ТЕМА 2.9 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Классификация методов криптографического преобразования информации

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

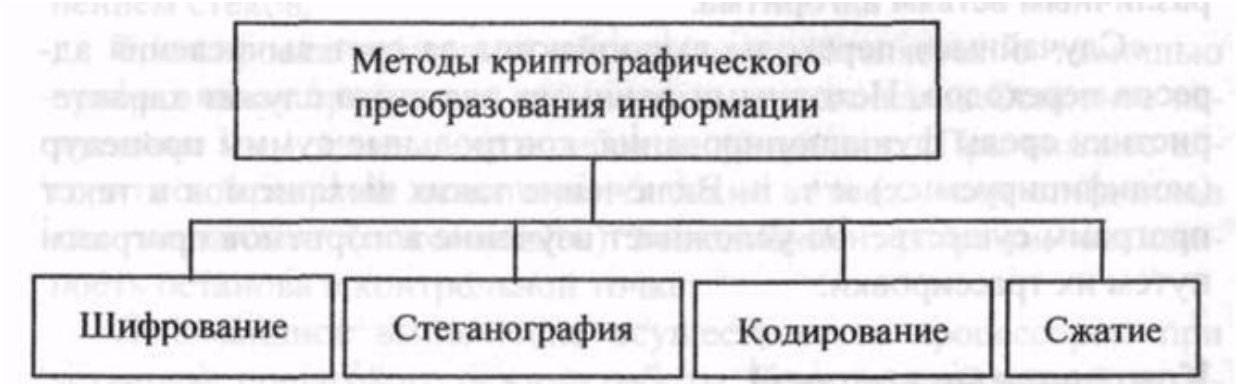

Рис. 14. Классификация методов криптографического преобразования информации

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы (рис. 14).

Процесс **шифрования** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация,

подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую ин- формацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования.

В отличие от других методов криптографического преобразования информации, методы **стеганографии** [2] позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается, но проведенные исследования показывают ее перспективность. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в КС открыла практически неограниченные возможности перед стеганографией.

Существует несколько методов скрытой передачи информации. Одним из них является простой метод скрытия файлов при работе в операционной системе MS DOS. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка EOF (комбинация клавиш Control и Z). При обращении к этому текстовому файлу стандартными средствами ОС считывание прекращается по достижению метки EOF и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информация представляются в числовом виде. Так в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды

определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ. Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т. п. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Ком- плексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса **кодирования** информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях АСУ. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть

сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрова- нию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

2. Шифрование. Основные понятия

Основным видом криптографического преобразования информации в КС является шифрование. Под **шифрованием** понимается процесс преобразования открытой информации в зашифрованную информацию **(шифртекст)** или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название **зашифрование,** а процесс преобразования закрытой информации в открытую - **расшифрование.**

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. **Методом шифрования (шифром)** называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление ЭВМ и КС инициировало процесс разработки новых шифров, учитывающих возможности использования ЭВМ как для зашифрования/расшифрования информации, так и для атак на шифр. Атака на шифр **(криптоанализ)** - это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

♦ стойкость шифра противостоять криптоанализу **(криптостойкость)** должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;

- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифртекст не должен существенно превосходить по объему исходную информацию;

ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации - перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

В качестве примера удачного метода шифрования можно привести шифр DES (Data Encryption Standard), применяемый в США с 1978 года в качестве государственного стандарта. Алгоритм шифрования не является секретным и был опубликован в открытой печати. За все время использования этого шифра не было обнародовано ни одного случая обнаружения слабых мест в алгоритме шифрования.

В конце 70-х годов использование ключа длиной в 56 бит гарантировало, что

для раскрытия шифра потребуется несколько лет непрерывной работы самых мощных по тем временам компьютеров. Прогресс в области вычислительной техники позволил значительно сократить время определения ключа путем полного перебора. Согласно заявлению специалистов Агентства национальной безопасности США 56-битный ключ для DES может быть найден менее чем за 453 дня с использованием суперЭВМ Cray T3D, которая имеет 1024 узла и стоит 30 млн. долл. Используя чип FPGA (Field Progammably Gate Array - программируемая вентильная матрица) стоимостью 400 долл., можно восстановить 40-битный ключ DES за 5 часов. Потратив 10000 долл. за 25 чипов FPGA, 40-битный ключ можно найти в среднем за 12 мин. Для вскрытия 56-битного ключа DES при опоре на серийную техноло-

гию и затратах в 300000 долл. требуется в среднем 19 дней, а если разработать специальный чип, то - 3 часа. При затратах в 300 млн. долл. 56- битные ключи могут быть найдены за 12 сек. Расчеты показывают, что в настоящее время для надежного закрытия информации длина ключа должна быть не менее 90 бит.

Все методы шифрования могут быть классифицированы по различным признакам. Один из вариантов классификации приведен на рис. 15 [8].

3. Методы шифрования с симметричным ключом Методы замены

Сущность методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу [56]. Самым простым является *метод прямой замены.* Символам исходного алфавита Ао, с помощью которых записывается ис- ходная информация, однозначно ставятся в соответствие символы Su шифрующего алфавита Аь В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы русского алфавита.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста To, длиной - K символов, по определенному алгоритму.

Алгоритм моноалфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1. Формирование числового кортежа Loь путем замены каждого символа soi e To (i=l,K), представленного в исходном алфавите Ao размера [lxR], на число hoi(soj), соответствующее порядковому номеру символа soi в алфавите Ao.

Шаг 2. Формирование числового кортежа Lih путем замены каждого числа кортежа Loh на соответствующее число Hli кортежа Lih, вычисляемое по формуле:

Ьн = (kixhoi(so)+k)(mod R),

где ki - десятичный коэффициент; к2 - коэффициент сдвига. Выбранные коэффициенты к1 к2 должны обеспечивать однозначное соответствие чисел hOi и hli, а при получении hli = 0 выполнить замену hli = R.

Шаг 3. Получение шифр текста Ti путем замены каждого числа hii(sli) кортежа L,h соответствующим символом SLI e Ti (i=l,K) алфавита шифрования A) размера [1XR].

Шаг 4. Полученный шифртекст разбивается на блоки фиксированной длины b. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).

Рис. 15. Классификация методов шифрования

Пример. Исходными данными для шифрования являются: T0 =

<МЕТОД_ШИФРОВАНИЯ>;

Ao = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩ **ЪЫЬЭЮЯ** >;

A1 = <ОРЩЬЯТЭ_ЖМЧХАВДЫФКСЕЗПИЦГН ЛЪШБУЮ>;

R=32; ki=3; k2=15, b=4.

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг1.Loh = <12,6,18,14,5,32,24,9,2O,16,14,3,1,13,9,31>. Шаг2.Lh1 = <19,1,5,25,30,15,23,10,11,31,25,24,18,22,10,12>. Шаг3.T1 = <СОЯГБДИМЧУГЦКПМХ>.

Шаг4.T2 = <СОЯГБДИМЧУГЦКПМХ>.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифртекст Ti длиной К символов. Расшифрование осуществляется путем решения целочисленного уравнения:

k1hoi+k2=nR+h1i,

При известных целых величинах k|,k2, hli и R величина hoi вычисляется методом перебора п.

Последовательное применение этой процедуры ко всем символам шифр текста приводит к его расшифрованию.

По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются в одном столбце (табл. 1).

Таблица 1

Таблица замены

s_{0i}	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш								
h_{0i}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24								
s_{1i}	К	З	Ц	Л	Б	О	Ь	Э	М	А	Ы	С	П	Г	Ъ	У	Р	Я	_	Ч	В	Ф	Е	И								
h_{1i}	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2	5	8	11	14	17	20	23								

s_{0i}	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
h_{0i}	25	26	27	28	29	30	31	32
s_{1i}	Н	Ш	Ю	Щ	Т	Ж	Х	Д
h_{1i}	26	29	32	3	6	9	12	15

Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки Soi таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки Sli, находящегося в том же столбце i таблицы. Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке Sli-

Основным недостатком метода прямой замены является наличие одних и тех же статистических характеристик исходного и закрытого текста. Зная, на каком языке написан исходный текст и частотную характеристику употребления символов алфавита этого языка, криптоаналитик путем статистической обработки пере- хваченных сообщений может установить соответствие между символами обоих алфавитов.

Существенно более стойкими являются методы полиалфавитной замены. Такие методы основаны на использовании нескольких алфавитов для замены символов исходного текста. Формально полиалфавитную замену можно представить следующим образом. При N - алфавитной замене символ Soi из исходного алфавита Ao заменяется символом sll из алфавита A1, S02 заменяется символом S22 из алфавита A2 и так далее. После замены SON СИМВОЛОМ S NN ИЗ AN СИМВОЛ So(N+i) замещается символом S1(N+1) ИЗ алфавита Ai и так далее.

Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера Тв, которая представляет собой квадратную матрицу [RxR], где R - количество символов в используемом алфавите. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). Если используется русский алфавит, то матрица Вижинера имеет размерность [32x32] (рис. 16).

Шифрование осуществляется с помощью ключа, состоящего из M

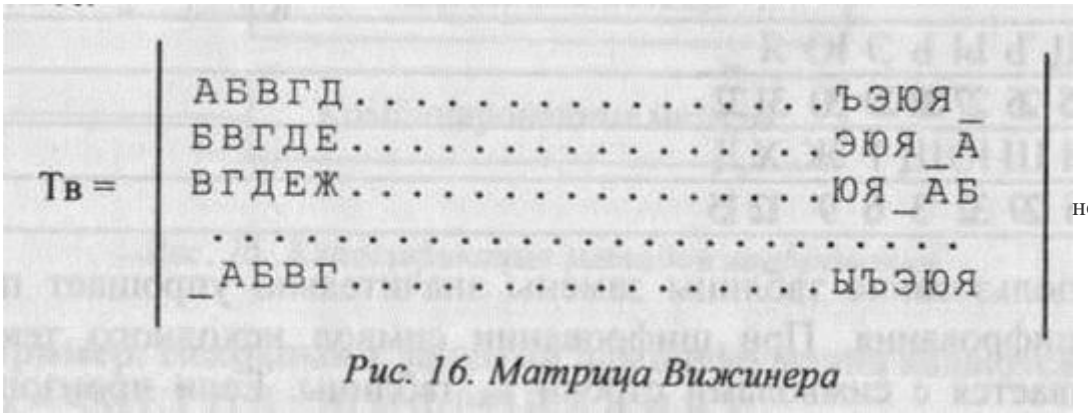

Рис. 16. Матрица Вижинера

неповторяющихся символов. Из полной матрицы Вижинера выделяется матрица шифрования Тш, размерностью [(M+1),R]. Она включает первую строку и строки, первые элементы которых совпадают с символами ключа. Если в качестве ключа выбрано слово <ЗОНД>, то матрица

шифрования содержит пять строк (рис. 17).

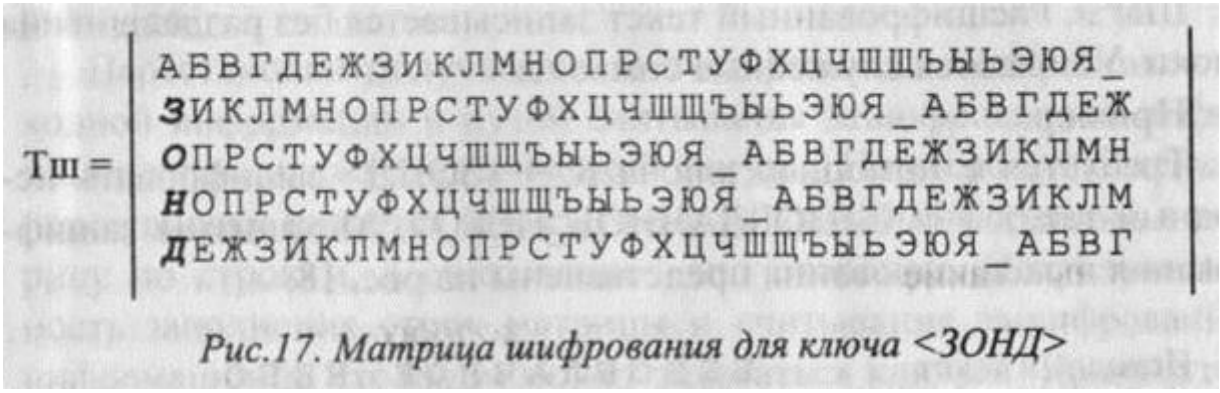

Рис.17. Матрица шифрования для ключа <ЗОНД>

Алгоритм зашифрования с помощью таблицы Вижинера представляет собой следующую последовательность шагов.

Шаг 1. Выбор ключа К длиной М символов.

Шаг 2. Построение матрицы шифрования Тш=(Ьiq) размерностью [(M+1),R] для выбранного ключа К.

Шаг 3. Под каждым символом Sor исходного текста длиной I символов размещается символ ключа km (рис. 20). Ключ повторяется необходимое число раз.

Шаг 4. Символы исходного текста последовательно замещаются символами, выбираемыми из Тш по следующему правилу:

1) определяется символ km ключа К, соответствующий заме щаемому символу sor;

2) находится строка i в Тш, для которой выполняется усло вие km=bil;

3) определяется столбец j, для которого выполняется условие: sOr=bij;

4) символ sor замещается символом by.

Шаг 5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

Расшифрование осуществляется в следующей последовательности:

Шаг 1. Под шифртекстом записывается последовательность символов ключа по аналогии с шагом 3 алгоритма зашифрования.

Шаг 2. Последовательно выбираются символы Sir из шифртекста и соответствующие символы ключа km. В матрице Тш определяется строка i, для которой выполняется условие km= bu. В строке i определяется элемент by= s]r. В расшифрованный текст на позицию г помещается символ bij.

Шаг 3. Расшифрованный текст записывается без разделения на блоки.

Убираются служебные символы.

Пример.

Требуется с помощью ключа К = <ЗОНД> зашифровать исходный текст Т =

<БЕЗОБЛАЧНОЕ НЕБО>. Механизмы зашифрования и расшифрования представлены на рис. 18.

Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО
Ключ	ЗОНДЗОНДЗОНДЗОНД
Текст после замены	ИУФТИШНЫФЫТГФУОТ
Шифртекст	ИУФТ ИШНЫ ФЫТГ ФУОТ
Ключ	ЗОНД ЗОНД ЗОНД ЗОНД
Расшифрованный текст	БЕЗО БЛАЧ НОЕ_ НЕБО
Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО

Рис. 18. Пример шифрования с помощью матрицы Вижинера

Криптостойкость методов полиалфавитной замены значительно выше методов простой замены, так как одни и те же символы исходной последовательности могут заменяться разными символами. Однако стойкость шифра к статистическим методам криптоанализа зависит от длины ключа.

Для повышения криптостойкости может использоваться модифицированная

матрица шифрования. Она представляет собой матрицу размерности [11,R], где R - число символов алфавита. В первой строке располагаются символы в алфавитном порядке. Остальные 10 строк нумеруются от 0 до 9. В этих строках символы располагаются случайным образом.

В качестве ключей используются, например, непериодические бесконечные числа *n,* е и другие. Очередной n-й символ исходного текста заменяется соответствующим символом из строки матрицы шифрования, номер которой совпадает с n-й цифрой бесконечного числа.

2. Методы перестановки

Суть методов перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановке символов внутри каждого блока по определенному алго-ритму[56].

Перестановки получаются за счет разницы путей записи исходной информации и путей считывания зашифрованной информации в пределах геометрической фигуры. Примером простейшей перестановки является запись блока исходной информации в матрицу по строкам, а считывание - по столбцам. Последователь- ность заполнения строк матрицы и считывания зашифрованной информации по столбцам может задаваться ключом. Криптостойкость метода зависит от длины блока (размерности матрицы). Так для блока длиной 64 символа (размерность матрицы 8x8) возможны 1,6x109 комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16x16) число возможных ключей достигает 1,4x1026. Решение задачи перебора ключей в последнем случае даже для современных ЭВМ представляет существенную сложность.

Перестановки используются также в методе, основанном на применении *маршрутов Гамильтона.* Этот метод реализуется путем выполнения следующих шагов.

Шаг 1. Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например, *).

Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (рис. 19).

Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом К.

Шаг 4. Зашифрованная последовательность символов разбивается на блоки фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходная информация на шаге 1.

Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

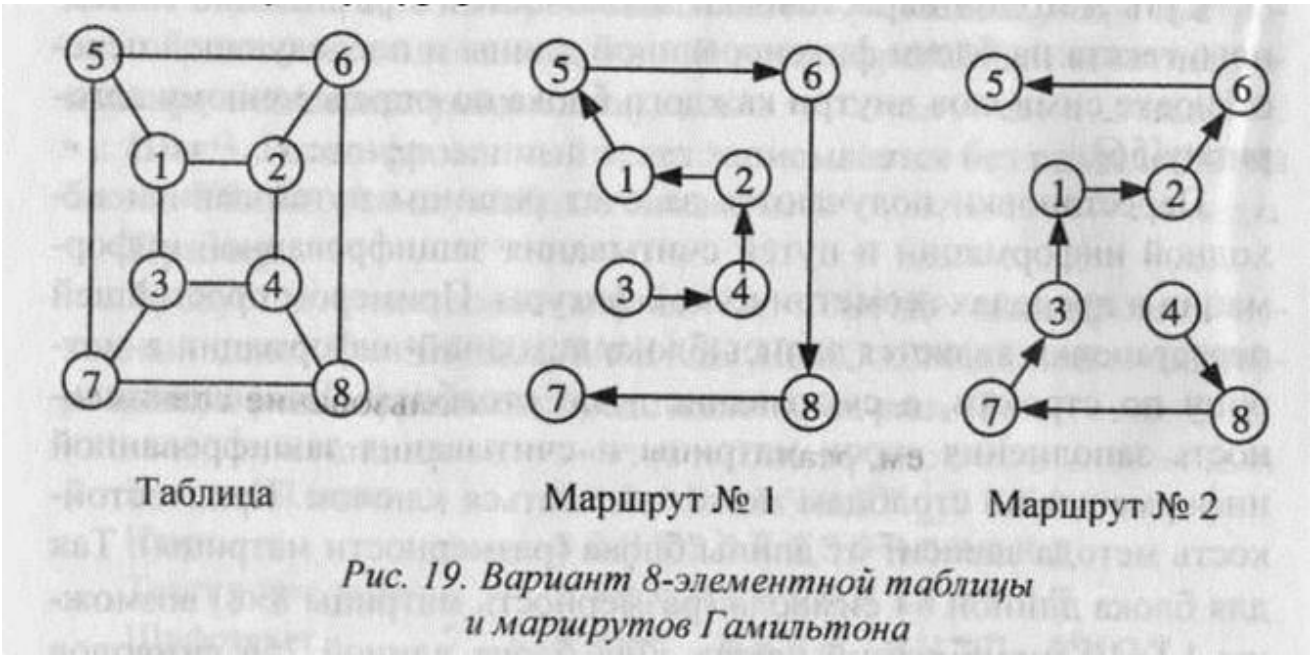

Рис. 19. Вариант 8-элементной таблицы и маршрутов Гамильтона

Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации с использованием маршрутов Гамильтона.

Пусть требуется зашифровать исходный текст To =

<МЕТОДЫЈІЕРЕСТАНОВКН>. Ключ и длина зашифрованных блоков соответственно равны: К=<2,1,1>, L=4. Для шифрования используются таблица и два маршрута, представленные на рис. 19. Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рис. 20.

Шаг 1. Исходный текст разбивается на три блока:

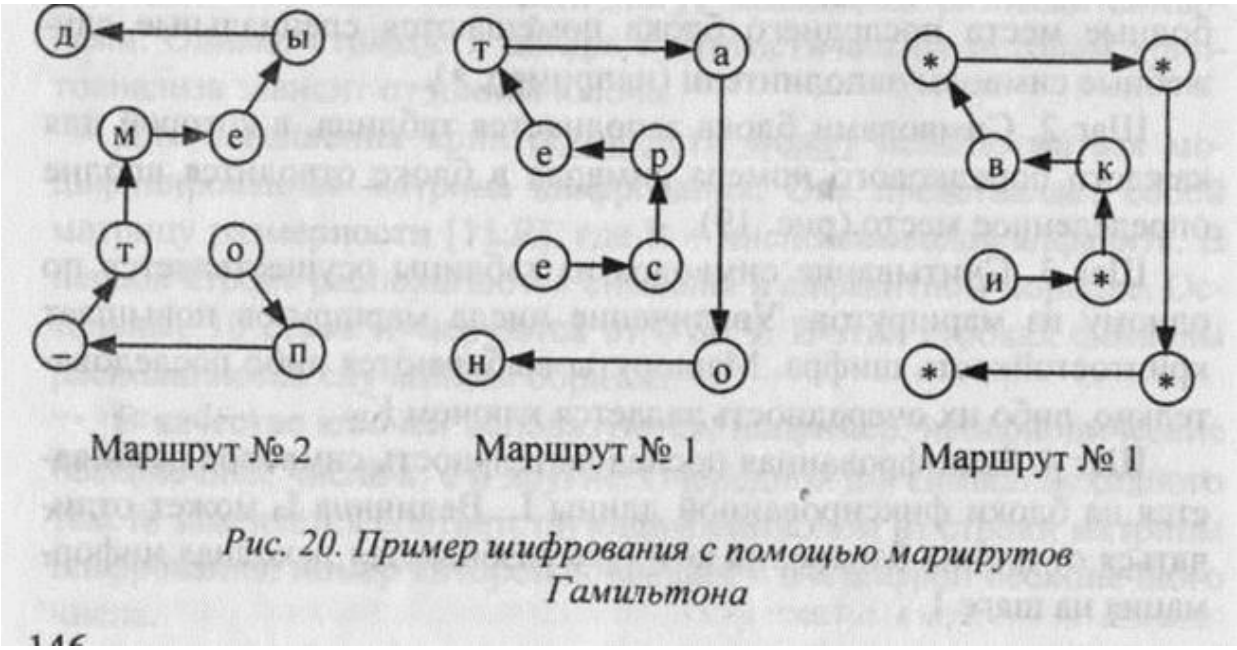

Рис. 20. Пример шифрования с помощью маршрутов Гамильтона

Б1 = <МЕТОДЫ_П>;

Б2 = <ЕРЕСТАНО>;

Б3 = <ВКИ*>.

Шаг 2. Заполняются три матрицы с маршрутами 2,1,1 (рис.20).

Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрутами.

Ti = <ОП_ТМЕЫДЕСРЕТАОНИ*КВ>.

Шаг 4. Разбиение на блоки шифртекста

Т! = <ОП_Т МЕЫД ЕСРЕ ТАОН И*КВ >.

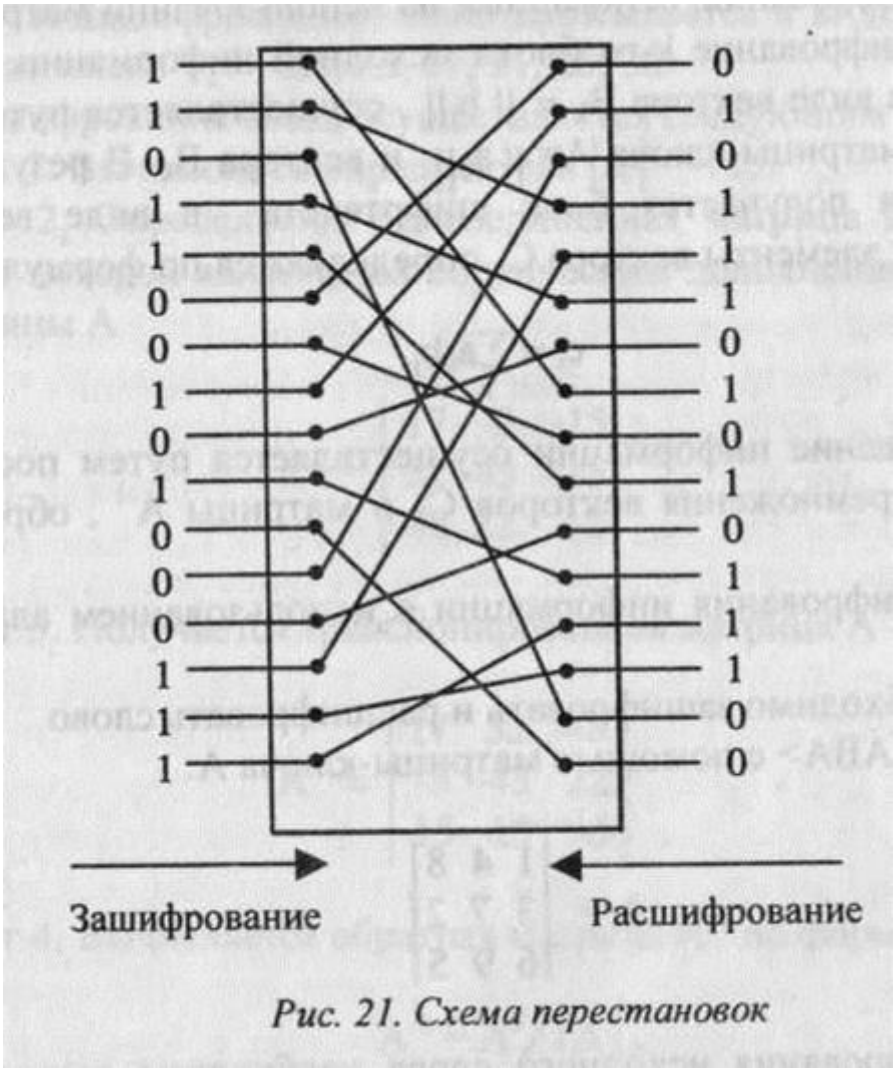

Рис. 21. Схема перестановок

В практике большое значение имеет использование специальных аппаратных схем, реализующих метод перестановок (рис. 21).

Параллельный двоичный код блока исходной информации (например, два байта) подаются на схему. За счет внутренней коммутации в схеме осуществляется перестановка бит в пределах блока. Для расшифрования блока информации входы и выходы схемы меняются местами [49]. Методы перестановок просто реализуются, но имеют два су-

щественных недостатка. Во-первых, они допускают раскрытие шифртекста при помощи статистической обработки. Во-вторых, если исходный текст разбивается на блоки длиной К символов, то криптоаналитику для раскрытия шифра достаточно направить в систему шифрования К-1 блок тестовой информации, в которых все символы за исключением одного одинаковы.

Аналитические методы шифрования

Для шифрования информации могут использоваться аналитические преобразования [8]. Наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры. Зашифрование k-го блока исходной информации, представленного в виде вектора Bk = || bj|| , осуществляется путем перемножения матрицы-ключа А= и гы| и вектора Вк. В результате перемножения получается блок шифртекста в виде вектора Ck= Iki

---

$$c_i = \sum_j a_{ij} b_j.$$

||, где элементы вектора Ск определяются по формуле:

Расшифрование информации осуществляется путем последовательного перемножения векторов Ск и матрицы А"1 , обратной матрице А.

Пример шифрования информации с использованием алгебры матриц.

Пусть необходимо зашифровать и расшифровать слово То = < ЗАБАВА> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

Для зашифрования исходного слова необходимо выполнить следующие шаги.

Шаг 1. Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слова Тэ:

$$T_э = <8, 1, 2, 1, 3, 1>.$$

Шаг 2. Умножение матрицы А на векторы В]={8, 1, 2} и В2={1,3, 1}:

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix};$$

Шаг 3. Зашифрованное слово записывается в виде

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix}$$

последовательности чисел T] = <28, 35, 67, 21, 26, 38>.

Расшифрование слова осуществляется следующим образом.

Шаг 1. Вычисляется определитель |A |=

-115.

Шаг 2. Определяется присоединенная матрица A*, каждый элемент которой является алгебраическим дополнением элемента ау матрицы

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

Шаг 3. Получается транспонированная матрица Ат

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

Шаг 4. Вычисляется обратная матрица A" по формуле:

$$A^{-1} = A^{T}/|A|.$$

В результате вычислений обратная матрица имеет вид:

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

Шаг 4. Определяются векторы B_1 и B_2:

$B_1 = A^{-1} \cdot C_1$; $B_2 = A^{-1} \cdot C_2$.

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix},$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}.$$

Шаг 5. Числовой эквивалент расшифрованного слова Тэ=<8, 1,2, 1,3, 1 > заменяется символами, в результате чего получается исходное слово То =

<ЗАБАВА>.

Аддитивные методы шифрования

Сущность аддитивных методов шифрования заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательностью кодов, которая соответствует некоторому кортежу символов [56]. Этот кортеж называется *гаммой.* Поэтому аддитивные методы шифрования называют также *гаммированием.*

Для данных методов шифрования ключом является гамма. Криптостойкость аддитивных методов зависит от длины ключа и равномерности его статистических характеристик. Если ключ короче, чем шифруемая последовательность символов, то шиф-ртекст может быть расшифрован криптоаналитиком статистическими методами исследования. Чем больше разница длин ключа и исходной информации, тем выше вероятность успешной атаки на шифртекст. Если ключ представляет собой непериодическую последовательность случайных чисел, длина которой превышает длину шифруемой информации, то без знания ключа расшифровать шифртекст практически невозможно. Как и для методов замены в качестве ключа могут использоваться неповторяющиеся последовательности цифр, например, в числах *п, е* и других.

На практике самыми эффективными и распространенными являются аддитивные методы, в основу которых положено использование *генераторов (датчиков) псевдослучайных чисел.* Генератор использует исходную информацию относительно малой длины для получения практически бесконечной последовательности псевдослучайных чисел.

Для получения последовательности псевдослучайных чисел (ПСЧ) могут использоваться конгруэнтные генераторы. Генераторы этого класса вырабатывают псевдослучайные последовательности чисел, для которых могут быть строго математически определены такие основные характеристики генераторов как перио- дичность и случайность выходных последовательностей.

Среди конгруэнтных генераторов ПСЧ выделяется своей простотой и эффективностью линейный генератор, вырабатывающий псевдослучайную последовательность чисел T(i) в соответствии с соотношением

T(i+l) = (a*T(i) + c)mod m,

где *a* и *c* - константы, T(0) - исходная величина, выбранная **в** качестве порождающего числа.

Период повторения такого датчика ПСЧ зависит от величин *a* и c. Значение *m* обычно принимается равным 2s, где s - длина слова ЭВМ в битах. Период повторения последовательности генерируемых чисел будет максимальным тогда и только тогда, когда *c* -нечетное число и *a* (mod 4) = 1 [39]: Такой генератор может быть сравнительно легко создан как аппаратными средствами, так и программно.

4. Системы шифрования с открытым ключом

Наряду с традиционным шифрованием на основе секретного ключа в последние годы все большее признание получают системы шифрования с открытым ключом. В таких системах используются два ключа. Информация шифруется с помощью открытого ключа, а расшифровывается с использованием секретного ключа.

В основе применения систем с открытым ключом лежит использование необратимых или односторонних функций [8]. Эти функции обладают следующим свойством. По известному *x* легко определяется функция *y* = f(x). Но по известному значению *y* практически невозможно получить *x.* В криптографии используются односторонние функции, имеющие так называемый потай-

ной ход. Эти функции с параметром z обладают следующими свойствами. Для определенного z могут быть найдены алгоритмы E*z* и *Dz.* С помощью E*z*, легко получить функцию fz (x) для всех *x* из области определения. Так же просто с помощью алгоритма Dz получается и обратная функция *x* - f'(y) для всех y из области допустимых значений. В то же время практически для всех z и почти для *всех y* из области допустимых значений нахождение f '(y) при помощи вычислений невозможно даже при известном Ez. В качестве открытого ключа используется *y,* а в качестве закрытого - *x.*

При шифровании с использованием открытого ключа нет необходимости в передаче секретного ключа между взаимодействующими субъектами, что существенно упрощает криптозащиту передаваемой информации.

Криптосистемы с открытыми ключами различаются видом односторонних функций. Среди них самыми известными являются системы RSA, Эль-Гамаля и Мак- Элиса. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом является алгоритм RSA, получивший свое название от первых букв фамилий его создателей: Rivest, Shamir и Adleman.

Алгоритм основан на использовании операции возведения в степень модульной арифметики. Его можно представить в виде следующей последовательности шагов [39].

Шаг 1. Выбираются два больших простых числа p и q. Простыми называются числа, которые делятся только на самих себя и на 1. Величина этих чисел должна быть больше 200. Шаг 2. Получается открытая компонента ключа *n:*

n=p-q. Шаг 3. Вычисляется функция Эйлера по формуле:

f(p,q) = (p-1)iq-1).

Функция Эйлера показывает количество целых положительных чисел от 1 до n, которые взаимно просты с *n.* Взаимно простыми являются такие числа, которые не имеют ни одного общего делителя, кроме 1.

Шаг 4. Выбирается большое простое число *d,* которое является взаимно простым со значением F*(p,q).*

Шаг 5. Определяется число *e,* удовлетворяющее условию: *ed =l(modf(p,q)).*

Данное условие означает, что остаток от деления (вычет) произведения *e-d* на функцию *f(p,q)* равен I. Число *e* принимается в качестве второй компоненты открытого ключа. В качестве секретного ключа используются числа *d u n.*

Шаг 6. Исходная информация, независимо от ее физической природы, представляется в числовом двоичном виде. Последовательность бит разделяется на блоки длиной L бит, где L - наименьшее целое число, удовлетворяющее условию: L>log2(n+1). Каждый блок рассматривается как целое положительное число X(i), принадлежащее интервалу [0,n-l]. Таким образом, исходная информация представляется последовательностью чисел X(i), i=l,I. Значение I определяется длиной шифруемой последовательности.

Шаг 7. Зашифрованная информация получается в виде последовательности чисел Y(i), вычисляемых по формуле:

X(i) = (Y(i))(mod n).

Шаг 8. Для расшифрования информации используется следующая зависимость:

X(i) = (Y(i))(mod n).

Пример применения метода RSA для криптографического закрытия информации. Примечание: для простоты вычислений использованы минимально возможные числа.

Пусть требуется зашифровать сообщение на русском языке «ГАЗ».

Для зашифрования и расшифрования сообщения необходимо выполнить следующие шаги.

Шаг 1. Выбирается *p = 3 u q= II.*

Шаг 2. Вычисляется *n* = 3*11=33. Шаг 3. Определяется функция Эйлера f(p.q) = (3-1)(11-1) = 2O.

Шаг 4. В качестве взаимно простого числа выбирается число

d=3.

Шаг 5. Выбирается такое число *e,* которое удовлетворяло бы соотношению: *(e- 3)* (mod 20) = 1. Пусть e = 7.

Шаг 6. Исходное сообщение представляется как последовательность целых чисел. Пусть букве А соответствует число 1. букве Г - число 4, букве З - число 9. Для представления чисел в двоичном коде требуется 6 двоичных разрядов, так как в русском алфавите используются 33 буквы (случайное совпадение с числом п).

Исходная информация в двоичном коде имеет вид: 000100 000001001001.

Длина блока L определяется как минимальное число из целых чисел, удовлетворяющих условию: L>log2(33+1), так как п=33. Отсюда L=6. Тогда исходный текст представляется в виде кортежа X(i) = <4, 1,9>.

Шаг 7. Кортеж X(i) зашифровывается с помощью открытого ключа {7, 33}: Y(l) = (47) (mod 33) = 16384 (mod 33) = 16; Y(2) = (17) (mod 33) = 1 (mod

33) = 1; Y(3) = (97) (mod 33) = 4782969 (mod 33) = 15. Получено

зашифрованное сообщение Y(i) = <16, 1, 15>.

Шаг 8. Расшифровка сообщения Y(i) = <16, 1, 15> осуществляется с помощью

секретного ключа {3, 33}: X(1) = (163) (mod 33) = 4096 (mod 33) я 4; X(2) = (I3)

(mod 33) = 1 (mod 33) = 1; X(3) = (153) (mod 33) = 3375 (mod 33) = 9.

Исходная числовая последовательность в расшифрованном виде X (i) = <4, 1, 9> заменяется исходным текстом «ГАЗ».

Система Элъ-Гамаля основана на сложности вычисления дискретных логарифмов в конечных полях [22]. Основным недостатком систем RSA и Эль- Гамаля является необходимость выполнения трудоемких операций в модульной арифметике, что требует привлечения значительных вычислительных ресурсов.

Криптосистема Мак-Элиса использует коды, исправляющие ошибки. Она реализуется в несколько раз быстрее, чем криптосистема RSA, но имеет и существенный недостаток. В криптосистеме *Мак-Элиса* используется ключ большой длины и получаемый шифртекст в два раза превышает длину исходного текста.

Для всех методов шифрования с открытым ключом математически строго не доказано отсутствие других методов криптоанализа кроме решения NP-полной задачи (задачи полного перебора). Если появятся методы эффективного решения таких задач, то криптосистемы такого типа будут дискредитированы. Например, ранее считалось, что задача укладки рюкзака является NP-полной. В настоящее время известен метод решения такой задачи, позволяющий избежать полного перебора.

5. Стандарты шифрования

Российский стандарт на шифрование информации ГОСТ 28147-89

В Российской Федерации установлен государственный стандарт (ГОСТ 28147—

89 [9]) на алгоритмы криптографического преобразования информации в ЭВМ, вычислительных комплексах и вычислительных сетях. Эти алгоритмы допускается использовать без ограничений для шифрования информации любого уровня

секретности. Алгоритмы могут быть реализованы аппаратными и программными способами.

Стандартом определены следующие алгоритмы криптографического преобразования информации:

- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.

Общим для всех алгоритмов шифрования является использование ключа размерностью 256 бит, разделенного на восемь 32-разрядных двоичных слов, и разделение исходной шифруемой двоичной последовательности на блоки по 64 бита.

Сущность алгоритма *простои замены* состоит в следующем. Блок из 64 - х бит исходной последовательности разбивается на два двоичных слова А и В по 32 разряда. Слово А образуют младшие биты, а слово В - старшие биты блока. Эти слова подвергаются итерационной обработке с числом итераций равным i=32. Слово, находящееся на месте младших бит блока, (А на первой итерации) суммируется по mod 232 с 32-разрядным словом ключа; разбивается на части по 4 бита в каждой (4-х разрядные входные векторы); с помощью специальных узлов замены каждый вектор заменятся на другой вектор (4 бита); полученные векторы объединяются в 32-разрядное слово, которое циклически сдвигается влево на 32 разряда и суммируется по mod 2 с другим 32-разрядным словом из 64-разрядного блока (слово В на первой итерации).

После выполнения первой итерации в блоке на месте младших бит будет расположено слово В, а слева преобразованное слово А. На следующих итерациях операции над словами повторяются.

$$j = \begin{cases} (i-1) \bmod 8, & \text{при } 1 \le i \le 24; \\ 32-i, & \text{при } i \ge 25; \\ 0, & \text{при } i=32. \end{cases}$$

На каждой итерации i 32-разрядное слово ключа j (всего их 8) выбирается по следующему правилу:

Блок замены состоит из 8 узлов замены, которые выбираются поочередно. Узел замены представляет собой таблицу из шестнадцати строк, в каждой из которых находятся векторы замены (4 бита). Входной вектор определяет адрес строки в таблице, число из которой является выходным вектором замены. Информация в таблицы замены заносится заранее и изменяется редко.

Алгоритм *гаммирования* предусматривает сложение по mod 2 исходной последовательности бит с последовательностью бит гаммы. Гамма получается в соответствии с алгоритмом простой замены. При выработке гаммы используются две специальные константы, заданные в ГОСТ 28147-89, а также 64-разрядная дво- ичная последовательность - синхропосылка. Расшифрование информации возможно только при наличии синхропосылки, которая не является секретной и может в открытом виде храниться в памяти ЭВМ или передаваться по каналам связи.

Алгоритм *гаммирования с обратной связью* очень схож с алгоритмом гаммирования. Они различаются лишь действиями на первом шаге итерационного процесса шифрования.

В ГОСТ 28147-89 определен алгоритм выработки *имито-вставки.* Она используется для защиты от навязывания ложной информации. Имитовставка является функцией преобразования исходной информации и секретного ключа. Она представляет собой двоичную последовательность длиной *к* бит. Значение параметра *к* выбирается с учетом вероятности навязывания ложной информации Рн, которая связана с параметром к соотношением:

P=1/2

Алгоритм выработки имитовставки может быть представлен следующей

последовательностью действий. Открытая информация разбивается на блоки T(i) (i

= 1, 2,...,m), где *m* определяется объемом шифруемой информации. Объем каждого блока - 64 би-

та. Первый блок T(1) подвергается преобразованию в соответствии с первыми 16-ю итерациями алгоритма простой замены. В качестве ключа используется ключ, по которому будет шифроваться исходная информация. Полученное 64-битовое двоичное слово суммируется по mod 2 со вторым блоком T(2). Результат суммирования подвергается тем же итерационным преобразованиям, что и блок T(1), а на завершающем этапе суммируется по mod 2 с третьим блоком T(3). Эти действия повторяются для m-*1* блоков исходной информации. Если последний блок T(m) не полный, то он дополняется соответствующим числом нулей до 64 разрядов. Этот блок суммируется по mod 2 с результатом, полученным при обработке T(m-1) блока, и подвергается преобразованию в соответствии с первыми 16-ю итерациями алгоритма простой замены. Из полученного 64-разрядного блока выделяется слово длиной к бит, которое и является имитовставкой.

Имитовставка помещается в конце зашифрованной информации. При получении (считывании) этой информации осуществляется ее расшифрование. По расшифрованной информации определяется имитовставка и сравнивается с полученной (считанной) имитовставкой. Если имитовставки не совпадают, то считается, что вся расшифрованная информация является ложной.

Стандарт США на шифрование информации

Государственным стандартом на шифрование информации является стандарт DES (Data Encryption Standard). Алгоритм шифрования, положенный в основу стандарта, был разработан фирмой IBM. После проверки специалистами Агентства Национальной Безопасности США алгоритм получил статус государственного стандарта. Стандарт DES используется федеральными департаментами для закрытия информации в автоматизированных системах, за исключением некоторых видов информации, определенных специальными актами. Кроме того, этот стандарт шифрования широко используется негосударственными организациями не только в США, но и во всем мире.

В стандарте DES исходная информация разбивается на блоки по 64 бита в каждом и подвергается криптографическому преобразованию с использованием ключа, длиной 56 или 64 бита [39]. Блоки исходной информации подвергаются итерационной обработке с использованием операций перестановки и функции шифрования. Для вычисления функции шифрования предусматривается получение 48-битового ключа из 64-битового, расширение 32-битового кода до 48-битового, преобразование 6-битового кода в 4-битовый и перестановка бит в 32-битовой последовательности [3].

Процесс расшифрования является инверсным по отношению к процессу шифрования и выполняется с использованием того же ключа, что и при шифровании.

6. Перспективы использования криптозащиты информации в КС

Криптостойкость рассмотренных методов шифрования определяется длиной ключа, которая для современных систем должна быть, по крайней мере, больше 90 бит.

Для особо ответственных применений секретным является не только ключ, но и алгоритм шифрования. Для повышения крипто-стойкости шифров могут использоваться несколько ключей (обычно три ключа). Зашифрованная с помощью первого ключа информация подвергается шифрованию с помощью второго ключа и т. д.

Предлагается использовать переменные алгоритмы шифрования. В этом случае ключ шифрования используется еще и для выбора конкретного алгоритма

шифрования. Развитие этого направления шифрования сдерживает сложность строгого доказательства криптостойкости такого шифрования.

Привлекательность методов шифрования с использованием открытых ключей заключается, прежде всего, в отсутствии необходимости рассылки секретных ключей. Для распределенных на больших расстояниях объектов КС рассылка секретных ключей становится довольно сложной и трудоемкой задачей. Распространение систем с открытыми ключами сдерживается отсутствием доказательств невозможности получения секретных ключей, кроме как путем их полного перебора.

Перспективным направлением развития криптозащиты информации является стеганография. Комплексное использовании стеганографии и шифрования намного повышает криптостойкость закрытой информации.