Криптографические методы защиты информации

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.

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.


Методы криптографического преобразования информации
Шифрование
Стеганография
Кодирование
Сжатие

Шифрова́ние — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

С помощью шифрования обеспечиваются три состояния безопасности информации:

Конфиденциальность.

Шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.

Целостность.

Шифрование используется для предотвращения изменения информации при передаче или хранении.

Идентифицируемость.

Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Для того, чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию.

Кодирование информации — процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки.

Сетевое кодирование — раздел теории информации, изучающий вопрос оптимизации передачи данных по сети с использованием техник изменения пакетов данных на промежуточных узлах.

Энтропийное кодирование — кодирование последовательности значений с возможностью однозначного восстановления с целью уменьшения объёма данных (длины последовательности) с помощью усреднения вероятностей появления элементов в закодированной последовательности.

Дельта-кодирование — способ представления данных в виде разницы (дельты) между последовательными данными вместо самих данных.

Кодирование (программирование) — процесс написания программного кода, скриптов, с целью реализации определённого алгоритма на определённом языке программирования.

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 шифрованию, и ключ шифрования.

Ключ содержит управляющую информацию, 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 позволяют скрыть** не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

Стеганогра́фия (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо. Стеганографию обычно используют совместно с методами криптографии.

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. Комплексное 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 шифрованию.

Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

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 Шифрование, 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 шифрования/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 технологию 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 рисунке.


Методы шифрования
По типу ключей
С симметричным ключом
С несимметричным ключом
По способу преобразования
Методы замены
Методы перестановки
Аналитические методы
Аддитивные методы
Комбинированные методы

Симметри́чные криптосисте́мы (также симметричное шифрование, симметричные шифры) (англ. symmetric-key algorithm) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME.

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.

Самым простым является *метод прямой замены.*

Символам So; исходного алфавита Ao, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы Su шифрующего алфавита Aь.

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 Lot, путем замены каждого символа s^ e To (i=l,K), представленного в исходном алфавите Ao размера [lxR], на число hoi(soi), соответствующее порядковому номеру символа soi в алфавите Ao.

Шаг 2. Формирование числового кортежа Lih путем замены каждого числа кортежа Loh на соответствующее число hn кортежа Lih.

Шаг 3. Получение шифртекста Ti путем замены каждого числа hi,(si,) кортежа Lih соответствующим символом Si, где Ti (i=l,K) алфавита шифрования Ai размера [1XR].

Шаг 4. Полученный шифртекст разбивается на блоки фиксированной длины Ь.

Если последний блок оказывается неполным, то в конец блока помещаются специальные символы- например, символ *).

Пример. Исходными данными для шифрования являются:

T0 = <МЕТОД_ШИФРОВАНИЯ>;

A0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩ

ЪЫЬЭЮЯ >;

A_1 = <О Р Щ Ь Я Т Э _ Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю >;

R=32; k_1=3; k_2=15, b=4.

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг 1. L_{0h} = <12,6,18,14,5,32,24,9,20,16,14,3,1,13,9,31>.

Шаг 2. L_{1h} = <19,1,5,25,30,15,23,10,11,31,25,24,18,22,10,12>.

Шаг 3. T_1 = <С О Я Г Б Д И М Ч У Г Ц К П М Х >.

Шаг 4. T_2 = <С О Я Г Б Д И М Ч У Г Ц К П М Х >.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифртекст T_1 длиной К символов. Расшифрование осуществляется путем решения целочисленного уравнения:

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 So, таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки si,, находящегося в том же столбце i таблицы.

Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке Sn.

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 перехваченных 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 s11 из алфавита Aь.
S02 заменяется символом S22 из алфавита Аг и так далее.
После замены SON СИМВОЛОМ S MM ИЗ AN СИМВОЛ SO(N+D замещается символом Si(N+i) 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].

Тв=
АБВГД……..ЪЭЮЯ_
ВВГДЕ ……..ЭЮЯ_А
ВГДЕЖ……. ЮЯ_АБ
_АБВГ …….ЫЪЭЮЯ

Матрица Вижинера

Шифрование осуществляется с помощью ключа, состоящего из M 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

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
ЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГДЕЖ
ОПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГДЕЖЗИКЛМН
НОПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГДЕЖЗИКЛМ
ДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГ

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=(Ьу) размерностью [(М+1),R] для выбранного ключа К.

Шаг 3. Под каждым символом s^ исходного текста длиной I символов размещается символ ключа km. 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 замещаемому символу sor;

2) находится строка i в Тш, для которой выполняется условие кт=Ьп;

3) определяется столбец j, для которого выполняется условие;

4) символ sor замещается символом Ь^.

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 Sjr из шифртекста и соответствующие символы ключа km. В матрице Тш определяется строка i, для которой выполняется условие km= Ь;1. В строке i определяется элемент by= Sir. 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>.

Пример шифрования с помощью матрицы Вижинера

Механизмы зашифрования и расшифрования представлены на рисунке.

Исходный текст БЕЗ0БЛАЧН0Е_НЕБ0

Ключ ЗОНДЗОНДЗОНДЗОНД

Текст после замены ИУФТИШНЫФЫТГФУОТ

Шифртекст ИУФТ ИШНЫ ФЫТГ ФУОТ

Ключ ЗОНД ЗОНД ЗОНД ЗОНД

Расшифрованный текст БЕЗО БЛАЧ НОЕ_ НЕБО

Исходный текст БЕЗ0БЛАЧН0Е_НЕБ0

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,* e и другие. Очередной n-й символ исходного текста заменяется соответствующим символом из строки матрицы шифрования, номер которой совпадает с n-й цифрой бесконечного числа.

Методы перестановки

Суть методов перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановке символов внутри каждого блока по определенному алгоритму.

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.

Последовательность 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 1,6x10>9 комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16x16) число возможных ключей достигает 1,4x10>26.

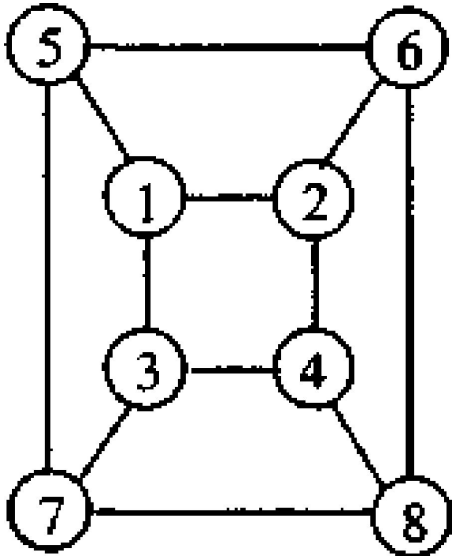
Перестановки используются также в методе, основанном на применении *маршрутов Гамильтона.*
Этот метод реализуется путем выполнения следующих шагов.

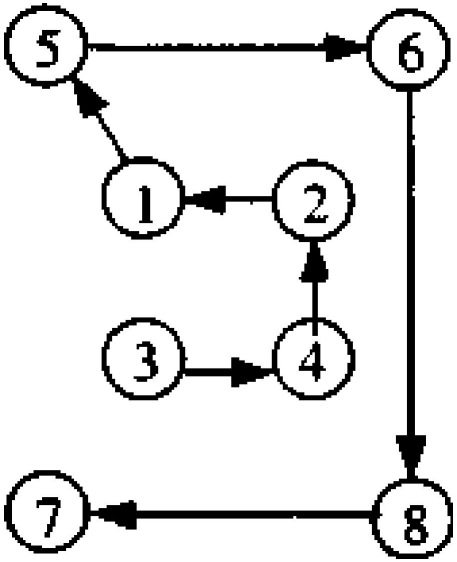
Шаг 1. Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например, *).

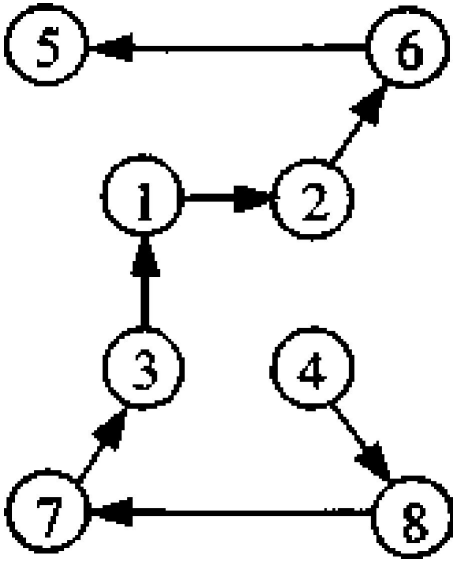
Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (следующий слайд).

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.


5
6
1
2
3
4
7
8


5
6
1
2
3
4
7
8


5
6
1
2
3
4
7
8

Расшифрование производится в обратном порядке.

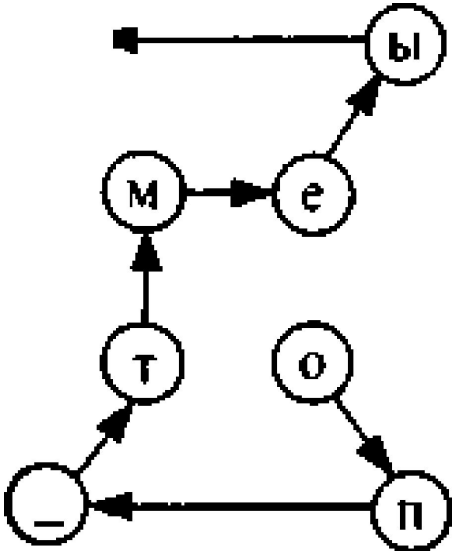
В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

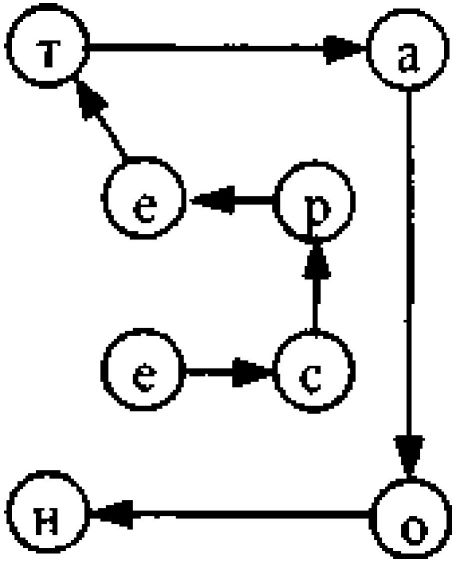
Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации с использованием маршрутов Гамильтона.

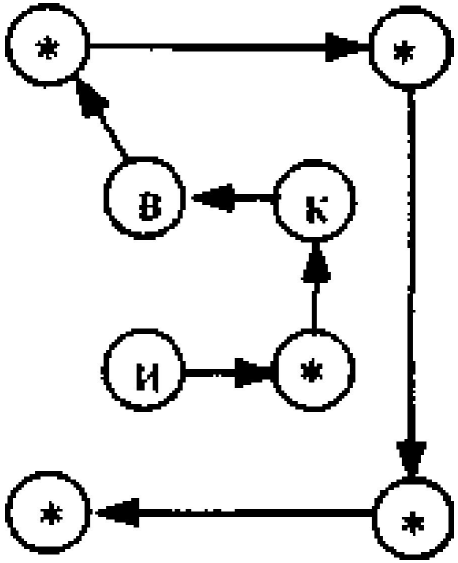
Пусть требуется зашифровать исходный текст To = <МЕТОДЫ_ПЕРЕСТАНОВКИ>. Ключ и длина зашифрованных блоков соответственно равны: K=<2,1.1>, L=4.

Для шифрования используются таблица и два маршрута, представленные на
выше.

Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рисунке.


ы
м
е
т
о
_
п


т
а
е
р
е
с
н
о


*
*
в
к
и
*
*
*

Шаг 1. Исходный текст разбивается на три блока:

Б1 =<МЕТОДЫ_П>;

Б2 = <ЕРЕСТАНО>;

БЗ = <ВКИ*****>.

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

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

Tj = <ОП_ТМЕЫДЕСРЕТАОНИ*КВ****>.

Шаг 4. Разбиение на блоки шифртекста

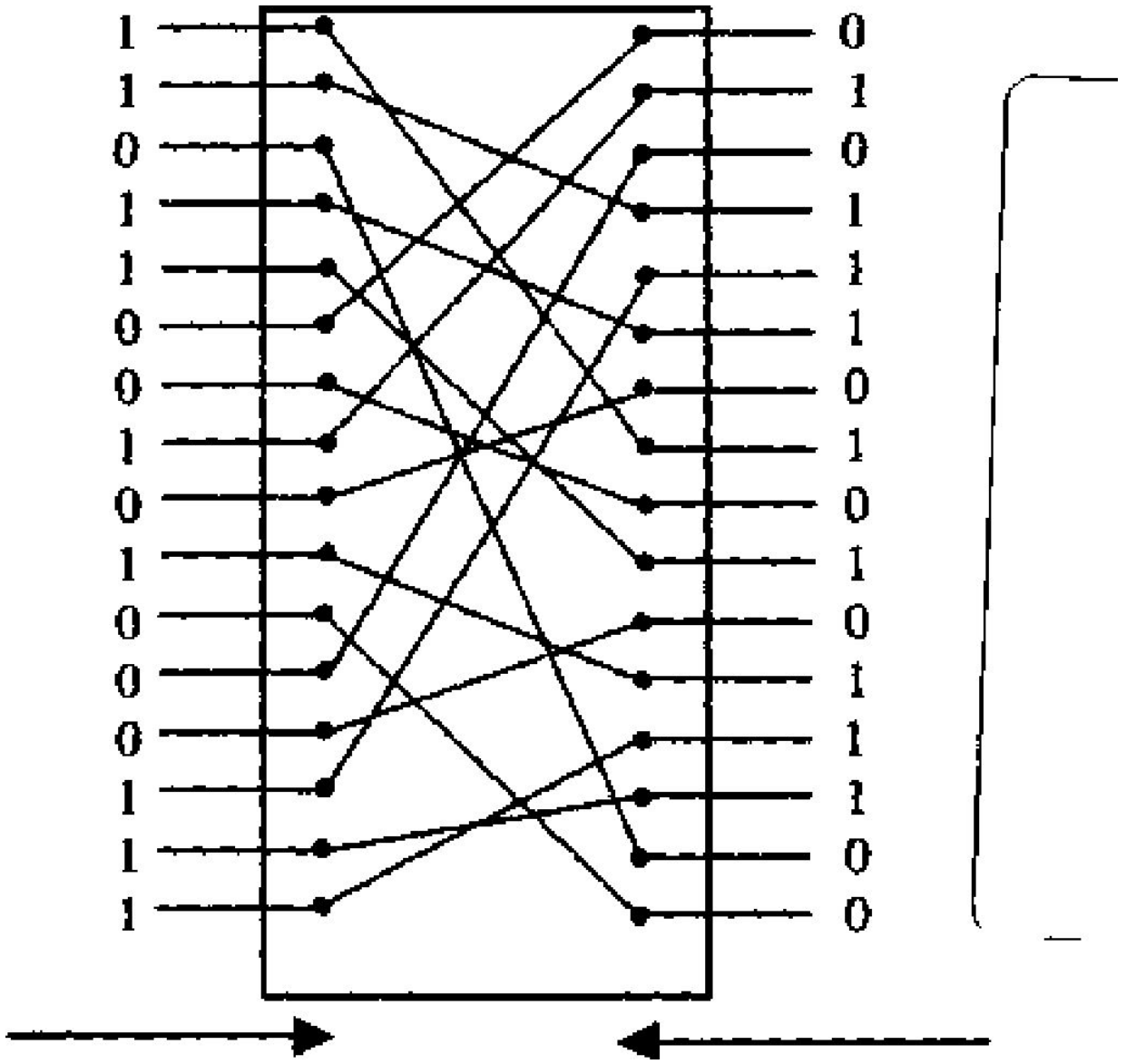
Т, = <ОП_Т МЕЫД ЕСРЕ ТАОН И*КВ ****>.

В практике большое значение имеет использование специальных аппаратных схем, реализующих метод перестановок.

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.

Методы перестановок просто реализуются, но имеют два существенных 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.


1
1
0
1
1
0
0
1
0
1
0
0
0
1
1
1
0
1
1
0
1
1
0
0
0
1
1
0
0
1
1
1
0
0

Аналитические методы шифрования

Для шифрования информации могут использоваться аналитические преобразования.
Наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры.

Зашифрование k-го блока исходной информации, представленного в виде вектора B^ = || bj|| , осуществляется путем перемножения матрицы-ключа A=|| Ai || и вектора Bj. В результате перемножения получается блок шифртекста в виде вектора Ck= ||ks | | , где элементы вектора Ск определяются по формуле:

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

Расшифрование информации осуществляется путем последовательного перемножения векторов C^ и матрицы A"1 , обратной матрице A.

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.

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 шифртекст 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

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 периодичность 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

$$T(i+1) = (a \cdot T(i) + c) \bmod m,$$

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 $a \pmod 4 = 1$ [Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь; МП ≪Веста≫, 1992. - 192 с.].

Такой генератор может быть сравнительно легко создан как аппаратными средствами, так и программными.

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 [Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2 кн. М.: Энергоатомиздат, 1994.].
Эти функции обладают следующим свойством. По известному x легко определяется функция $y = f(x)$. Но по известному значению y практически невозможно получить x.
При шифровании с использованием открытого ключа нет необходимости в передаче секретного ключа между взаимодействующими субъектами, что существенно упрощает криптозащиту передаваемой информации.