ГАПОУ СО «Асбестовский политехникум»

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

дисциплина
«Информационная безопасность

для студентов специальности
09.02.03
Программирование в компьютерных системах

2017 г.

«Криптографические методы защиты информации» - это раздел дисциплины «Информационная безопасность». Эту дисциплину изучают студенты специальности 09.02.03 «Программирование в компьютерных системах».

В учебном пособии приведены материалы, связанные с криптографическими методами защиты информации в автоматизированных системах обработки данных, в персональных компьютерах и в сетях ЭВМ.

С простейшими методами шифрования текста студенты познакомились при изучении дисциплин «Информатика» и «Дискретная математика».

Особое внимание в учебном пособии уделено не только методам криптографического преобразования данных, но и проблемам реализации методов криптографической защиты в АСОД. Представлены материалы и по истории развития криптографии. Шифрование текста используется человечеством с того самого момента, как появилась первая секретная информация. Существует много разных систем шифрования текста. С некоторыми из них студенты познакомятся в учебном пособии. В практической части пособия предложены задания для самостоятельной работы.

Дальнейшее изучение криптографических методов защиты информации даст возможность студентам реализовать любой метод шифрования информации через программные средства.

Разработала Савина О.Н. – преподаватель Асбестовского политехникума

СОДЕРЖАНИЕ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ.....2

КРИПТОЛОГИЯ И ОСНОВНЫЕ ЭТАПЫ ЕЕ РАЗВИТИЯ.....2

МЕТОДЫ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ.....6

ШИФРОВАНИЕ.....9

КОДИРОВАНИЕ.....14

ПРОБЛЕМЫ РЕАЛИЗАЦИИ МЕТОДОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В АСОД (АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ).....21

ТЕХНИЧЕСКИЕ СРЕДСТВА КРИПТОГРАФИИ.....22

ПРОГРАММНЫЕ СРЕДСТВА.....23

ПРОБЛЕМА УПРАВЛЕНИЯ КЛЮЧАМИ.....23

ХАРАКТЕРИСТИКИ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ.....25

ПРАКТИЧЕСКАЯ ЧАСТЬ.....29

КОНТРОЛЬНЫЕ ВОПРОСЫ.....35

Литература.....36

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии — ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Криптографическое закрытие является специфическим способом защиты информации, оно имеет многовековую историю развития и применения. Поэтому у специалистов не возникало сомнений в том, что эти средства могут эффективно использоваться также и для защиты информации в АСОД, вследствие этого им уделялось и продолжает уделяться большое внимание. Достаточно сказать, что в США еще в 1978 г. утвержден и рекомендован для широкого применения национальный стандарт (DES) криптографического закрытия информации. Подобный стандарт в 1989 г. (ГОСТ 28147—89) утвержден и у нас в стране. Интенсивно ведутся исследования с целью разработки высокостойких и гибких методов криптографического закрытия информации. Более того, сформировалось самостоятельное научное направление — криптология, изучающая и разрабатывающая научно-методологические основы, способы, методы и средства криптографического преобразования информации.

КРИПТОЛОГИЯ И ОСНОВНЫЕ ЭТАПЫ ЕЕ РАЗВИТИЯ

Можно выделить следующие три периода развития криптологии.

Первый период — эра донаучной криптологии, являвшейся ремеслом — уделом узкого круга искусных умельцев. Началом второго периода можно считать 1949 г., когда появилась работа К. Шеннона «Теория связи в секретных системах», в которой проведено фундаментальное научное исследование шифров и важнейших вопросов их стойкости. Благодаря этому труду криптология оформилась как прикладная математическая дисциплина. И наконец, начало третьему периоду было положено появлением в 1976 г. работы У. Диффи, М. Хеллмана «Новые направления в криптографии», в которой было показано, что секретная связь возможна без предварительной передачи секретного ключа. Так началось и продолжается до настоящего времени развитие наряду с обычной классической криптографией и криптографии с открытым ключом.

Еще несколько веков назад само применение письменности можно было рассматривать как способ закрытия информации, так как владение письменностью было уделом немногих.

XX в. до н. э. При раскопках в Месопотамии был найден один из самых древних шифротекстов. Он был написан клинописью на глиняной табличке и содержал рецепт глазури для покрытия гончарных изделий, что, по-видимому, было коммерческой тайной. Известны древнеегипетские религиозные тексты и медицинские рецепты.

Середина IX в. до н. э. Именно в это время, как сообщает Плутарх, использовалось шифрующее устройство — скиталь, которое реализовывало так называемый шифр перестановки. При шифровании слова писались на узкую ленту, намотанную на цилиндр, вдоль образующей этого цилиндра (скиталя). После этого лента разматывалась и на ней оставались переставленные буквы открытого текста. Неизвестным параметром-ключом в данном случае служил диаметр этого цилиндра. Известен и метод дешифрования такого шифротекста, предложенный Аристотелем, который наматывал ленту на конус, и то место, где появлялось читаемое слово или его часть, определяло неизвестный диаметр цилиндра.

56 г. н. э. Во время войны с галлами Ю. Цезарь использует другую разновидность шифра — шифр замены. Под алфавитом открытого текста писался тот же алфавит со сдвигом (у Цезаря на три позиции) по циклу. При шифровании буквы открытого текста у верхнего алфавита заменялись на буквы нижнего алфавита. Хотя этот шифр был известен до Ю. Цезаря, тем не менее он был назван его именем.

Другим более сложным шифром замены является греческий шифр — квадрат Полибия. Алфавит записывается в виде квадратной таблицы. При шифровании буквы открытого текста заменялись на пару чисел — номера столбца и строки этой буквы в таблице. При произвольном расписывании алфавита по таблице и шифровании такой таблицей короткого сообщения этот шифр является стойким даже по современным понятиям. Идея была реализована в более сложных шифрах, применявшихся во время Первой мировой войны.

Крах Римской империи в V в. н. э. сопровождался закатом искусства и наук, в том числе и криптографии. Церковь в те времена преследовала тайнопись, которую она считала чернокнижием и колдовством. Сокрытие мыслей за шифрами не позволяло церкви контролировать эти мысли.

Р. Бэкон (1214—1294) — францисканский монах и философ — описал семь систем секретного письма. Большинство шифров в те времена применялись для закрытия научных записей.

Вторая половина XV в. Леон Баттиста Альберта, архитектор и математик, работал в Ватикане, автор книги о шифрах, где описал шифр замены на основе двух концентрических кругов, по периферии которых были нанесены на одном круге — алфавит открытого текста, а на другом — алфавит шифротекста. Важно, что шифроалфавит был непоследовательным и мог быть смещен на любое количество шагов. Именно Альберта впервые применил для дешифрования свойство неравномерности встречаемости различных букв в языке. Он впервые также предложил для повышения стойкости применять повторное шифрование с помощью разных шифросистем.

Известен факт, когда король Франции Франциск I в 1546 г. издал указ, запрещающий подданным использование шифров. Хотя шифры того времени были исключительно простыми, они считались нераскрываемыми.

Иоганн Тритемий (1462—1516) — монах-бенедиктинец, живший в Германии. Написал один из первых учебников по криптографии. Предложил оригинальный шифр многозначной замены под названием «Ave Maria». Каждая буква открытого текста имела не одну замену, а несколько, по выбору шифровальщика. Причем буквы заменялись буквами или словами так, что полу-

чался некоторый псевдооткрытый текст, тем самым скрывался сам факт передачи секретного сообщения. Разновидность шифра многозначной замены применяется до сих пор, например в архиваторе ARJ.

Джироламо Кардано (1506—1576) — итальянский математик, механик, врач — изобрел систему шифрования, так называемую решетку Кардано, на основе которой, например, был создан один из наиболее стойких военно-морских шифров Великобритании во время Второй мировой войны. В куске картона с размеченной решеткой определенным образом прорезались отверстия, нумерованные в произвольном порядке. Чтобы получить шифротекст, нужно положить этот кусок картона на бумагу и начинать вписывать в отверстия буквы в выбранном порядке. Затем после поворота решетки на 90° процедура повторялась. Скрытие легко достигается, если эти промежутки достаточно велики, а слова языка имеют небольшую длину, как, например, в английском языке. Решетка Кардано — это пример шифра перестановки.

XVI в. Шифры замены получили развитие в работах итальянца Джованни Батиста Порты (математик) и француза Блеза де Вижинера (дипломат). Система Вижинера в том или ином виде используется до настоящего времени.

XVII в. Кардинал Ришелье (министр при короле Франции Людовике XIII) создал первую в мире шифрслужбу.

Лорд Френсис Бэкон (1562—1626) был первым, кто обозначил буквы 5-значным двоичным кодом: A = 00001, B = 00010, ... и т. д. Правда, Бэкон никак не обрабатывал этот код, поэтому такое закрытие было совсем нестойким. Просто интересно, что через три века этот принцип был положен в основу электрической и электронной связи. Тут уместно вспомнить коды Морзе, Бодо, международный телеграфный код № 2 (МККТТ-2), код ASCII, также представляющие собой простую замену.

В XVII же веке были изобретены так называемые словарные шифры. При шифровании буквы открытого текста обозначались двумя числами — номером строки и номером буквы в строке на определенной странице какой-нибудь выбранной распространенной книги. Эта система является довольно стойкой, но неудобной. К тому же книга может попасть в руки противника.

К. Гаусс (1777—1855) — великий математик, тоже не обошел своим вниманием криптологию. Он создал шифр, который ошибочно считал нераскрываемым. При его создании использовался интересный прием — рандомизация (от random — случайный) открытого текста. Открытый текст можно преобразовать в другой текст, содержащий символы большего алфавита, путем замены часто встречающихся букв случайными символами из соответствующих определенных им групп. В получающемся тексте все символы большого алфавита встречаются с примерно одинаковой частотой. Зашифрованный таким образом текст противостоит методам раскрытия на основе анализа частот появления отдельных символов. После расшифровывания законный получатель легко снимает рандомизацию. Такие шифры называют «шифрами с многократной подстановкой» или «равночастотными шифрами». Ниже будет приведен пример такого шифра.

Как известно, до недавнего времени криптографические средства использовались преимущественно для сохранения государственной тайны, поэтому сами средства разрабатывались специальными органами, причем

использовались криптосистемы очень высокой стойкости, что, естественно, сопряжено было с большими затратами. Однако, поскольку сфера защиты информации в настоящее время резко расширяется, становится весьма целесообразным системный анализ криптографических средств с учетом возможности и целесообразности их широкого применения для сохранения различных видов секретов и в различных условиях. Кроме того, в последние годы интенсивно разрабатываются новые способы криптографического преобразования данных, которые могут найти белее широкое по сравнению с традиционным применение.

Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод предупреждения несанкционированного доступа к информации имеет многовековую историю. В настоящее время разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющее число этих методов может быть успешно использовано и для закрытия информации.

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Internet, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически нераскрываемыми.

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

Криптография занимается поиском и исследованием математических методов преобразования информации.

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

Современная криптография включает в себя четыре крупных раздела:

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

Основные направления использования криптографических методов — передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод предупреждения несанкционированного доступа к информации имеет многовековую историю. В настоящее время разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющее число этих методов может быть успешно использовано и для закрытия информации.

МЕТОДЫ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ

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

Перечислим вначале некоторые основные понятия и определения.

Алфавит — конечное множество используемых для кодирования информации знаков.

Текст — упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных ИС, можно привести следующие:

- алфавит Z_{33} — 32 буквы русского алфавита и пробел;
- алфавит Z_{256} — символы, /входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит — $Z_2 = \{0,1\}$;
- восьмеричный или шестнадцатеричный алфавит. Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство Т преобразований открытого текста. Члены этого семейства индексируются или обозначаются символом к; параметр к является ключом.

Пространство ключей К — это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита

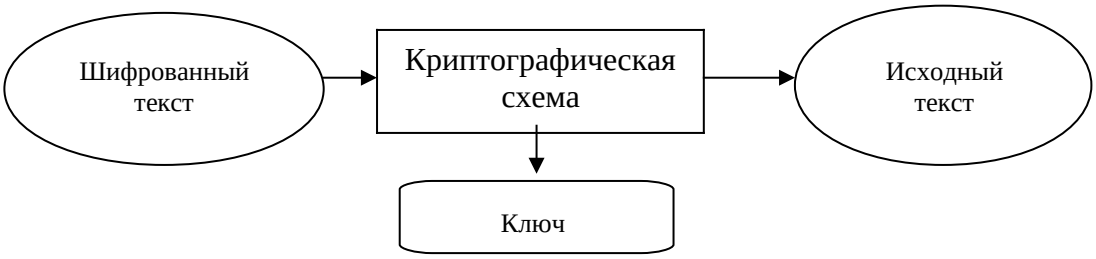

Рисунок 1 – процедура шифрования файлов

Криптосистемы разделяются на симметричные и с открытым ключом.

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины «распределение ключей» и «управление ключами» относятся к процессам системы обработки информации, содержанием которых являются составление и распределение ключей между пользователями.

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

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

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

Преобразование $T_к$ определяется соответствующим алгоритмом и значением параметра к. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т. д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должноиметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых Зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Классификацию методов криптографического закрытия

1. **Шифрование**
   1.1. Замена (подстановка)
   - простая (одноалфавитная);
   - многоалфавитная одноконтурная обыкновенная;
   - многоалфавитная одноконтурная монофоническая;
   - многоалфавитная многоконтурная.

   1.2. Перестановка
   - простая;
   - усложненная по таблице;
   - усложненная по маршрутам.

   1.3. Аналитическое преобразование
   - с использованием алгебры матриц;
   - по особым зависимостям;

   1.4. Гаммирование
   - с конечной короткой гаммой;
   - с конечной длинной гаммой;
   - с бесконечной гаммой.

   1.5. Комбинированные методы
   - замена и перестановка;
   - замена и гаммирование;
   - перестановка и гаммирование;
   - гаммирование и гаммирование;
2. **Кодирование**
   2.1. Смысловое
   - по специальным таблицам (словарям);
   - символьное;
   - по кодовому алфавиту.
3. **Другие виды**
   - рассечение-разнесение;
   - смысловое;
   - механическое;
   - сжатие-расширение.

Под шифрованием понимается такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения. Все известные способы шифрования можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование,

гаммирование и комбинированное шифрование. Каждый из этих способов может иметь несколько разновидностей.

Под кодированием понимается такой вид криптографического закрытия, при котором некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т. п.). Этот метод имеет две разновидности: смысловое и символьное кодирование. При смысловом кодировании кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений). При символьном кодировании кодируется каждый символ защищаемого сообщения. Символьное кодирование по существу совпадает с шифрованием заменой.

ШИФРОВАНИЕ

Шифрование заменой (подстановка). В этом наиболее простом методе символы шифруемого текста заменяются другими символами, взятыми из одного (одно- или моноалфавитная подстановка) или нескольких (много- или полиалфавитная подстановка) алфавитов.

Самой простой разновидностью является прямая (простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого или некоторого другого алфавита. Для этого составляется таблица замены и по ней происходит шифрование текста

Однако такой шифр имеет низкую стойкость, так как зашифрованный текст имеет те же статистические характеристики, что и исходный. Текст содержит символы с определёнными частотами появления.

При большом объеме зашифрованного текста частоты появления букв до шифрования и после шифрования будут совпадать и расшифровка будет упрощена. Поэтому простую замену используют редко и лишь в тех случаях, когда шифруемый текст короток.

Для повышения стойкости шифра используют ***полиалфавитные подстановки,*** в которых для замены символов исходного текста используются символы нескольких алфавитов. Известно несколько разновидностей полиалфавитной подстановки. Наиболее известными, из которых являются одно- (обыкновенная и монофоническая) и многоконтурная.

При полиалфавитной одноконтурной обыкновенной подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется последовательно и циклически, т. е. первый символ заменяется соответствующим символом первого алфавита, второй — символом второго алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.

Схема шифрования Вижинера. Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита. На рисунке 2 показана таблица Вижинера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе. Пример такой рабочей матрицы для ключа СТОЛ приведен на рисунке 2.

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**	**ъ**	**э**	**ю**	**я**
с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	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	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к

Рисунок 2 – Таблица Вижинера

Процесс шифрования выглядит следующим образом:

1) под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз;
2) каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа;
3) полученный текст может разбиваться на группы по несколько знаков.

Нетрудно видеть, что процедуры как прямого, так и обратного преобразований являются строго формальными, что позволяет реализовать их алгоритмически. Более того, обе процедуры легко реализуются по одному и тому же алгоритму.

Одним из недостатков шифрования по таблице Вижинера является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключ с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющую смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Вижинера. Приведем некоторые из них:

1) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке;
2) в качестве ключа используются случайные последовательности чисел.
3) из таблицы Вижинера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10. Эти строки используются в соответствии с чередованием цифр в выбранном ключе. Известны и другие модификации метода.

Монофоническая замена. Частным случаем рассмотренной полиалфавитной замены является так называемая монофоническая замена. Особенность этого метода состоит в том, что количество и состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется

криптоанализ зашифрованного текста с помощью его статистической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается использование большего числа заменяющих элементов, чем для редко встречающихся.

Полиалфавитная многоконтурная замена заключается в том, что для шифрования используется циклически несколько наборов (контуров) алфавитов, причем каждый контур в общем случае имеет свой индивидуальный период применения. Этот период исчисляется, как правило, количеством знаков, после зашифровки которых меняется контур алфавитов. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Если в полиалфавитной подстановке $n > m$ (где m — число знаков шифруемого текста) и любая последовательность (w_1, w_2, ... w_n) используется только один раз, то такой шифр является теоретически нераскрываемым, если, конечно, злоумышленник не имеет доступа к исходному тексту. Такой шифр получил название шифра Вермэна.

Шифрование методом перестановки. Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые наиболее часто встречающиеся разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ.

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке возникнут серьезные проблемы.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).

После этого вертикальные столбцы по порядку писали и строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Потом разбить строки на пятерки букв:

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ

Если строки укоротить, а количество строк увеличить, то получится прямоугольник-решетка, в который можно записывать исходный текст. Но тут

уже требуются предварительные договоренности между адресатом и отправителем посланий, поскольку сама решетка может быть различной длины-высоты, записывать в нее можно по строкам, по столбцам, по спирали туда или по спирали обратно, можно писать и по диагоналям, а для шифрования можно брать тоже различные направления. В общем, здесь масса вариантов.

Из рассмотренных примеров очевидно, что все процедуры шифрования и расшифровки по методу перестановок являются в достаточной степени формальными и могут быть реализованы алгоритмически.

Шифрование методом гаммирования. Суть этого метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название гаммирование.

Процедуру наложения гаммы на исходный текст можно осуществить двумя способами.

При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю к, где к — число символов в алфавите, т. е.

$$R_i = (s_i + G) \bmod (k - 1)$$

где R_i, S_i, G — символы соответственно зашифрованного, исходного текста и гаммы.

При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю два. Вместо сложения по модулю два при гаммировании можно использовать и другие логические операции, например преобразование по правилу логической эквивалентности или логической неэквивалентности.

Такая замена равносильна введению еще одного ключа, которым является выбор правила формирования символов зашифрованного сообщения из символов исходного текста и гаммы.

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы — длительностью периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода.

Обычно разделяют две разновидности гаммирования — с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При этом, если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким, т. е. его нельзя вскрыть с помощью статистической обработки зашифрованного текста. Это, однако, не означает, что дешифрование такого текста вообще невозможно: при наличии некоторой дополнительной информации исходный текст может быть частично или полностью восстановлен даже при использовании бесконечной гаммы.

В качестве гаммы может быть использована любая последовательность случайных символов, например последовательность цифр числа л, числа е (основание натурального логарифма) и т. п. При шифровании с помощью ЭВМ последовательность гаммы может формироваться с помощью датчика

псевдослучайных чисел (ПСЧ). В настоящее время разработано несколько алгоритмов работы таких датчиков, которые обеспечивают удовлетворительные характеристики гаммы.

Шифрование с помощью аналитических преобразований. Достаточно надежное закрытие информации может быть обеспечено при использовании для шифрования некоторых аналитических преобразований. Для этого можно использовать методы алгебры матриц, например умножение матрицы на вектор по правилу:

$$\overline{C} = A * \overline{B}; \sum_{j=1}^{N} a_{\ddot{y}} b_{j}$$

Если матрицу А - (a_{ij}) использовать в качестве ключа, а вместо компонента вектора В = (b_j) подставить символы текста, то компоненты вектора С=(c_j) будут представлять собой символы зашифрованного текста.

Приведем пример, взяв в качестве ключа квадратную матрицу третьего порядка

$$A = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите: А — О, Б — 1, В — 2 и т. д. Тогда отрывку текста ВАТАЛА будет соответствовать последовательность 2, 0, 19, 0, 12, 0. По принятому алгоритму шифрования выполним необходимые действия:

$$\overline{C} = A * \overline{B} = \begin{Bmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{Bmatrix} \times \begin{Bmatrix} 2 \\ 0 \\ 19 \end{Bmatrix} = \begin{Bmatrix} 85 \\ 54 \\ 25 \end{Bmatrix};$$

$$\overline{C} = A * \overline{B} = \begin{Bmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{Bmatrix} \times \begin{Bmatrix} 2 \\ 0 \\ 19 \end{Bmatrix} = \begin{Bmatrix} 85 \\ 54 \\ 25 \end{Bmatrix};$$

При этом зашифрованный текст будет иметь вид: 85, 54, 25, 96, 60, 24.

Дешифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве ключа берётся матрица, обратная ой, с помощью которой осуществляется шифрование, в в качестве вектора-сомножителя – соответствующие фрагменты символов закрытого текста; тогда значениями вектора–результата будут цифровые эквиваленты знаков открытого текста.

КОДИРОВАНИЕ

Одним из средств криптографического закрытия информации, также имеющим длительную историю практического использования, является кодирование. Кодирование - это замена элементов закрываемых данных некоторыми цифровыми, буквенными или комбинированными сочетаниями — кодами. Нетрудно заметить, что между кодированием информации и ее шифрованием подстановкой существует значительная аналогия. Однако между этими методами можно найти и различия.

При шифровании подстановкой заменяемыми единицами информации являются символы алфавита, и, следовательно, шифрованию могут подвергаться любые данные, для фиксирования которых используется данный алфавит.

При кодировании замене подвергаются смысловые элементы информации, поэтому для каждого специального сообщения в общем случае необходимо использовать свою систему кодирования. Правда, в последнее время разработаны специальные коды, цель которых - сократить объем информации при записи ее в ЗУ. Специфика этих кодов заключается в том, что для записи часто встречающихся символов используются короткие двоичные коды, а для записи редко встречающихся — длинные.

Такое кодирование имеет криптографическую стойкость на уровне шифрования простой заменой.

При смысловом кодировании основной кодируемой единицей является смысловой элемент текста. Для кодирования составляется специальная таблица кодов, содержащая перечень кодируемых элементов и соответствующих им кодов. Введем, например, следующую кодовую таблицу:

Автоматизированные системы управления	001
Автоматизация управления	002
Осуществляет	415
Позволяет	632

Тогда предложение «Автоматизированные системы управления позволяют осуществлять автоматизацию управления» после кодирования будет иметь вид: 001 632 415 002.

ДРУГИЕ ВИДЫ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ ИНФОРМАЦИИ

К ним относятся рассечение-разнесение и сжатие данных. Рассечение-разнесение данных состоит в том, что массив защищаемых данных рассекается на такие элементы, каждый из которых не позволяет раскрыть содержание защищаемой информации, и выделенные таким образом элементы размещаются в различных зонах ЗУ. Обратная процедура называется сборкой данных. Совершенно очевидно, что алгоритм разнесения и сборки данных должен тщательно охраняться.

Системы с открытым ключом

Как бы ни были сложны и надежны криптографические системы, их слабое место при практической реализации — проблема распределения ключей. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС (информационная система) , ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. То есть, в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом.

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется втайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату.

Криптографические системы с открытым ключом используют так называемые необратимые, или односторонние, функции, которые обладают следующим свойством: при заданном значении *x* относительно просто вычислить значение f(x), однако если известен результат y=f(x), то нет простого пути для вычисления значения *x*.

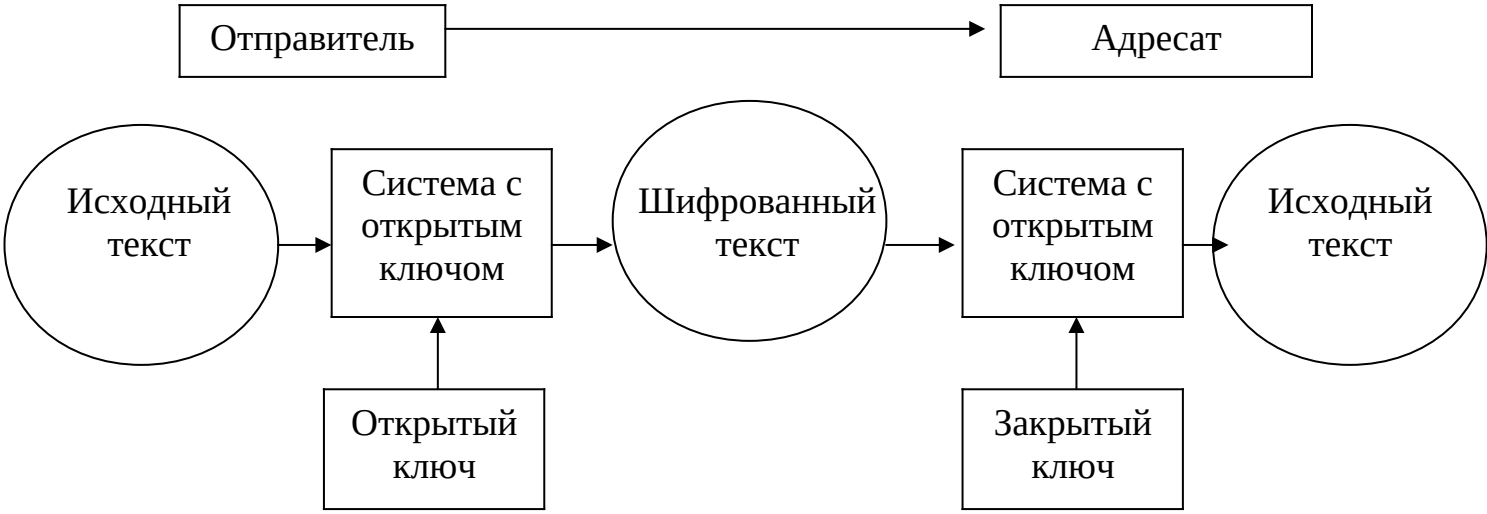

Рисунок 3 - Реализация процедуры шифрования с открытым ключом

Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС.

В самом определении необратимости присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая

невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени. Поэтому, чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.
2. Определение закрытого ключа на основе открытого также должно быть невозможным при современном уровне технологии. При этом желательна точная нижняя оценка сложности (количества операций, необходимых для раскрытия шифра).

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем.

Вообще же, все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

- разложение больших чисел на простые множители;
- вычисление логарифма в конечном поле;
- вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в трех назначениях.

1) Как самостоятельные средства защиты передаваемых и хранимых данных.
2) Как средства для распределения ключей. Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, информационный объем которых незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими потоками данных.
3) Средства аутентификации пользователей (электронная подпись).

Несмотря на довольно большое число различных СОК, наиболее популярна криптосистема RSA, разработанная в 1977 г. и получившая название в честь ее создателей — Рона Ривеста, Ади Шамира и Леонарда Эйдельмана.

Они воспользовались тем фактом, что нахождение большие: простых чисел в вычислительном отношении осуществляете) легко, но разложение на множители произведения двух таких чисел практически невыполнимо.

Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется и банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

Электронная цифровая подпись

Целью применения цифровой подписи является во-первых, гарантированное подтверждение подлинности информации, содержащейся в конкретном электронном документе, во-вторых, иметь возможность неопровержимо доказать третьей стороне (арбитру, суду и т. д.), что документ составлен именно этим конкретным лицом, являющимся действительным автором данного документа.

Для достижения указанной цели автор должен, используя свое секретное индивидуальное число (индивидуальный ключ, пароль и т. д.), определенным образом выполнять процесс «цифрового подписывания» документа. При таком подписывании каждый раз индивидуальный ключ соответствующим образом сворачивается (замешивается) с содержимым электронного документа. Полученное в результате такого сворачивания число (последовательность определенной длины цифровых разрядов) и является цифровой подписью автора под данным конкретным документом. Следовательно, процедуры подписывания и проверки цифровой подписи, в которых используется по одному ключу из пары ключей, должны быть известны, но при этом должна обеспечиваться гарантированная невозможность восстановления ключа подписывания по ключу проверки.

Впервые идея цифровой подписи как законного средства подтверждения подлинности и авторства электронного документа была выдвинута в работе Диффи и Хсллмана в 1976 г.

Как известно, при передаче сообщения по линиям связи или хранении его в памяти должны быть обеспечены вместе или по отдельности следующие требования:

1) Соблюдение конфиденциальности сообщения — злоумышленник не должен иметь возможности узнать содержание передаваемого (или хранимого) сообщения.
2) Удостоверение в подлинности полученного (или считанного из памяти) сообщения, которое включает два понятия:
   - целостность — сообщение должно быть защищено от случайного или умышленного изменения по пути его следования (или во время хранения в памяти);
   - идентификацию отправителя (проверку авторства) — получатель должен иметь возможность проверить, кем отправлено (или составлено) сообщение.

Шифрование может обеспечить конфиденциальность, а в некоторых системах и целостность. Целостность сообщения проверяется вычислением некоторой контрольной функции от сообщения (некоего числа небольшой длины). Она должна с достаточно высокой степенью вероятности изменяться даже при малых изменениях самого сообщения. Называют и вычисляют контрольную функцию по-разному:

- код подлинности сообщения (Message Authentical Code — MAC);
- квадратичный конгруэнтный алгоритм (Qua dratic Congru-entical Manipulation Detection Code — QCMDC);
- контрольная сумма;

- символ контроля блока (Block Check Character — BCC);
- циклический избыточный код (ЦИК, Cyclic Redundance Check - CRC);
- хэш-функция (Hash);
- имитовставка по ГОСТ 28147—89;
- алгоритм с усечением до п битов (n-bit Algorithm with Truncation).

При вычислении контрольной функции может использоваться какой-либо алгоритм шифрования. Возможно шифрование и самой контрольной суммы.

В настоящее время широкое применение получила цифровая подпись (цифровое дополнение к передаваемому или же хранящемуся зашифрованному тексту, которое гарантирует целостность последней и позволяет проверить авторство). Известны модели цифровой подписи на основе алгоритмов симметричного шифрования. Однако при широком использовании криптографических систем с открытыми ключами целесообразно применить цифровую подпись, так как она при этом осуществляется более удобно.

КРИПТОГРАФИЧЕСКИЕ СТАНДАРТЫ DBS И ГОСТ28147—89

Рассмотрим кратко алгоритмы блочного шифрования, принятые в качестве государственных стандартов шифрования данных в США и России.

В 1973 г. Национальное бюро стандартов США начало разработку программы по созданию стандарта шифрования данных на ЭВМ. Был объявлен конкурс среди фирм-разработчиков США, который выиграла фирма IBM, представившая в 1974 г. алгоритм шифрования, известный под названием DES (Data Encryption Standart).

В этом алгоритме входные 64-битовыс векторы, называемые блоками открытого текста, преобразуются в выходные 64-битовые векторы, называемые блоками шифртекста, с помощью двоичного 56-битового ключа K. Число различных ключей DES-алгоритма равно$2^{56}>7*10^{16}$.

Алгоритм реализуется в последовательности 16 аналогичных циклов шифрования, где на i-м цикле используется цикловой ключ K_i, представляющий собой алгоритмически вырабатываемую выборку 48 битов из 56 битов ключа K_i, i= 1,2, ..., 16.

Алгоритм обеспечивает высокую стойкость, однако недавние результаты показали, что современная технология позволяет создать вычислительное устройство стоимостью около 1 млн долларов США, способное вскрыть секретный ключ с помощью полного перебора в среднем за 3,5 часа.

Из-за небольшого размера ключа было принято решение использовать DES-алгоритм для закрытия коммерческой (несекретной) информации. Практическая реализация перебора всех ключей в данных условиях экономически нецелесообразна, так как затраты на реализацию перебора не соответствуют ценности информации, закрываемой шифром.

DES-алгоритм явился первым примером широкого производства и внедрения технических средств в области защиты информации. Национальное бюро стандартов США проводит проверку аппаратных реализаций DES-алгоритма, предложенных фирмами-разработчиками, на специальном

тестирующем стенде. Только после положительных результатов проверки производитель получает от Национального бюро стандартов сертификат на право реализации своего продукта. К настоящему времени аттестовано несколько десятков изделий, выполненных на различной элементной базе.

Достигнута высокая скорость шифрования. По некоторым сообщениям, разработаны микросхемы, реализующие DES-алгоритм со скоростью 45 Мбит/с. Велика доступность этих изделий: стоимость некоторых аппаратных реализаций ниже 100 долл. США.

Основные области применения DES-алгоритма:

1) хранение данных в ЭВМ (шифрование файлов, паролей);
2) аутентификация сообщений (имея сообщение и контрольную группу, несложно убедиться в подлинности сообщения);
3) электронная система платежей (при операциях с широкой клиентурой и между банками);
4) электронный обмен коммерческой информацией (обмен данными между покупателем, продавцом и банкиром защищен от изменений и перехвата).

В 1989 г. в СССР был разработан блочный шифр для использования в качестве государственного стандарта шифрования данных. Разработка была принята и зарегистрирована как ГОСТ 28147—89. И хотя масштабы применения этого алгоритма шифрования до сих пор уточняются, начало его внедрению, в частности в банковской системе, уже положено. Алгоритм, судя по публикациям, несколько медлителен, но обладает весьма высокой стойкостью.

Блок-схема алгоритма ГОСТ отличается от блок-схемы DES-:1лгоритма лишь отсутствием начальной перестановки и числом циклов шифрования (32 в ГОСТе против 16 в DES-алгоритме).

Ключ алгоритма ГОСТ — это массив, состоящий из 32-мерных векторов А",, X_2, ... $X_{\%}$. Цикловой ключ /-го цикла К, равен Xs, где ряду значений / от 1 до 32 соответствует следующий ряд значений s:

1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 8, 7, 6, 5,4, 3, 2, 1.

В шифре ГОСТ используется 256-битовый ключ, и объем ключевого пространства составляет 2^{256}. Ни на одной из существующих в настоящее время или предполагаемых к реализации в недалеком будущем ЭВМ общего применения нельзя подобрать ключ за время, меньшее многих сотен лет. Российский стандарт проектировался с большим запасом, по стойкости он на много порядков превосходит американский стандарт DES с его реальным размером ключа в 56 бит и объемом ключевого пространства всего 2^{56}. В свете прогресса современных вычислительных средств этого явно недостаточно. В этой связи DES может представлять скорее исследовательский или научный, чем практический интерес.

Алгоритм расшифровки отличается от алгоритма зашифровки тем, что последовательность ключевых векторов используется в обратном порядке.

Расшифровка данных возможна только при наличии синхропосылки, которая в скрытом виде хранится в памяти ЭВМ или передается по каналам связи вместе с зашифрованными данными.

Важной составной частью шифросистемы является ключевая система шифра. Под ней обычно понимается описание всех видов ключей (долговременные, суточные, сеансовые и др.), используемых шифром, и алгоритмы их использования (протоколы шифрованной связи).

В электронных шифраторах в качестве ключей могут использоваться начальные состояния элементов памяти в схемах, реализующих алгоритм шифрования, функциональные элементы алгоритма шифрования.

Ключ может состоять из нескольких ключевых составляющих различных типов: долговременных, сеансовых и т. д. Одной из основных характеристик ключа является его размер, определяющий число всевозможных ключевых установок шифра. Если размер ключа недостаточно велик, то шифр может быть вскрыт простым перебором всех вариантов ключей. Если размер ключа чрезмерно велик, то это приводит к удорожанию изготовления ключей, усложнению процедуры установки ключа, понижению надежности работы шифрующего устройства и т. д. Таким образом, выбранный криптографом размер ключа — это всегда некий компромисс.

Заметим, что DES-алгоритм подвергался критике именно в связи с небольшим размером ключа, из-за этого многие криптологи пришли к мнению, что необходимым «запасом прочности» DES-алгоритм не обладает.

Другой важной характеристикой ключа является его случайность.

Наличие закономерностей в ключе приводит к неявному уменьшению его размера и, следовательно, к понижению криптографической стойкости шифра. Такого рода ослабление криптографических свойств шифра происходит, например, когда ключевое слово устанавливается по ассоциации с какими-либо именами, датами, терминами. Всякая логика в выборе ключа наносит ущерб криптографическим свойствам шифра.

Таким образом, требование случайности ключей выступает как одно из основных при их изготовлении.

Для изготовления ключей могут использоваться физические датчики и псевдослучайные генераторы со сложным законом образования ключа. Использование хорошего физического датчика более привлекательно с точки зрения обеспечения случайности ключей, но является, как правило, более дорогим и менее производительным способом. Псевдослучайные генераторы более дешевы и производительны, но привносят некоторые зависимости если не в отдельные ключи, то в совокупности ключей, что также нежелательно.

Важной частью практической работы с ключами является обеспечение секретности ключа. К основным мерам по защите ключей относятся следующие:

1) ограничение круга лиц, допущенных к работе с ключами;
2) регламентация рассылки, хранения и уничтожения ключей;
3) регламентация порядка смены ключей;
4) применение технических мер защиты ключевой информации от несанкционированного доступа.

Важной составляющей зашиты информации являются про-юколы связи, определяющие порядок вхождения в связь, зашифровки и передачи информации. Протокол связи должен быть построен с учетом следующих обстоятельств:

1) протокол должен защищать открытый текст и ключ от несанкционированного доступа на всех этапах передачи информации от источника к получателю сообщений;
2) протокол не должен допускать выхода в линии связи «лишней» информации, предоставляющей криптоаналитику противника дополнительные возможности дешифрования криптограмм.

Нетрудно видеть, что использование криптосистем с секретным ключом предполагает заблаговременные до сеансов связи договоренности между абонентами о сеансовых секретных ключах или их предварительную пересылку по защищенному каналу связи.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ МЕТОДОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В АСОД
(автоматизированные системы обработки информации)

Проблема реализации методов защиты информации имеет два аспекта [2]: разработку средств, реализующих криптографическое закрытие, и методику использования этих средств. Каждый из рассмотренных выше методов закрытия информации может быть реализован либо аппаратными, либо программными средствами. Возможность программной реализации обусловливается тем, что все методы криптографического закрытия формальны и могут быть представлены в виде конечной алгоритмической процедуры.

При аппаратной реализации все процедуры шифрования и дешифрования реализуются специальными электронными схемами. Обычно такие схемы выполняются в виде отдельных модулей, сопрягаемых с ЭВМ, терминалами пользователей, модемами связи, с другими элементами автоматизированных систем. Наибольшее распространение получили модули, реализующие комбинированные методы шифрования. При этом непременным компонентом всех аппаратно реализованных комбинаций шифров является гаммирование. Это объясняется, с одной стороны, достаточно высокой степенью закрытия с помощью гаммирования, а с другой — сравнительно простой схемой, реализующей этот метод. Обычно в качестве генератора гаммы применяют широко известный регистр сдвига с обратными (линейными или нелинейными) связями. Минимальный период порождаемой таким регистром последовательности составляет 2^N- 1 двоичных знаков. Если, например, N=56 (столько рабочих разрядов в регистре сдвига шифрующего аппарата для уже упоминавшегося DES), то 2^{56} - 1 = 10^{16}. Если перебирать знаки этой гаммы со скоростью 1 млн знаков в секунду, то для перебора всех знаков одного периода потребуется не менее 3000 лет.

Для повышения качества генерируемой последовательности можно предусмотреть специальный блок управления работой регистра сдвига. Такое управление может заключаться, например, в том, что после зашифровки определенного объема исходного текста содержимое регистра сдвига циклически изменяется (например, сдвигается на несколько тактов). Дальнейшего повышения качества генерируемой гаммы можно достичь, если использовать три регистра

сдвига, два из которых являются рабочими, а третий — управляющим. На каждом такте работы в качестве знака гаммы принимается выходной сигнал первого или второго регистра, причем выбор определяется значением выходного сигнала третьего регистра (0 — выбор первого регистра, 1 — выбор второго регистра).

Еще одна возможность улучшения криптографических свойств гаммы заключается в использовании нелинейных обратных связей. При этом улучшение достигается не за счет увеличения длины гаммы, а за счет усложнения закона ее формирования, что существенно усложняет криптоанализ. Показано, что N регистров сдвига с нелинейными обратными связями обеспечивают такую же стойкость шифра, что и 2^N регистров с линейными связями.

ТЕХНИЧЕСКИЕ СРЕДСТВА КРИПТОГРАФИИ

К настоящему времени разработано значительное число шифровальных аппаратов, различающихся и алгоритмом работы, и методом формирования гаммы. Рассмотрим некоторые из них.

Например, фирмой AEG-Tclcfunkcn разработана система Telekrypt, реализующая шифрование гаммированием. Формирование гаммы осуществляется с помощью специальной процедуры с использованием двух ключей — основного, определяемого пользователем, и дополнительного, определяемого системой. Основной ключ может принимать 10^{30} различных значений, он вводится в систему с помощью специальной карты. Дополнительный ключ выбирается системой случайно, он передается на щифроаппарат получателя сообщения в начале каждого нового сообщения. Благодаря наличию дополнительного ключа появляется возможность применения двухкаскадного ключа с варьируемой периодичностью изменения. С использованием одного и того же основного ключа можно в таком случае передавать больший объем информации при обеспечении требуемой надежности закрытия информации.

Шифровальное устройство Telekrypt выполнено на интегральных схемах. Для предотвращения выдачи в линию открытого исходного текста предусмотрено специальное устройство контроля. Максимальная скорость формирования гаммы достигает 10 Кбит/с,

Американская фирма Cryptex разработала устройство шифрования данных для вычислительной системы TRS-80. Устройство размером с пачку сигарет подключается к задней панели ЭВМ или шине интерфейса.

В этом устройстве применен алгоритм шифрования, который существенно отличается от DES. Хотя структура алгоритма держится в секрете, его разработчики утверждают, что достигнутая ими стойкость шифрования превышает стойкость DES. Повышения стойкости удалось добиться за счет увеличения длины исходного ключа, используемого для формирования гаммы. Ключ состоит из 10 символов кода ASCII. В двоичном исчислении длина кода равна 80 битам, что значительно превышает длину ключа DES. За счет дополнительного усложнения алгоритма (ветвление кода и задержка в использовании формируемой гаммы) удается увеличить объем пространства ключей до 2^{350} двоичных знаков. Максимальная скорость шифрования до 15 тыс.

символов в минуту. Устройство имеет усиленный корпус и защиту от воздействия внешних электромагнитных полей.

ПРОГРАММНЫЕ СРЕДСТВА

Основным достоинством программных методов реализации криптографической защиты является их гибкость, т. е. возможность быстрого изменения алгоритма шифрования. При этом можно предварительно создать пакет шифрования, содержащий программы для различных методов шифрования или их комбинаций. Смена программ будет производиться оперативно в процессе функционирования системы.

Основным недостатком программной реализации криптографических методов является существенно меньшее быстродействие. Например, при аппаратной реализации национального стандарта время на обработку одного блока составляет примерно 5 мкс, при программной реализации на большой ЭВМ — 100 мкс, а на специализированной мини-ЭВМ это время составляет примерно 50 мкс. Поэтому при больших объемах защищаемой информации аппаратные методы представляются более предпочтительными. Программные методы, кроме того, могут быть реализованы только при наличии в составе аппаратуры мощного процессора, тогда как шифрующие аппараты с помощью стандартных интерфейсов могут подключаться практически к любым подсистемам автоматизированных систем.

По способу использования средств закрытия информации обычно различают потоковое и блочное шифрование. При потоковом шифровании каждый символ исходного текста преобразуется независимо от других. Поэтому такое шифрование может осуществляться одновременно с передачей данных по каналу связи. При блочном шифровании одновременно преобразуется некоторый блок символов закрываемого исходного текста, причем преобразование символов в пределах блока является взаимозависимым. Может существовать зависимость и между преобразованиями символов в некоторых смежных блоках.

ПРОБЛЕМА УПРАВЛЕНИЯ КЛЮЧАМИ

Большие трудности возникают при формировании механизма распределения ключей криптографического преобразования. Одним из принципов, которого придерживаются многие специалисты в области криптографии, является несекретность используемого способа закрытия. Предполагается, что необходимая надежность закрытия полностью обеспечивается за счет сохранения в тайне ключей. Именно этим объясняется то, что алгоритм и архитектура аппаратной реализации DES были широко опубликованы в печати. Отсюда с однозначностью вытекает принципиальная важность формирования ключей, распределения их и доставки в пункты пользования. Существенными аспектами этой проблемы являются следующие соображения:

- ключи должны выбираться случайно, чтобы исключалась возможность их отгадывания на основе каких-либо ассоциаций;

- выбранные ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю;
- механизм распределения ключей должен обеспечивать тайну ключей на всех этапах функционирования системы. Ключи должны передаваться по линиям связи и храниться в системе обработки только в защищенном виде;
- должна быть предусмотрена достаточно частая смена ключей, причем частота их изменения должна определяться двумя факторами: временем действия и объемом закрытой с их использованием информации.

Если система криптографического закрытия информации разработана правильно, то доступ злоумышленников к информации невозможен. Однако любое отступление от правил использования реквизитов защиты может явиться причиной утечки информации. Поэтому соблюдение этих правил является непременным условием надежной защиты информации.

Очень сложной является проблема распределения ключей в сети с большим числом пользователей. Суть проблемы состоит в том, чтобы в случае необходимости обеспечить секретную связь между любыми двумя пользователями, и только эти пользователи должны знать ключ, используемый для шифрования сообщений. Эту задачу можно решить, предоставив каждому из пользователей по m - 1 ключу, т. е. по одному ключу для связи с каждым из остальных пользователей. При этом необходимо распределить m(m - 1) пар ключей, что представляется невыполнимой на практике задачей.

Применение другого метода требует от пользователей доверия к сети. При этом каждому пользователю нужно запомнить только один ключ. Этим ключом шифруются сообщения, которые передаются к одному из узлов сети. Там оно перешифровывается и передается к следующему узлу. Этот процесс продолжается до тех пор, пока сообщение не поступить точку назначения. Так как при таком подходе для разрушения секретности в сети достаточно разрушить защиту лишь в одном узле, то авторы не настаивают на использовании этого метода. Они предлагают два дополнительных полхода, которые позволяют разрешить возникающие проблемы.

При первом подходе требуется, чтобы небольшое число к узлов сети функционировало в качестве узлов распределителей ключей. Каждый пользователь запоминает к ключей, каждый из которых должен применяться при связи с определенным узлом. Когда два пользователя захотят установить между собой связь, они соединяются со всеми узлами и получают случайные ключи от каждого из узлов. Затем пользователь объединяет эти ключи с помощью операции «исключающее ИЛИ» и использует результат в качестве действительного ключа для шифрования любых сообщений. Преимуществом такого подхода является уменьшение распределяемого числа ключей. Кроме того, для разрушения секретности в такой сети нужно разрушить секретность во всех узлах-распределителях ключей в сети.

При использовании второго подхода допускается, чтобы некоторые ключи были известны. При этом пользователь имеет два ключа — А и Б, ключ А используется для шифрования сообщений самого пользователя, а Б — для

расшифровки сообщений, поступающих к пользователю. Необходимым условием при этом является выполнение следующих требований: пары А—Б должны формироваться с помощью простых методов, при этом, однако, вычисление ключа Б по ключу А должно представлять собой невыполнимую задачу. Ключ А является общим, так как он используется всеми пользователями системы для передачи сообщений к данному пользователю. Так как ключи А и Б связаны между собой, то требование невозможности восстановления А и Б является совершенно обязательным.

Задача управления большим числом ключей является очень важной при использовании любого метода шифрования. Известен метод, который применим для обеспечения секретности связи в системе с единственной центральной ЭВМ и большим числом терминалов.

Предположим, что каждый терминал имеет единственный главный терминальный ключ, известный на терминале и в центральной ЭВМ. В этой ЭВМ ключ может быть защищен с помощью главного ключа ЭВМ, который недоступен для любой программы пользователя. Для любого интервала работы центральная ЭВМ генерирует интервальный ключ, который передается на терминал после зашифронывания с помощью главного ключа терминала. После расшифровки интервального ключа с помощью своего главного ключа терминал использует его в течение всего интервала работы с центральной ЭВМ.

Таким образом, используемые в системе ключи подразделяются на ключи для шифрования данных и ключи для шифрования ключей. Последние должны быть очень устойчивыми, поэтому для их генерации рекомендуется использовать случайные процессы. Ключи для шифрования данных используются в значительно большем количестве и сменяются значительно чаще. Поэтому их можно формировать с помощью некоторого детерминированного процесса или устройства.

ХАРАКТЕРИСТИКИ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

Важнейшей характеристикой криптографического закрытия информации является его стойкость [8]. Под этим понимается тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, по стойкости шифра можно определить предельно допустимый объем информации, зашифровываемой при использовании одного ключа.

При выборе криптографического алгоритма для использования в конкретной разработке его стойкость, т. е. устойчивость к попыткам противоположной стороны его раскрыть, является одним из определяющих факторов. Вопрос о стойкости шифра при ближайшем рассмотрении сводится к двум взаимосвязанным вопросам:

- можно ли вообще раскрыть данный шифр;
- если да, то насколько это трудно сделать практически.

Шифры, которые вообще невозможно раскрыть, называются абсолютно или теоретически стойкими. Существование подобных шифров доказывается теоремой Шеннона, однако ценой этой стойкости является необходимость

использования для шифрования каждого сообщения ключа, не меньшего по размеру самого сообщения.

Во всех случаях, за исключением ряда особых, эта цена чрезмерна, поэтому на практике в основном используются шифры, не обладающие абсолютной стойкостью. Таким образом, наиболее употребительные схемы шифрования могут быть раскрыты за конечное время или, что точнее, за конечное число шагов, каждый из которых является некоторой операцией над числами. Для таких схем важнейшее значение имеет понятие практической стойкости, выражающее практическую трудность их раскрытия. Количественной мерой этой трудности может служить число элементарных арифметических и логических операций, которые необходимо выполнить, чтобы раскрыть шифр, т. е. чтобы для заданного шифротекста с вероятностью, не меньшей заданной величины, определить соответствующий открытый текст. При этом в дополнение к дешифруемому массиву данных криптоаналитик может располагать блоками открытых данных и соответствующих им зашифрованных данных или даже иметь возможность получить для любых выбранных им открытых данных соответствующие зашифрованные данные. В зависимости от перечисленных и многих других неуказанных условий различают отдельные виды криптоанализа.

Все современные криптосистемы построены по принципу Кирхгофа, т. е. секретность зашифрованных сообщений определяется секретностью ключа. Это значит, что даже если сам алгоритм шифрования известен криптоаналитику, тот тем не менее не в состоянии расшифровать сообщение, если не располагает соответствующим ключом. Все классические блочные шифры, в том числе DES и ГОСТ, соответствуют этому принципу и спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полным перебором по всему ключевому пространству, т. е. по всем возможным значениям ключа. Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

Оценка стойкости методов шифрования

Моноалфавитная подстановка является наименее стойким шифром, так как при ее использовании сохраняются все статистические закономерности исходного текста. Уже при длине зашифрованного текста в 20—30 символов указанные закономерности проявляются в такой степени, что, как правило, позволяют вскрыть исходный текст. Поэтому такое шифрование считается пригодным только для закрытия паролей, коротких сигнальных сообщений и отдельных знаков.

Стойкость **простой полиалфавитной подстановки** (из подобных систем нами была рассмотрена подстановка по таблице Вижинера) оценивается значением 20^n, где n — число различных алфавитов, используемых для замены. При использовании таблицы Вижинера число различных алфавитов определяется числом букв в ключевом слове. Усложнение полиалфавитной подстановки существенно повышает ее стойкость.

Монофоническая подстановка может быть весьма стойкой (и даже теоретически нераскрываемой), однако строго монофоническую подстановку, в которой все символы имеют равные вероятности появления, реализовать на

практике трудно, а любые отклонения от монофоничности снижают реальную стойкость шифра.

Стойкость **простой перестановки** однозначно определяется размерами используемой матрицы. Например, при использовании матрицы 16 x 16 число возможных перестановок достигает $1,4 \times 10^{26}$. Такое число вариантов невозможно перебрать даже с использованием современных ЭВМ. Стойкость усложненных перестановок может быть выше. Однако следует иметь в виду, что при шифровании перестановкой полностью сохраняются вероятностные характеристики исходного текста, что облегчает криптоанализ.

Стойкость **гаммирования** однозначно определяется длиной периода гаммы. В настоящее время реальным становится применение бесконечной гаммы, при использовании которой теоретическая стойкость зашифрованного текста также будет бесконечной.

Можно отметить, что для надежного закрытия больших массивов информации наиболее пригодны гаммирование и усложненные перестановки и подстановки.

При использовании **комбинированных методов шифрования** стойкость шифра равна произведению стойкостей отдельных методов. Поэтому комбинированное шифрование является наиболее надежным способом криптографического закрытия. Именно такой метод был положен в основу работы всех известных в настоящее время шифрующих аппаратов (в том числе и аппарата, реализующего DES).

Рассмотренные значения стойкости шифров являются потенциальными величинами. Они могут быть реализованы при строгом соблюдении правил использования криптографических средств защиты. Основными из этих правил являются: сохранение в тайне ключей, исключение дублирования и достаточно частая смена ключей. Остановимся на двух последних правилах. Под дублированием здесь понимается повторное шифрование одного и того же отрывка текста с использованием тех же ключей (например, если при первом шифровании имел место сбой). Нарушение этого правила резко снижает надежность шифрования, так как исходный текст может быть восстановлен с помощью статистического анализа двух вариантов текста.

Важнейшим правилом использования криптографических средств является достаточно частая смена ключей. Причем эту частоту можно определять и исходя из длительности использования ключа, и объема зашифрованного текста. При этом смена ключей по временному графику является защитной мерой против возможного их хищения, а смена после шифрования определенного объема текста — от раскрытия шифра статистическими методами.

До сих пор мы предполагали, что злоумышленник не обладает никакой другой информацией, кроме отрезка зашифрованного текста. Однако для крупных современных систем коллективного пользования, для которых более характерно территориальное распределение отдельных элементов, злоумышленнику может стать доступной и дополнительная информация, которая может существенно облегчить криптоанализ.

На практике, например, может встретиться ситуация, когда злоумышленник имеет возможность направить в систему ряд специально подобранных сообщений и получить их от системы в зашифрованном виде. Особенно опасна такая

ситуация при использовании перестановок. При использовании полиалфавитных подстановок это облегчает определение количества используемых алфавитов, а при использовании гаммирования — закономерности формирования гаммы. Более того, если злоумышленнику удается полностью перехватить зашифрованное сообщение, то он может попытаться получить «куски» шифрованного и соответствующего исходного текстов, предполагая наличие в сообщении служебных слов: адреса отправителя, даты, времени, грифа секретности и т. п. Все это может быть использовано при криптоанализе зашифрованного текста.

Технико-экономические показатели криптографических средств

Расходы на программную реализацию криптографических методов защиты определяются сложностью алгоритмов прямого и обратного преобразований. Оценка затрат на эти цели производится по тем же методикам, что и оценка затрат на другие компоненты программного обеспечения. При этом, однако, надо иметь в виду, что для подавляющего большинства методов закрытия прямое и обратное преобразования осуществляются по одному и тому же алгоритму.

Расходы на аппаратную реализацию могут быть оценены приближенно стоимостью шифрующей аппаратуры. По данным зарубежной печати, такие аппараты в настоящее время поступают на коммерческий рынок. Выпускаются и поступают в продажу, например, шифрующие аппараты, реализующие DES.

Одной из наиболее важных технико-экономических характеристик систем криптографического закрытия является трудоемкость метода шифрования, которую можно выразить числом элементарных операций, необходимых для шифрования одного символа исходного текста.

При шифровании подстановкой необходимо выполнить выбор алфавита и поиск необходимого символа в этом алфавите. При полиалфавитной подстановке дополнительно необходимо выполнить выбор очередного алфавита. Основными процедурами, выполняемыми при перестановке, являются выбор знаков исходного текста, определение места записи и запись в поле шифрованного текста. Трудоемкость аналитического преобразования определяется сложностью используемого преобразования. Если, например, используется правило перемножения матрицы и вектора, то для шифрования одного символа необходимо осуществить т умножений и т - 1 сложений, где т — размерность матрицы.

При шифровании гаммированисм основная трудоемкость связана с формированием гаммы. Если, например, для этой цели применен линейный рекуррентный генератор, реализующий алгоритм вида $/_{;+|}$ = (flf, + c) mod m, где a и c — константы, то нетрудно заметить, что для формирования каждого знака гаммы необходимо выполнить не менее трех операций.

Таким образом, наиболее трудоемкими являются аналитические преобразования, затем по мере снижения трудоемкости следует гаммирование, перестановки и замены.

ПРАКТИЧЕСКАЯ ЧАСТЬ

ШИФР ЦЕЗАРЯ

Один из самых первых методов шифрования носит имя римского императора Юлия Цезаря (I век до н.э.), который если и не сам изобрел его, то активно им пользовался. Этот метод основан на замене каждой буквы шифруемого текста на другую, путем смещения в алфавите от исходной буквы на фиксированное количество символов, причем алфавит читается по кругу, т.е. после буквы ***я*** рассматривается ***а***. Регистр символов не учитывается. Так, например, слово ***байт*** при смещении на два символа вправо кодируется словом ***гвлф.***

Задание:

1. Расшифруйте слово НУЛТХСЁУГЧЛВ, закодированное с помощью шифра Цезаря. Известно, что каждая буква исходного текста заменяется третьей после неё буквой.
2. Расшифруйте четверостишие Омара Хайяма:

РЛЗЪЁМЭЙЗ АВБЖУ ИЙЗАВЛУ, БЖЩЛУ ЖЩЭЗЪЖЗ ЖЮЁЩЕЗ,
ЭЫЩ ЫЩАЖФО ИЙЩЫВЕЩ БЩИЗЁЖВ ЭЕШ ЖЩРЩЕЩ:
ЛФ ЕМРСЮ ЬЗЕЗЭЩГ, РЮЁ РЛЗ ИЗИЩЕЗ ЮКЛУ
В ЕМРСЮ ЪМЭУ ЗЭВЖ, РЮЁ ЫЁЮКЛЮ К ДЮЁ ИЗИЩЕЗ.

Конкретный вариант шифрования методом Цезаря неизвестен.

ШЕРЛОК ХОЛМС И ШИФРОВКА

Шерлок Холмс обнаружил начальную строку зашифрованного послания, написанного неизвестным ему шифром:

ШЫР-ПИР Ю ПАПУЖГЫ
ЗЭЛЭМЪГЫЙ ГЁСРЫГ…

Помогите Холмсу расшифровать послание.

«ТАРАБАРСКАЯ ГРАМОТА»

Найдите ключ к «тарабарской грамоте» - тайнописи, применявшейся ранее в России для дипломатической переписки:

Пайцике тсюг т «камащамлтой чмароке» - кайпонили, нмирепяшвейля ш Моллии цся цинсоракигелтой неменилти

Ключом в данном случае будем называть правила, по которым шифруется исходный текст.

НОМЕРА ВМЕСТО БУКВ

Если в некотором слове заменить буквы на номера этих букв в алфавите, то получится число 222122111121. Какое это слово?

ОДНАЖДЫ В ПОЕЗДЕ

Когда-то давно, когда ещё существовала страна под названием «СССР», автор ехал в поезде и с удивлением обнаружил, что если в названиях пунктов отправления и назначения поезда заменить буквы их номерами в алфавите, то они (названия) записываются с помощью всего лишь двух цифр: 211221 и 21221.
Откуда и куда ехал автор?

ЧТО ТАКОЕ "ЛЯГЯНЯ"?

Расшифруйте следующий текст:

Тядзгьщхоэь пэжо ч йчтэяшаь гэнэшюэь
епяу дызысю, бэхыэь пыъ бэ лягяня
чтгыщюпмчо ю ч ячпыхмшаью дызысыью,
ЫIщпяга.

Известно, что он зашифрован следующим образом.

Гласные буквы: а, о, у, ы, я, е, ю, и, э, й как-то разбиты на пары. При этом буква «й» условно причислена к гласным, а буквы «ъ, ь» - к согласным
Согласные буквы:
б, в, г, д, ж, з, к, л, м, н, п, р, с, т, ф, х, ц, ч, ш, щ, ъ, ь
также как-то разбиты на пары.

Каждая буква в тексте заменена на другую букву из той же пары. Зашифрованный текст записан по правилам русской пунктуации.

ШИФР ВИЖИНЕРА

Шифр Вижинера представляет собой шифр Цезаря с переменной величиной сдвига. Величина сдвига задается некоторым ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 3 1 9 1 3 1 9 1 и т.д.

Используя ключевое слово ВАГОН, зашифруйте слова: АЛГОРИТМ, ПРАВИЛА, ИНФОРМАЦИЯ.

ПОСЛАНИЕ БУДУЩИМ ИЗДАТЕЛЯМ

В одной книге, которая переводилась с английского языка, при переводе были сделаны ошибки. Тем, кто будет готовить новое издание книги, послали следующую шифровку:

ИВСЬПТРЕА СРТЫАЕ ОБШКИИ И ОАПТЕКЧИ И НЕ ДЙЕТЛЕА НЫОХВ!

Расшифруйте ее.

ШИФРОВАНИЕ ДВУМЯ ЦИФРАМИ

Шифр можно ещё более усложнить, если дополнительно к этому каждую букву заменять не одним, а двумя или несколькими символами (буквами или числами). Вот пример. Расположим буквы русского алфавита в квадратной таблице 6х6 произвольным образом, например, так как в таблице 1.

Таблица 1

	0	1	2	3	4	5
0		з	и	ы	р	с
1	а	т	у	й	ь	э
2		б	в	ф	к	л
3	м	ю	я	г	х	ц
4	ч	н	о		д	е
5	ж	ш	щ	п		

Каждую букву шифруем парой цифр: первая цифра – это номер строки, в которой стоит данная буква, вторая – номер столбца. Например, букве *б* соответствует обозначение 21, а слову *шифр* – обозначение 51022304.

Задания для самостоятельной работы

1. Расшифруйте следующий текст, зашифрованный с использованием таблицы 1.

   2205110445401053450445414205021105324 1

   1041454253044544452545414103130504422 4

2. Используя таблицу 1, зашифруйте текст: «Срочно приезжай Ангел».

ШИФРОВАНИЕ ТЕКСТА С ПОМОЩЬЮ ТАБЛИЧЕК

Например, необходимо зашифровать текст, содержащий k букв. Пусть $\sqrt{k}=m$. Заменим m на ближайшее к нему целое четное число, не меньшее $\sqrt{k}$. Возьмем квадратную таблицу порядка m (m строк, m столбцов), в которой по определенному правилу будем вырезать квадраты-«окошки».

В качестве примера зашифруем фразу «Тарабарская грамота – несложный шифр». В ней 31 буква, $\sqrt{31}\approx 5{,}6$. Значит, $m=6$, т.е. наша таблица будет содержать 6 строк и 6 столбцов.

Разделим квадратную таблицу на четыре равных квадрата, обозначим их **A, B, C, D**.

A	**B**
C	**D**

При этом каждый из квадратов содержит $m/2$ строк. Заполним квадрат **A** последовательно числам от 1 до $(m/2)^2$. Для $m=6$ получим:

1	2	3
4	5	6
7	8	9

При повороте квадрата **A** на 90^0 по часовой стрелке мы получим квадрат **B**, при этом числа квадрата **A** тоже повернутся:

7	4	1
8	5	2
9	6	3

Точно так же заполним числами квадраты **C** и **D.** Таким образом, таблица принимает вид, показанный на рисунок 1:

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

Рисунок 1

Теперь остается вырезать 9 «окошек» (всего клеток 6x6=36; поворотов – 4, значит, окошек должно быть 36/4=9).

Выделяем числа от 1 до 9 из любого квадрата, например, такие, как на рисунке 2:

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

Рисунок 2

Итак, окончательный вид вспомогательной таблицы-трафарета:

Рисунок 3

Вписываем в окошки построчно текст без пробелов, поворачивая вспомогательную таблицу по мере заполнения. Так как букв во фразе всего 31,

а клеток – 36, то 5 оставшихся клеток заполним последовательными буквами алфавита: *а, б, в, г, д* (рисунок 4).

н	ш	т	и	а	ф
р	а	е	я	с	р
л	а	г	о	а	р
б	а	б	в	ж	а
н	р	г	с	а	м
о	ы	т	й	а	к

Рисунок 4

Для расшифровки получателю послания необходимо воспользоваться такой же точно вспомогательной таблицей, четырежды повернуть её и прочитать текст.

Вариантов вспомогательных таблиц размера 6х6 очень много. В нашем примере окно под номером 1 мы взяли из квадрата **C**, хотя возможных вариантов – 4 (из квадрата **A, B, C** или **D**). Точно так же число 2 можно взять не из квадрата **B**, а из любого из четырех. Значит, существует $4*4=4^2=16$ способов выбрать два окна. Рассуждая таким образом, приходим к выводу, что существует $4^9=262\ 144$ различных комбинаций для таблицы размера 6х6. Так что вероятность подобрать таблицу для расшифровки крайне мала.

Как только что говорилось, для последующей расшифровки второй участник секретной переписки должен иметь точно такую же вспомогательную таблицу, то есть вместе с сообщением необходимо передавать и матрицу, что не всегда удобно. Если бы можно было и её закодировать! Один из вариантов решения этой задачи заключается в том, чтобы «окошечки» обозначить единицей, а «невырезанные» клетки – нулем. Тогда каждой строке таблицы можно сопоставить в соответствие некоторое двоичное число. Далее следует перевести полученные двоичные числа в десятичные. В результате такого шифрования в приведенной чуть выше вспомогательной матрице будут записаны числа:

- 1-я строка: $001010_2=1010_2=10_{10}$
- 2-я строка: $000001_2=1_2=1_{10}$
- 3-я строка: $010000_2=10000_2=16_{10}$
- 4-я строка: $001001_2=1001_2=9_{10}$
- 5-я строка: $010100_2=20_{10}$
- 6-я строка: $000001_2=1_2=1_{10}$

Задания для самостоятельной работы

1. Расшифруйте сообщение

   АЬИЛППТИООСОЗСДЬЬПРМГОВРААРМОВМ
   ЛУРЯЕЮОТЧИЕТТДААПКРЦТБАЬЕВУКИДРЮ2,
   69,16,66,149,32,4,164

2. Зашифруйте рассмотренным методом текст:
   ВСЁИДЁТПОПЛАНУ

ЗАДАНИЯ ДЛЯ ДЕШИФРОВКИ ТЕКСТОВ, ЗАШИФРОВАННЫХ МЕТОДАМИ ПЕРЕСТАНОВКИ

1. Изречение немецкого философа Фридриха Ницце:

   ОЬТСО НЙАЧУ ЛСВТЯ РЕВЕН ИЛЕТИ ДЕБОЛ

2. Изречение немецкого ученого – гуманиста Эразма Роттердамского

   ЙЫТЫР КСТНА ЛАТЕН ТЕАДЗ ОСИИЦ АТУПЕ РОООО

3. Изречение чешского писателя Карела Чапека:

   ЕЛЙГС АМОЛТ ЕМИЬР УНСЕО МОООП МОЖОЕ ОЕКШО ШРАОЬ АЙОСЙ ДОДНДР ОЕЕУО

4. Изречение датского ученого-физика Нильса Бора:

   ТПРРО УСЕБД ОДИН ОБЖВЛ ООЕЕУ ИОЧОЕ НАДТО ЩНЬЕУ ОТДБУ

5. Изречение французского философа Жана-Поля Сартра:

   ИНККО ОТСОЧ ЯЧПОТ ЕАРЕЯ ОЛНЕА АЕМТК ОНСТШ

6. Высказывания польского писателя-фантаста Станислава Лемма:

   ТОУМА МЕЖЕЧ ЫАООО ОММГЗ ЕСНМЕ ДЕООО ЧЫАОД НЛОТМ УМООО ТДЕРО ЕОЧОМ МОООО

7. Высказывание американского писателя Джона Стейнбека:

   АРЕНО ЫЕТМО ЕЖОИБ ЕДДЖЙ ЯПТВС ОДОКМ ПСИОЖ ОЙЛГО ОИЕНТ

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое криптология?
2. Что такое ключ?
3. Определите понятие «криптологический алгоритм».
4. Какие функции выполняет криптологический протокол?
5. Что из себя представляет криптосистема?
6. Дайте определение стойкости криптосистемы.
7. Дайте общее определение цифровой подписи.
8. В чем заключается суть электронной цифровой подписи?
9. Объясните суть преобразования перестановка – замена.
10. Что из себя представляет система шифрования с использованием таблицы Вижинера?
11. Что из себя представляет симметричная криптографическая система?
12. Объясните суть алгоритма DES и укажите на его особенности.
13. В каких режимах может работать алгоритм DES?
14. Дайте описание отечественного алгоритма криптографического преобразования данных и его отличительных особенностей.
15. Какие режимы имеет отечественный алгоритм криптографического преобразования данных (ГОСТ 28147-90) ?
16. Какими характеристиками оценивается стойкость криптографических систем?

ЛИТЕРАТУРА

1. Баричев С.В. Криптография без секретов. М.: Наука, 1998 г.
2. Герасименко В.А. Защита информации в автоматизированныхсистемах обработки данных. М.: Энергоавтоиздат, 1994 г.
3. Мельников В.П. Информационная безопасность: учебное пособие для студентов СПО. – М.: Издательский центр «Академия», 2008.
4. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие для студентов СПО. – М.: ФОРУМ, 2008.
5. Златопольский Д.М. Простейшие методы шифрования текста. – газета «Информатика» №5(17)/2007.