ПРЕДИСЛОВИЕ

Информационная безопасность — одна из главных проблем, с которой сталкивается современное общество. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации. Решение проблемы информационной безопасности связано с гарантированным обеспечением трех ее главных составляющих: *доступности*, *целостности* и *конфиденциальности*.

Предлагаемый практикум включает 12 методических описаний лабораторных работ с комплектом исполняемых модулей. Весь практикум разделен на три части с той целью, чтобы при проведении занятий преподаватель в зависимости от количества часов, выделенных на проведение занятий, и своего видения курса мог выбирать из предложенных разделов те или иные работы.

В первую часть включены практические задания: по методам шифрования, использующим классические симметричные алгоритмы; исследованиям различных методов защиты текстовой информации и их стойкости на основе подбора ключей; изучению устройства и принципа действия шифровальной машины «Энигма» с использованием программного эмулятора; изучению современного стандарта симметричного шифрования AES Rijndael.

При выполнении практических заданий первой части предполагается рассмотрение следующих вопросов.

Изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров (лабораторная работа № 1).

Рассмотрение методов шифрования/расшифрования перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. Исследование и сравнение стойкости различных методов на основе атак путем перебора всех возможных ключей (лабораторная работа № 2).

Изучение принципов шифрования/расшифрования информации, используемых в шифровальной машине «Энигма». Ознакомление с общими принципами действия шифровальной машины «Энигма» на примере эмулятора Enigma3S (лабораторная работа № 3).

Ознакомление с принципами шифрования, используемыми в алгоритме симметричного шифрования AES Rijndael (лабораторная работа № 4).

Вторая часть включает практические задания для изучения процессов генерации простых чисел для систем асимметричного шифрования; процессов постановки и верификации электронной цифровой подписи; исследования шифра скользящей перестановки; изучения пакета PGP (Pretty Good Privacy) — программного обеспечения для защиты конфиденциальной информации.

При выполнении практических заданий из второй части предполагается рассмотрение следующих вопросов.

Рассмотрение методов генерации простых чисел, используемых в системах шифрования с открытым ключом (лабораторная работа № 5).

Знакомство с основными положениями федеральной целевой программы «Электронная Россия». Ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (лабораторная работа № 6).

Исследование шифра скользящей перестановки с использованием программной реализации XY-Mover (лабораторная работа № 7).

Ознакомление с общими принципами построения и использования программных средств защиты информации, в частности с программой PGP.

Освоение средств программной системы PGP, предназначенных:

- для шифрования конфиденциальных ресурсов и разграничения доступа к ним;
- обеспечения целостности информационных ресурсов с помощью механизма электронной цифровой подписи;
- надежного уничтожения остаточной конфиденциальной информации;
- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска (лабораторная работа № 8).

В третью часть включены работы по исследованию механизмов сохранения целостности информации с использованием кодов, исправляющих ошибки (коды Хэмминга и CRC-коды), и эффективному сжатию данных: алгоритмы сжатия по Шеннону — Фано, Хаффмену и LZW-сжатие.

При выполнении практических заданий третьей части рассматриваются следующие вопросы.

Ознакомление с общими принципами построения и использования корректирующих кодов для контроля целостности информа-

ции, распространяемой по телекоммуникационным каналам. Изучение принципов построения кодов Хэмминга и циклических кодов (лабораторные работы № 9 и 10).

Рассмотрение статистических принципов сжатия информации с использованием методов Шеннона — Фано и Хаффмена (лабораторная работа № 11).

Ознакомление с принципами сжатия информации с использованием метода LZW (Lempel — Ziv — Welch) (лабораторная работа № 12).

В практикум вошли материалы лабораторных работ, которые проводились авторами на протяжении последних лет для студентов Российского государственного социального университета (РГСУ) и Московского государственного университета экономики, статистики и информатики (МЭСИ). Большая часть демонстрационных программ для исследования процессов защиты информации написаны студентами этих вузов под руководством авторов в рамках курсовых и дипломных работ.

ЧАСТЬ 1

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Проблемы защиты информации. В настоящее время во всем мире резко повысилось внимание к проблеме информационной безопасности. Это обусловлено процессами стремительного расширения потоков информации, пронизывающих все сферы жизни общества.

Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности. Она приобрела ощутимую стоимость, которая определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба с разной степенью вероятности наносимого владельцу информации. Однако создание индустрии переработки информации порождает целый ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях.

Появление глобальных компьютерных сетей сделало простым доступ к информации как отдельным пользователям, так и большим организациям. Однако легкость и высокая скорость доступа к данным с помощью таких компьютерных сетей, как Internet, также сделали значительными следующие угрозы безопасности данных при отсутствии мер их защиты:

- неавторизованный доступ к информации;
- неавторизованное изменение информации;
- неавторизованный доступ к сетям и сервисам;
- другие сетевые атаки, например повтор перехваченных ранее транзакций и атаки типа «отказ в обслуживании».

При обработке любой значимой информации при помощи отдельного компьютера, а тем более в сети, возникает вопрос о ее защите от несанкционированного доступа и использования. Наиболее распространенный в компьютерных системах способ защиты — использование паролей — более пригоден для защиты доступа к вычислительным ресурсам, нежели для защиты информации. Пароль — своеобразный экран, отгораживающий законных пользователей системы от посто-

ронних, пройдя сквозь который санкционированный пользователь получает доступ практически ко всей информации.

В настоящее время исключительно важное значение в разных областях приобрели вопросы, связанные с сохранением и передачей конфиденциальной информации. Возникающие при этом задачи решает *криптография* — наука о методах преобразования информации в целях ее защиты от незаконных пользователей.

Ретроспективный взгляд на историю развития криптографии как специфическую область человеческой деятельности позволяет выделить три основных периода. Первый, наиболее продолжительный, — период «ручной криптографии». Его начало теряется в глубокой древности, а закончился он в 1930-е гг. Криптография прошла путь от магического искусства до вполне прозаической прикладной специальности чиновников дипломатических и военных ведомств.

Второй период — создание и широкое внедрение в практику сначала механических, затем электромеханических и электронных устройств шифрования, организация целых сетей засекреченной связи. Его началом можно считать разработку Гилбертом Вернамом (G. Vernam) в 1917 г. схемы телеграфной шифровальной машины, использующей одноразовую гамму (рис.1.1).

Рис. 1.1. Схема шифрования методом Вернама

К середине 1970-х гг. с развитием разветвленных коммерческих сетей связи, электронной почты и глобальных информационных систем на первый план вышли новые проблемы — снабжения ключами и подтверждения подлинности.

В 1976 г. американские ученые Уитфилд Диффи (W. Diffie) и Мартин Хеллман (M. Hellman) предложили два новых принципа организации засекреченной связи без предварительного снабжения абонентов

секретными ключами шифрования — принцип так называемого *открытого шифрования* и принцип *открытого распределения ключей*. Этот момент можно считать началом нового периода в развитии криптографии. В настоящее время это направление современной криптографии очень интенсивно развивается.

Из истории криптографии. Понятие «безопасность» охватывает широкий круг интересов как отдельных лиц, так и целых государств. Во все исторические времена существенное внимание уделялось проблеме информационной безопасности, обеспечению защиты конфиденциальной информации от ознакомления, кражи, модификации, подмены. Решением этих вопросов занимается криптография.

Термин «криптография» (тайнопись) ввел английский математик Джон Валлис (John Wallis) (1616—1703) (рис. 1.2). Потребность шифровать и передавать шифрованные сообщения возникла очень давно.

Сцитала. Еще в V—VI вв. до н.э. греки использовали специальное шифрующее устройство. По описанию Плутарха, это устройство состояло из двух цилиндрических стержней одинаковой длины и толщины, которые называли *сциталами* (рис. 1.3). При необходимости передачи сообщения длинную ленту папируса наматывали на сциталу, не оставляя на ней никакого промежутка, и писали на нем необходимую информацию. Затем папирус снимали и без стержня отправляли адресату. Поскольку буквы оказывались разбросанными в беспорядке, то прочитать сообщение мог только тот, кто имел свою сциталу такой же длины и толщины, чтобы намотать на нее папирус.

Рис. 1.2. Джон Валлис

Квадрат Полибия[1]. В Древней Греции (II в. до н.э.) был известен шифр, называемый *квадратом Полибия*. Это устройство представляло собой квадрат 5×5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку записывалась одна буква (в греческом варианте одна клетка оказывалась пустой, а в латинском — в одну клетку помещали две буквы: I, J). В результате каждой букве отвечала пара чисел по номеру строки и столбца.

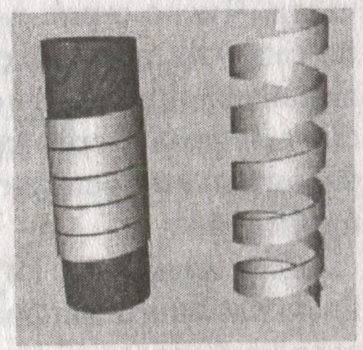

Рис. 1.3. Сцитала

[1] Полибий (200—120 гг. до н.э.) — древнегреческий историк.

Пример квадрата Полибия приведен на рис. 1.4.

	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

а

13 34 22 24 44 34 15 42 22 34 43 45 32

Congito ergo sum (лат.) — «Я мыслю, следовательно, существую» (Р. Декарт).

б

Рис. 1.4. Квадрат Полибия (*а*) и пример шифрования (*б*)

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

Пример кода Цезаря изображен на рис. 1.5.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

а

YHQL YLGL YLFL

Veni vidi vici (лат.) — «Пришел, увидел, победил» (Ю. Цезарь. Донесение Сенату о победе над понтийским царем).

б

Рис. 1.5. Код Цезаря (*а*) и пример шифрования (*б*)

Шифр Цезаря относится к так называемому классу *моноалфавитных подстановок* и имеет множество модификаций.

Решетка Кардано. Широко известны шифры, относящиеся к классу *перестановки,* в частности «*решетка Кардано*»[1]. Это прямоугольная карточка с отверстиями, чаще всего квадратная, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. Число строк и столбцов на карточке четное. Карточка сделана так, что при последовательном ее поворачивании каждая клетка лежащего под ней листа окажется занятой. Карточку поворачивают сначала вдоль вертикальной оси симметрии на 180°, а затем вдоль горизонтальной оси также на 180° (рис. 1.6). И вновь повторяют ту же процедуру.

Диск Альберти. Итальянец Альберти (XVI в.) впервые выдвинул идею двойного шифрования — текст, полученный в результате первого шифрования, подвергался повторному шифрованию. В трактате

[1] Кардано Джероламо (1501—1576) — итальянский математик, философ и врач.

Альберти был приведен его собственный шифр, который он назвал «шифром, достойным королей». Он утверждал, что этот шифр недешифруем. Реализация шифра осуществлялась с помощью шифровального диска, положившего начало целой серии *многоалфавитных подстановок.* Устройство представляло собой пару дисков — внешний, неподвижный (на нем были нанесены буквы в естественном порядке и цифры от 1 до 4) и внутренний — подвижный (на нем буквы были переставлены) (рис. 1.7). Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замену ее на соответствующую (стоящую под ней) букву шифрованного текста. После шифрования нескольких слов внутренний диск сдвигался на один шаг. Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска.

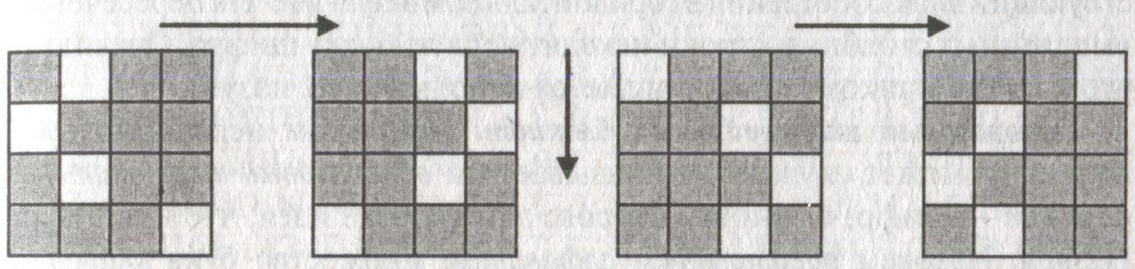

Рис. 1.6. Решетка Кардано

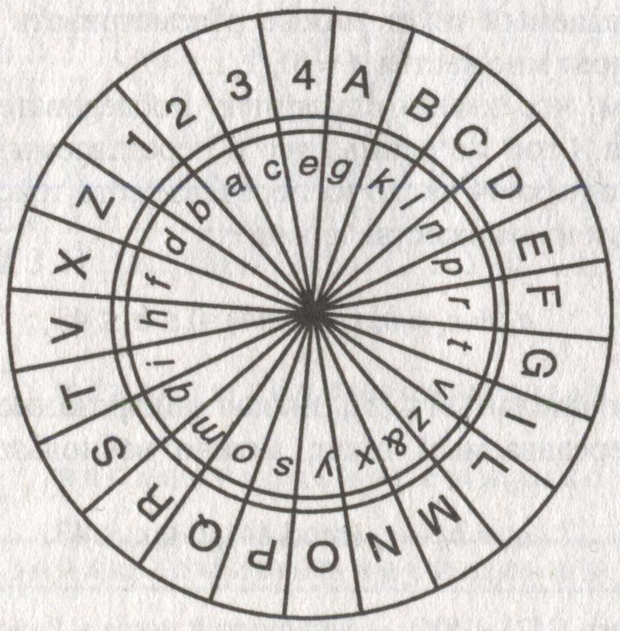

Рис. 1.7. Диск Альберти

Таблица Виженера[1]. Неудобство рассмотренных выше шрифтов моноалфавитных подстановок очевидно, так как в случае использования стандартного алфавита таблица частот встречаемости букв алфавита позволяет определить один или несколько символов, а этого иногда достаточно для вскрытия шифра («Пляшущие человечки» Конан Дойля или «Золотой жук» Эдгара По). Поэтому, для того чтобы затруднить дешифрование, использовали различные приемы, например *таблицу Виженера*, представляющую собой квадратную таблицу с числом строк и столбцов, равным количеству букв алфавита (рис 1.8). Чтобы зашифровать какое-либо сообщение, выбирают слово-лозунг (например, «монастырь») и надписывают его над сообщением с необходимым повторением.

Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого, в вертикальном алфавите, а ему — соответствующий знак сообщения в горизонтальном алфавите. На пересечении выделенных столбца и строки находят первую букву шифра. Очевидно, что ключом к такому шифру является используемый лозунг.

Одноразовый шифровальный блокнот. Примером нераскрываемого шифра может служить так называемый *одноразовый шифровальный блокнот* — шифр, в основе которого лежит та же идея, что и в шифре Цезаря. Назовем *расширенным алфавитом* множество букв алфавита и знаков препинания {. , : ; ! ? () — “ <пробел>}, число символов расширенного кириллического алфавита в данном варианте будет равно 44. Занумеруем символы расширенного алфавита числами от 0 до 43. Тогда любой передаваемый текст можно рассматривать как последовательность $\{a_n\}$ чисел множества $A = \{0, 1, ..., 43\}$.

Предположим, что имеем случайную последовательность $\{c_n\}$ из чисел множества A той же длины, что и передаваемый текст — *ключ*. Складывая по модулю 44 число из передаваемого текста a_n с соответствующим числом из множества ключа c_n:

$$a_n + c_n \equiv b_n \pmod{44},\ 0 \le b_n \le 43,$$

получим последовательность $\{b_n\}$ знаков шифрованного текста. Чтобы получить передаваемый текст, можно воспользоваться тем же ключом:

$$a_n \equiv b_n - c_n \pmod{44},\ 0 \le a_n \le 43.$$

[1] Блез де Виженер (1523—1596) — французский посол в Риме, который написал большой труд о шифрах. Квадратный шифр Виженера на протяжении почти 400 лет не был дешифрован и считался недешифруемым шифром.

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

а

м о н а с т ы р ь м о н а с т ы р ь м о н

р а с к и н у л о с ь м о р е ш и р о к о

э о я к щ а п ы й ю й щ о в ч ф ш л ь ш ы

б

Рис. 1.8. Таблица Виженера (*а*) и пример шифрования (*б*)

У двух абонентов, находящихся в секретной переписке, имеются два одинаковых блокнота. В каждом из них на нескольких листах напечатана случайная последовательность чисел множества *A*. Отправитель свой текст шифрует указанным выше способом при помощи первой страницы блокнота. Зашифровав сообщение, он уничтожает использованную страницу и отправляет текст сообщения второму абоненту. Получатель шифрованного текста расшифровывает его и также уничтожает использованный лист блокнота. Очевидно, что одноразовый шифр не раскрываем в принципе, так как символ в тексте может быть заменен любым другим символом и этот выбор совершенно случаен.

Методы шифрования. ***Одноалфавитный метод***[1]. Данный метод, пожалуй, самый древний из всех известных методов. В его основе лежит простой способ шифрования: отправитель и получатель зашифрованного документа заранее договариваются об определенном смещении букв относительно их обычного местоположения в алфавите. Например, для кириллицы если смещение равно 1, то буква «А» соответствует букве «Б», «Б» — «В» и т.д. Когда алфавит заканчивается, берут буквы из начала списка. И выходит, например, следующее: из слова КОДИРОВАНИЕ получается ЛПЕЙСПГБОЙЖ.

Частным случаем этого является ранее рассмотренный шифр Цезаря. Очевидно, что произвольный шифр из класса одноалфавитных методов не является шифром Цезаря (если мощность алфавита текста равна *n*, то число шифров Цезаря равно *n*, а число всех одноалфавитных шифров — *n!*). Однако и для таких методов легко предложить способы дешифрования, основанные на статистических свойствах шифрованных текстов, поскольку открытый и закрытый тексты имеют одинаковые статистические характеристики.

Шифрование методом перестановки символов. Суть этого метода заключается в том, что символы текста переставляются по определенным правилам, при этом используются только символы исходного (незашифрованного) текста. Перестановки в классической криптографии обычно получают в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры. Простейшим примером перестановки является запись исходного текста по строкам некоторой матрицы и чтение его по столбцам этой матрицы.

Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом. Таким образом, для матрицы размером

[1] В лабораторной работе № 1 рассматриваются два варианта одноалфавитного метода: с фиксированным смещением и с произвольным (задаваемым) смещением.

8×8 (длина блока 64 символа) возможно $1{,}6\times10^9$ ключей, что позволяет на современных компьютерах путем перебора дешифровать текст. Однако для матрицы размером 16×16 (длина блока 256 символов) существует $1{,}4\times10^{26}$ ключей, и перебор их с помощью современных вычислительных средств весьма затруднителен.

Примером применения метода перестановки символов является восьмиэлементная таблица, обладающая совокупностью маршрутов, которые называются «маршруты Гамильтона». Последовательность заполнения таблицы каждый раз соответствует нумерации ее элементов. Если длина шифруемого текста не кратна числу элементов, то при последнем заполнении в свободные элементы заносится произвольный символ. Выборка из таблицы для каждого заполнения может выполняться по своему маршруту, при этом маршруты могут использоваться как последовательно, так и в порядке, задаваемом ключом.

Для методов перестановки характерны простота алгоритма, возможность программной реализации и низкий уровень защиты, так как при большой длине исходного текста в его зашифрованном варианте проявляются статистические закономерности ключа, что и позволяет его быстро раскрыть. Другой недостаток этих методов — легкое раскрытие, если удается направить в систему для шифрования несколько специально подобранных сообщений. Так, если длина блока в исходном тексте равна *K* символам, то для раскрытия ключа достаточно пропустить через шифровальную систему $K-1$ блоков исходного текста, в которых все символы, кроме одного, одинаковы.

Шифрование инверсными символами (по дополнению до 255). Данный метод шифрования является частным случаем одноалфавитной замены в алфавите мощности 256. Суть метода заключается в замене символа ASCII-кодировки с номером *i* на символ с номером $255-i$. Аналогично проводится и операция расшифрования.

Многоалфавитные методы шифрования[1]. Многоалфавитное шифрование (многоалфавитная замена) заключается в том, что для последовательных символов шифруемого текста используются одноалфавитные методы с различными ключами.

Например, первый символ заменяется по методу Цезаря со смещением 14, второй — со смещением 10 и т.д. до конца заданного ключа. Затем процедура продолжается периодически. Более общей является ситуа-

[1] В лабораторной работе № 1 рассматриваются три варианта многоалфавитного метода: с фиксированным ключом, с ключом фиксированной длины и с ключом произвольной длины.

ция, когда используется не шифр Цезаря, а последовательность произвольных подстановок, соответствующих одноалфавитным методам.

Более наглядным примером подобного шифрования является метод гаммирования. Этот способ преобразования заключается в том, что символы закрываемого текста последовательно складываются с символами некоторой специальной последовательности, именуемой гаммой. Такое преобразование иногда называют наложением гаммы на открытый текст.

Собственно процедура наложения может осуществляться одним из двух способов:

1) символы закрываемого текста и гаммы заменяются цифровыми эквивалентами, а затем складываются по модулю K:

$$T_{ш} = (T_{о} \oplus T_{г}) \bmod K,$$

где $T_{ш}$ — шифротекст; $T_{о}$ — открытый текст; $T_{г}$ — гамма; K — количество символов алфавита;

2) символы текста и гаммы представляются в двоичных кодах, а затем каждая пара двоичных разрядов складывается по mod 2.

Стойкость шифрования методом гаммирования определяется главным образом качеством гаммы, которое характеризуется длиною периода и случайностью распределения по периоду.

Длинна периода гаммы — минимальное количество символов, после которого последовательность начинает повторяться. Случайность распределения символов по периоду означает отсутствие закономерностей между появлением различных символов в пределах периода.

Основные требования, предъявляемые к методам шифрования информации:

- сложность и трудоемкость процедур шифрования и расшифрования должны определяться в зависимости от степени секретности защищаемых данных;
- надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику известен способ закрытия;
- способ закрытия и набор используемых служебных данных (ключевых установок) не должны быть слишком сложными. Затраты на защитные преобразования должны быть приемлемые при заданном уровне сохранности информации;
- выполнение процедур прямого и обратного преобразования должно быть формальным и как можно проще;

- процедуры прямого и обратного преобразования не должны зависеть от длины сообщения;
- ошибки, возникающие в процессе преобразования, не должны распространяться по системе и вызывать потерю информации. Из-за появления ошибок передачи зашифрованного сообщения по каналам связи не должна исключаться возможность надежной расшифровки текста на приемном конце;
- избыточность сообщений, вносимая закрытием, должна быть как можно меньшей;
- объем ключа не должен затруднять его запоминание и пересылку.

Гистограмма текста[1]. Одним из наиболее известных методов криптоанализа является изучение статистических характеристик шифрованных текстов. Графическое отображение совокупности частот встречаемости символов в тексте называют гистограммой этого текста.

Предположим, что мы имеем дело с методом одноалфавитного шифрования. Зная частоту встречаемости букв в алфавите, можно предположить, какая буква была заменена на данную. Например, часто встречаемая буква «О» заменена на редко встречающуюся букву «Щ».

Следует иметь в виду, что вид гистограммы для стандартного распределения зависит от вида исходного текста следующим образом: если исходный текст содержит символы кириллицы и латинского алфавита, то выводится статистическое распределение для кириллицы и латиницы, если только кириллицы (латиницы), то выводится статистическое распределение для кириллицы (латиницы).

[1] Для наглядности в лабораторной работе № 1 используются двойные гистограммы, отображающие частоту встречаемости символов в исходном и зашифрованном текстах.