен на рис. 84.

	3	5	2	6	1	4
2	М	А	Р	Ш	Р	У
5	Т	Т	Р	А	Н	С
4	П	О	Р	Т	А	И
1	З	В	Е	С	Т	Е
6	Н	П	Р	О	Т	И
3	В	Н	И	К	А	М

Рис. 84. Таблица до перестановки

	1	2	3	4	5	6
2	Р	Р	М	У	А	Ш
5	Н	Р	Т	С	Т	А
4	А	Р	П	И	О	Т
1	Т	Е	З	Е	В	С
6	Т	Р	Н	И	П	О
3	А	И	В	М	Н	К

Рис. 85. Перестановка столбцов по ключевой строке

В таблице на рис. 85 представлен результат перестановки столбцов по ключу 3 5 2 6 1 4, а в таблице на рис. 86 – результат перестановки строк по ключу 2 5 4 1 6 3.

	1	2	3	4	5	6
1	Т	Е	З	Е	В	С
2	Р	Р	М	У	А	Ш
3	А	И	В	М	Н	К
4	А	Р	П	И	О	Т
5	Н	Р	Т	С	Т	А
6	Т	Р	Н	И	П	О

Рис. 86. Перестановка строк по ключевому столбцу

В итоге при построчном извлечении букв из таблицы получим такую криптограмму:

ТЕЗЕВСРРМУАШАИВМНКАРПИОТНРТСТАТРНИПО.

Чтобы ее дешифровать, все действия нужно выполнить в обратном порядке.

Число вариантов двойной перестановки для таблицы 6×6 равно 518400 (6!×6!). Но, несмотря на большое число вариантов перестановок, шифры перестановок, в том числе и рассмотренный шифр, сравнительно просто взламываются при любом размере таблицы шифрования. Метод взлома шифров двойной перестановки основан на определении маловероятных сочетаний букв и нахождении на их основе истинной последовательности столбцов и строк в шифровальной таблице.

5.2.5. Трехмерные маршрутные перестановки

Стойкость шифрования перестановкой можно повысить усложнением перестановок путем использования в качестве шифрующих таблиц объемных геометрических фигур с несколькими ключами маршрутных перестановок. Наиболее известным шифром маршрутной перестановки на основе использования объемных геометрических фигур является шифр перестановки по маршрутам Гамильтона.

В 1859 г. знаменитый ирландский математик Вильям Гамильтон, автор теории комплексных чисел, придумал детскую головоломку, в которой предлагалось совершить «кругосветное путешествие», посетив 20 городов, расположенных в различных частях земного шара. Каждый город соединялся дорогами с тремя соседними так, что дорожная сеть образовывала 30 ребер додекаэдра, в вершинах которого находились города А, В, …, Т. Общее число маршрутов или решений этой головоломки равнялось 60. Обязательным условием при составлении маршрута движения было требование посетить каждый город, за исключением первого, только 1 раз. То есть нужно было вернуться в пункт отправления. Эта головоломка и легла в основу шифра маршрутной перестановки, получившего название «маршруты Гамильтона», или «шифр Гамильтона».

Сложные трехмерные фигуры применять для шифрования не совсем удобно. Используются простые трехмерные фигуры, которые можно представить в виде плоского графа или специальной таблицы.

Основой шифра Гамильтона является специальная таблица, имеющая вид графа, состоящего из нескольких вершин, соединенных ребрами в определенном порядке. В общем случае граф может содержать различное число вершин. В специальной литературе чаще всего встречается описание графа из восьми вершин. Для удобства будем обозначать вершины не в виде окружностей, а в виде квадратов. Пример маршрутной таблицы с такими вершинами приведен на рис. 87. Представленная таблица является плоским вариантом куба, который изображен на рис. 87 справа.

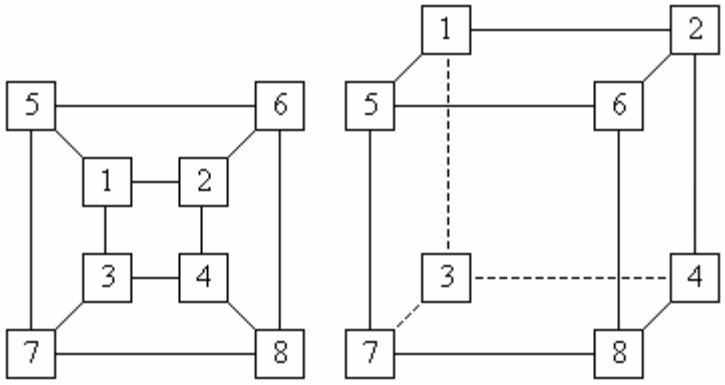

Рис. 87. Таблица трехмерной перестановки, соответствующая кубу

Номера вершин графа используются при заполнении графа символами открытого текста. Маршрут шифрования, он же ключ шифрования, задает порядок излечения символов криптограммы. При составлении маршрута шифрования сперва указывается начальная вершина графа, содержащая первый символ криптограммы для данного маршрута. Затем задается порядок обхода всех вершин графа для извлечения остальных символов, при этом двигаться можно только по ребрам графа. В качестве примера на рис. 88 представлен порядок обхода вершин для ключа 4 2 1 5 6 8 7 3.

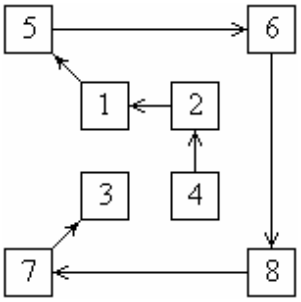

Рис. 88. Пример составления маршрута

Секретным ключом для данного шифра являются вид графа перестановки, число и порядок использования маршрутов при шифровании. Вид графа определяет количество вершин для шифрования текста и количество возможных маршрутов обхода этих вершин.

При шифровании с использованием графа, представленного на рис. 89, сначала задается количество используемых для шифрования маршрутов, затем для каждого маршрута формируется маршрутная таблица и соответствующий

ключ шифрования. После этого открытый текст разбивается на блоки по 8 символов. Если количество символов открытого текста не кратно 8, то последний блок дополняется произвольными символами. Символы каждого блока открытого текста заносятся в маршрутные таблицы последовательно либо в порядке, установленном с помощью дополнительного ключа. При этом порядок заполнения каждой таблицы также может задаваться ключом, но обычно символы заносят в таблицу в порядке нумерации вершин. Извлечение символов криптограммы из маршрутных таблиц производится в соответствии с установленными для них маршрутами. В качестве примера зашифруем текст «КРИПТОГРАФИЧЕСКАЯ ТЕХНИКА», используя три различных маршрута, заданных ключами:

К1 = 6 8 4 2 1 3 7 8, К2 = 3 4 2 1 5 7 8 6 и К3 = 7 8 6 5 1 3 4 2.

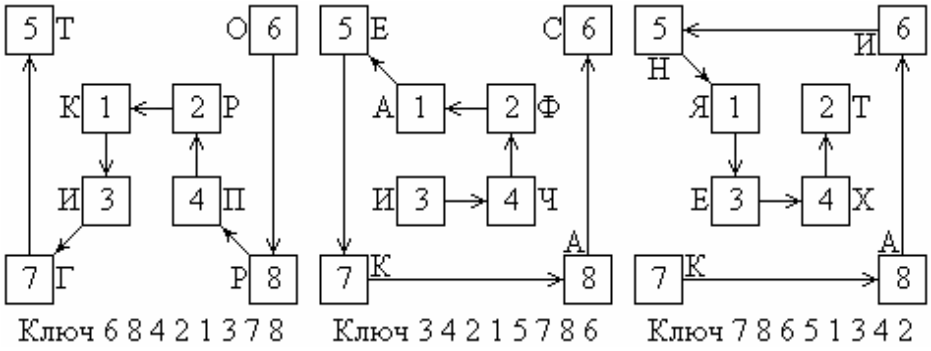

Рис. 89. Пример шифрования шифром Гамильтона

Извлечем символы криптограммы из таблицы в соответствии с ключами. В результате получим – ОРПРКИГТ ИЧФАЕКАС КАИНЯЕХТ. При дешифровании таблицы заполняют, используя ключи, а извлекают открытый текст в порядке нумерации вершин, начиная с первой.

6. Шифры дробления

6.1. Расщепленный шифр Bifid

Наиболее значимый вклад в криптографию внесли кадровые военные, дипломаты и ученые. Феликс Деластелль, который, по мнению известного исследователя шифров Дэвида Кана, изобрел криптографическую систему значительной важности в криптологии, разрабатывал шифры в свободное от основной работы время. Расщепленный шифр, который считается одним из наиболее стойких ручных шифров, был изобретен им в 1901 г. Суть его идеи состояла в последовательном использовании расщепления и объединения при получении шифротекста. Каждый символ исходного текста в данном шифре представлялся в виде совокупности двух частей этого символа, выделяемых при шифровании, а для получения символа криптограммы использовались части двух различных символов исходного текста.

В рассматриваемом шифре для преобразования символов Феликс Деластелль использовал таблицу размером 5×5, строки и столбцы которой были пронумерованы. Таблица заполнялась латинским алфавитом в произвольном порядке, при этом порядок расположения символов являлся ключом шифра. Для упрощения запоминания ключа заполнение могло производиться по ключевому слову или фразе.

Идею расщепленного шифра проиллюстрируем на примере квадрата, заполненного буквами русского алфавита. Для размещения всех букв русского алфавита используем квадратную таблицу размером 6×6 (рис. 90), дополнив алфавит символами пробела, точкой и запятой.

	1	2	3	4	5	6
1	Ё	Р	О	К	В	Ф
2	У	Ш	Ъ	Ц	Й	Е
3	Х	Э	А	С	Щ	Т
4	Л	.	И	Ю	Ж	,
5	Ь	М		Б	Я	Н
6	Г	Ч	Ы	З	П	Д

Рис. 90. Таблица для расщепленного шифра (русский алфавит)

Зашифруем с помощью расщепленного шифра сообщение:

СРОЧНО УХОДИТЕ.

Для этого под каждым символом шифруемого сообщения запишем его координаты в таблице шифрования: сначала номер строки, а под ним – номер столбца (рис. 91).

С	Р	О	Ч	Н	О		У	Х	О	Д	И	Т	Е
3	1	1	6	5	1	5	2	3	1	6	4	3	2
4	2	3	2	6	3	3	1	1	3	6	3	6	6

Рис. 91. Порядок изменения координат при шифровании расщепленным шифром

Х	Ф	Ь	М	Х	З	Э	.	Э	Ы	Х	О	Ы	Д
3	1	5	5	3	6	3	4	3	6	3	1	6	6
1	6	1	2	1	4	2	2	2	3	1	3	3	6

Рис. 92. Пример шифрования сообщения расщепленным шифром

Для получения символов криптограммы последовательность цифр в строках на рис. 91 разбивают на пары. Первую цифру в паре используют в качестве координаты строки, а вторую – в качестве координаты столбца соответствующего символа криптограммы (рис. 92). Символы криптограммы, восстановленные по таблице с помощью этих координат, приведены на рис. 92. Таким обра-

зом, каждый символ криптограммы зависит от двух символов открытого сообщения. Чтобы расшифровать криптограмму, координаты символов криптограммы записывают под ними в две строки, а затем по вертикально расположенным координатам восстанавливают исходный текст.

Длинные сообщения сначала разбивают на блоки длиной 36 символов, каждый блок шифруется отдельно.

6.2. Расщепленный шифр Trifid

Феликс Деластелль является также автором трехмерного расщепленного шифра, в котором каждый символ открытого текста расщепляется на три части. В рассматриваемом шифре для преобразования символов Феликс Деластелль использовал три таблицы размером 3×3, образующие трехмерный куб и содержащие расширенный латинский алфавит из 27 символов, в который добавлена точка. Пример заполнения шифрующих таблиц представлен на рис. 93, в левом верхнем углу указан номер страницы шифрования.

1	1	2	3
1	I	C	B
2	H	K	L
3	Q	R	S

2	1	2	3
1	M	P	G
2	T	V	N
3	F	A	.

3	1	2	3
1	W	O	X
2	E	U	J
3	D	Z	Y

Рис. 93. Пример заполнения шифрующих таблиц для шифра Trifid

В качестве примера зашифруем с помощью этих таблиц открытый текст «SECRET MESSAGE». Для этого на первом шаге запишем под буквами сообщения их координаты вертикально (рис. 94).

S	E	C	R	E	T	M	E	S	S	A	G	E
1	3	1	1	3	2	2	3	1	1	2	2	3
3	2	1	3	2	2	1	2	3	3	3	1	2
3	1	2	2	1	1	1	1	3	3	2	3	1

Рис. 94. Пример шифрования для шифра Trifid

На втором шаге выпишем координаты из трех рядов в одну строку с разбивкой по три цифры: 131, 132, 231, 122, 332, 132, 212, 333, 123, 122, 111, 133, 231.

Используя их как вертикальные координаты символов, получим криптограмму, представленную на рис. 95.

Q	R	F	K	Z	R	P	Y	L	K	I	S	F
1	1	2	1	3	1	2	3	1	1	1	1	2
3	3	3	2	3	3	1	3	2	2	1	3	3
1	2	1	2	2	2	2	3	3	2	1	3	1

Рис. 95. Результат шифрования для шифра Trifid

Расщепленный шифр является одним из наиболее стойких ручных шифров, надежность которого можно повысить путем использования набора полноразмерных шифрующих таблиц в трехмерном шифре.

7. Шифры гаммирования

В XIX в. применялось предварительное шифрование сообщений. В этом случае отправитель зашифровывал передаваемое сообщение, после чего относил шифрованное сообщение на телеграф. В XX в. такое замедление в передаче сообщений часто оказывалось неприемлемым. Потребовалось разработать методы линейного шифрования сообщений, при котором шифратор встраивался непосредственно в аппаратуру передачи сообщений, и передача шифрованного сообщения не отличалась от передачи несекретного сообщения. Реализовать линейное шифрование удалось благодаря использованию метода гаммирования. Гаммирование заключается в сложении символов исходного сообщения с символами гаммы, представленными в числовом виде, по модулю, равному мощности алфавита исходного сообщения. Результатом сложения двух целых чисел по модулю является остаток от деления суммы на модуль, например, (5+10) *mod* 4 = 3, а (30+9) *mod* 32 = 7.

В литературе шифры гаммирования называют поточными. В отличие от блочных шифров, которые при шифровании оперируют с блоками битов, выполняя криптографические преобразования блоков открытого текста, поточные шифры не делят сообщение на блоки. При использовании двоичного алфавита они представляют открытый текст в виде потока битов и выполняют шифрование каждого бита отдельно, по одному биту за операцию с помощью обратимой логической операции – XOR, которая также называется суммой по модулю 2 (□). Дешифрование также производится побитно с помощью такой же логической операции. Указанная операция выполняется между битами открытого текста и битами псевдослучайного ключевого потока, который называют гаммой (по названию буквы γ греческого алфавита, часто используемой в математических формулах для обозначения случайных величин). При суммировании по модулю 2 результат операции равен 0, если складываются одинаковые биты (0□0=0 и 1□1=0) и равен 1, если складываются разные биты (0□1=1 и 1□0=1). Таким образом, для реализации поточного шифра требуется генератор ключевого потока. Он производит поток битов k1, k2, k3, ... , km, объединяемых с помощью логической операции XOR с потоком битов p1, p2, p3, ... , pm открытого текста, в целях получения потока битов шифротекста c1, c2, c3, ... , cm, где: ci = pi□ki. При дешифровании восстановление открытого текста выполняется по формуле pi = ci□ki, то есть путем объединения с помощью операции XOR потока битов шифротекста (c1, c2, c3, ... , cm) с ключевым потоком (k1, k2, k3, ..., km), который генератор ключевого потока формирует так же, как и при шифровании (рис. 96).

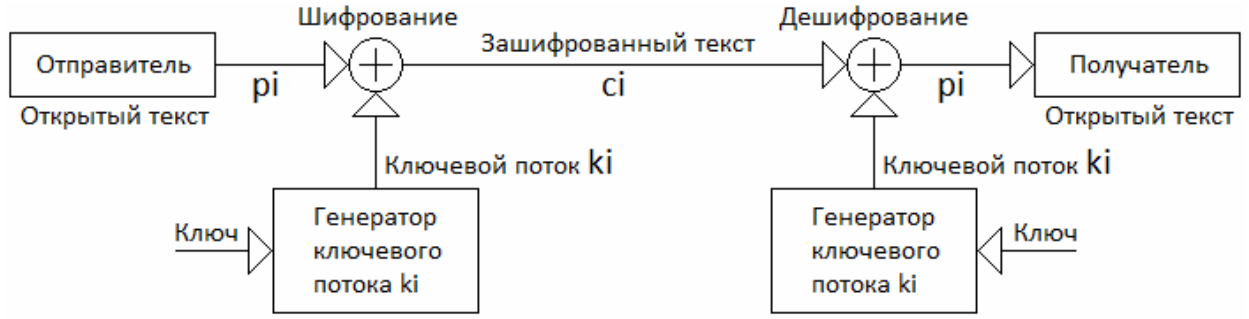

Рис. 96. Поточный шифр

Стойкость к взлому или криптостойкость поточного шифра полностью зависит от свойств генератора ключевого потока. Идеальная стойкость обеспечивается, если генератор формирует случайный ключевой поток. Однако невозможно сгенерировать две одинаковые случайные последовательности отправителем и получателем зашифрованного текста. Реально генератор формирует ключевой поток, лишь похожий на случайный, но который в действительности детерминирован и может быть воспроизведен при дешифровании. Для этого все поточные шифры используют генераторы, которые могут формировать различные псевдослучайные ключевые потоки в зависимости от ключа. При использовании одинаковых ключей отправителем в процессе шифрования и получателем во время дешифрования генераторы формируют одинаковые псевдослучайные ключевые потоки, чем и обеспечивается обратимость процедур шифрования и дешифрования.

На сегодняшний день генерирование непредсказуемых псевдослучайных последовательностей является одной из важных криптографических задач, которая ставится таким образом, чтобы при наличии определенного количества битов последовательности нельзя было предсказать следующие биты. Помимо этого, 1 и 0 на выходе генератора должны быть равновероятны.

7.1. Классификация поточных шифров

Допустим, например, что в режиме гаммирования для поточных шифров при передаче по каналу связи произошло искажение одного знака шифротекста. Очевидно, что в этом случае все знаки, принятые без искажения, будут расшифрованы правильно. Произойдет потеря лишь одного знака текста. А теперь представим, что один из знаков шифротекста при передаче по каналу связи был потерян. Это приведет к неправильному расшифрованию всего текста, следующего за потерянным знаком.

Практически во всех каналах передачи данных для поточных систем шифрования присутствуют помехи. Поэтому для предотвращения потери информации решают проблему синхронизации шифрования и расшифрования текста. По способу решения этой проблемы шифрсистемы подразделяются на синхронные и системы с самосинхронизацией.

7.2. Синхронные поточные шифры

Синхронными поточными шифрами называются шифры, в которых поток ключей генерируется независимо от открытого текста и шифротекста.

При шифровании генератор потока ключей выдает биты потока ключей, которые идентичны битам потока ключей при дешифровании. Потеря знака шифротекста приведет к нарушению синхронизации между этими двумя генераторами и невозможности расшифрования оставшейся части сообщения. Очевидно, что в этой ситуации отправитель и получатель должны повторно синхронизоваться для продолжения работы. Синхронизация должна выполняться так, чтобы ни одна часть потока ключей не была повторена.

Обычно синхронизация производится вставкой в передаваемое сообщение специальных маркеров. В результате этого пропущенный при передаче знак приводит к неверному расшифрованию лишь до тех пор, пока не будет принят один из маркеров.

7.3. Самосинхронизирующиеся поточные шифры

Самосинхронизирующимися, или асинхронными поточными шифрами называются шифры, в которых поток ключей является функцией ключа и фиксированного числа знаков шифротекста.

Поскольку внутреннее состояние генератора потока ключей является функцией предыдущих N битов шифротекста, то расшифровывающий генератор потока ключей, приняв N битов, автоматически синхронизируется с шифрующим генератором.

Реализация этого режима происходит следующим образом: каждое сообщение начинается случайным заголовком длиной N битов, который шифруется, передается и расшифровывается. После расшифровки случайного заголовка из N бит, который представлен случайной последовательностью битов и не учитывается при приеме, оба генератора будут синхронизированы, и последующие биты шифра будут приниматься и расшифроваться правильно.

8. Комбинированные шифры ADFGX и ADFGVX

Одним из важнейших требований, предъявляемых к системе шифрования, является ее высокая стойкость. Однако повышение стойкости любого метода шифрования приводит, как правило, к существенному усложнению самого процесса шифрования и увеличению затрат ресурсов (времени, аппаратных средств, уменьшению пропускной способности и т.п.).

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов

шифрования, то есть последовательное шифрование исходного текста с помощью двух или более методов.

Как показали исследования, стойкость комбинированного шифрования не ниже произведения стойкостей используемых способов.

Комбинировать можно любые методы шифрования и в любом количестве, однако на практике наибольшее распространение получили следующие комбинации:

1) подстановка + гаммирование;
2) перестановка + гаммирование;
3) гаммирование + гаммирование;
4) подстановка + перестановка.

Типичным примером комбинированного шифра может служить американская криптографическая система DES, которая является сложной компьютерной системой шифрования. Для того, чтобы получить представление о комбинированных шифрах, разберем простые комбинированные шифры.

В рассматриваемых шифрах комбинируются подстановка и перестановка. Эти шифры применяли немцы во время Первой мировой войны.

В шифре ADFGX используется матрица размером 5×5, в которую случайным образом вписываются буквы латинского алфавита. Вариант заполнения (рис. 97) является первым ключом к шифру.

	A	D	F	G	X
A	n	l	f	z	q
D	r	t	b	c	p
F	e	a	u	x	i,j
G	k	v	d	h	w
X	m	s	o	y	g

Рис. 97. Таблица шифрования шифра ADFGX

Затем выполняется предварительное шифрование по таблице: каждой букве открытого текста ставятся в соответствие две координатные буквы. Например, зашифруем по таблице текст «one two three». Результат показан на рис. 98.

o	n	e	t	w	o	t	h	r	e	e	e	e	e
XF	AA	FA	DD	GX	XF	DD	GG	DA	FA	FA	FA	FA	FA

Рис. 98. Результат первичного шифрования шифром ADFGX

Выбираем второй ключ шифра, например, «formula» и записываем под ключом результат предварительного шифрования. На данном этапе получим следующую таблицу (рис. 99). Поскольку при заполнении этой таблицы образуются пустые ячейки, дополним шифруемый текст на рис. 98 тремя буквами «e» и получим недостающие коды (в нашем примере FA, FA и FA).

f	o	r	m	u	l	a
X	F	A	A	F	A	D
D	G	X	X	F	D	D
G	G	D	A	F	A	F
A	F	A	F	A	F	A

Рис. 99. Таблица перестановки шифра ADFGX

На следующем этапе переставляем столбцы таблицы по ключу (рис. 100).

a	f	l	m	o	r	u
D	X	A	A	F	A	F
D	D	D	X	G	X	F
F	G	A	A	G	D	F
A	A	F	F	F	A	A

Рис. 100. Таблица перестановки шифра ADFGX

На последнем этапе выписываем результат шифрования по столбцам. Получим следующую криптограмму: DDFA XDGA ADAF AXAF FGGF AXDA FFFA.

Шифром ADFGX можно зашифровать только 25 символов (в латинском алфавите – 26 букв). Символы «*i*»и «*j*» шифруются одинаково, в рассматриваемом примере комбинацией FX.

Шифр ADFGVX аналогичен шифру ADFGX. Отличие состоит в размерах таблицы шифрования. В шифре ADFGVX используется таблица размером 6×6, которая позволяет шифровать 36 символов (26 символов латинского алфавита и цифры от 0 до 9).

Дешифрование шифров ADFGX и ADFGVX выполняется в обратном порядке.

Литература

1. Бабаш А.В., Шанкин Г.П. Криптография / под ред. В.П. Шерстюка, Э.А. Применко. М.: СОЛОН-ПРЕСС, 2007. 512 с.
2. Баричев С.Г. Криптография без секретов. М.: Горячая линия-Телеком. 2004. 43 с.
3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2001. 120 с
4. Введение в криптографию. 3-е изд., доп. / под общ. ред. В.В. Ященко. М.: МЦНМО: ЧеРо, 2000. 288 с.
5. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. М.: ТЕИС, 1994. 69 с.
6. Жельников В.Г. Криптография от папируса до компьютера. М.: ABF, 1996. 336 с.
7. Смарт Н. Криптография. М.: Техносфера. 2005. 528 с.
8. Соболева Т.А. История шифровального дела в России. М.: Олма-Пресс, 2002. 511 с.
9. Шеннон К. Теория связи в секретных системах: сб. // Работы по теории информации и кибернетике. М. : Изд-во иностр. лит., 1963. С. 333 - 402.
10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 816 с.

ОГЛАВЛЕНИЕ

Введение…… 3

1. Основные понятия…….. 4
2. История развития криптологии…… 5
3. Классификация криптографических алгоритмов…… 24
4. Шифры подстановки (замены)…….. 27
4.1. Моноалфавитные подстановки…… 29
4.1.1. Шифры равнозначной замены……. 29
4.1.2. Шифры пропорциональной замены (гомофонические подстановки)…….. 32
4.2. Шифры многозначной замены……. 33
4.3. Полиграммные шифры……. 34
4.4. Полиалфавитные подстановки……. 40
4.5. Многопетлевые полиалфавитные подстановки……. 49
4.6. Аналитические методы шифрования…….. 51
5. Шифры перестановки…… 59
5.1. Шифры одинарной перестановки…… 59
5.1.1. Шифр простой одинарной перестановки…… 59
5.1.2. Шифр блочной одинарной перестановки……... 60
5.2. Шифры маршрутной перестановки……. 60
5.2.1. Шифры простой маршрутной перестановки…….. 60
5.2.2. Шифры маршрутной перестановки на основе магических квадратов…….. 61
5.2.3. Шифры маршрутной перестановки на основе решеток… 63
5.2.4. Шифры множественной перестановки……... 66
5.2.5. Трехмерные маршрутные перестановки……. 67
6. Шифры дробления……. 69
6.1. Расщепленный шифр Bifid……... 69
6.2. Расщепленный шифр Trifid…….. 71
7. Шифры гаммирования……... 72
7.1. Классификация поточных шифров…….. 73
7.2. Синхронные поточные шифры…… 74
7.3. Самосинхронизирующиеся поточные шифры……... 74
8. Комбинированные шифры ADFGX и ADFGVX……..... 74

Литература 77

Учебное издание

Гиль Владимир Тимофеевич

кандидат технических наук, доцент

КЛАССИЧЕСКИЕ АЛГОРИТМЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ИНФОРМАЦИИ

Учебное пособие

Редактор Н.Ю. Орел

Подписано в печать 15.11.2013. Формат 60х84 1/16.
Бумага офис. Усл. печ. л. 4,65.
Тираж 50 экз. Заказ № 81.
Дальневосточный юридический институт МВД РФ.
Редакционно-издательский отдел. Типография.
680020, г. Хабаровск, Казарменный пер., 15.

Для заметок