*Калужский*

# Лабораторная работа №1

Исследование традиционных методов симметричного шифрования

Цель работы: сформировать практические навыки применения традиционных методов симметричного шифрования.

Задачи: Изучить классические алгоритмы симметричного шифрования. Разработать алгоритмы симметричного шифрования и расшифровывания. Реализовать на их основе программы для защиты текстовых данных.

Требования к отчету.

Отчет по лабораторной работе должен содержать:

1. Титульный лист установленного образца.
2. Постановку задачи.
3. Описание хода выполнения работы
4. Вывод

Длительность работы:8 академических часов.

Защита работы: собеседование с преподавателем по контрольным вопросам.

Задание: разработать программу, осуществляющую криптографическую защиту информации, содержащейся в файле данных, с помощью алгоритма шифрования, указанного в варианте.

Дополнительное задание: написать программу/модуль генерации случайных ключей шифра, оценить размерность ключевого пространства.

Варианты заданий:

1. Шифрующие таблицы с перестановкой по ключу – размеру таблицы
2. Шифрующие таблицы с числовым ключом
3. Шифрующие таблицы с ключевым словом
4. Шифрующие таблицы с двойной перестановкой по числовому ключу
5. Полибианский квадрат для русского алфавита
6. Полибианский квадрат для английского алфавита
7. Шифрующие таблицы Трисемуса
8. Шифр Уинстона

Вариант повышенной сложности:

1. Магические квадраты

Теоретические сведения

Симметричными называют алгоритмы, в которых шифрование и дешифрование ведется на одном и том же ключе. И этот ключ является секретным. Сам алгоритм зашифровывания, как правило, считается известным всем.

Рассмотрим традиционные (классические) ме­тоды симметричного шифрования, отличающиеся простотой и наглядностью.

Табличные шифры перестановки

Табличные шифры появились в эпоху Возрождения (конец XIV столетия). Разработанные в то время шифрующие таблицы по существу задают правила перестановки букв в сообщении. Они относятся к шифрам перестановки и являются блочными шифрами, где длина блока определяется размером таблицы.

Шифрующие таблицы с перестановкой по ключу – размеру таблицы.

Одним из самых примитивных табличных шифров является простая перестановка, для которой ключом служит размер таблицы. Например, сообщение записывается в таблицу поочередно по столбцам. После заполнения таблицы текстом сообщения по столбцам для формирования шифротекста считывают содержимое таблицы по строкам. При расшифровывании действия выполняют в обратном порядке. Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы.

Шифрующие таблицы с перестановкой по числовым или буквенным ключам.

Несколько большей стойкостью к раскрытию обладает ме­тод шифрования, называемый перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову или набору чисел длиной в строку таблицы. В верхней (ключевой) строке таблицы до перестановки записывается ключ, затем столбцы таблицы переставляются в соответствии с алфавитным порядком букв ключа в алфавите или по возрастанию или убыванию цифр ключа. Затем буквы считываются по строкам, получается блок шифротекста.

Пример. Зашифруем сообщение: «ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ» с помощью таблицы 5х7 и ключевого слова «ПЕЛИКАН»:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | Е | Л | И | К | А | Н |  | А | Е | И | К | Л | Н | П |
| 7 | 2 | 5 | 3 | 4 | 1 | 6 |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Т | Н | П | В | Е | Г | Л |  | Г | Н | В | Е | П | Л | Т |
| Е | А | Р | А | Д | О | Н |  | О | А | А | Д | Р | Н | Е |
| Р | Т | И | Е | Ь | В | О |  | В | Т | Е | Ь | И | О | Р |
| М | О | Б | Т | М | П | Ч |  | П | О | Т | М | Б | Ч | М |
| И | Р | Ы | С | О | О | Ь |  | О | Р | С | О | Ы | Ь | И |

При считывании содержимого правой таблицы по строкам и записи шифротекста группами по пять букв получим шифрованное сообщение:

«ГНВЕП ЛТООА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ».

Магические квадраты

Применялись в средние века. В те времена считалось, что созданные с помощью магических квадратов шифротексты охраняет не только ключ, но и магическая сила. В качестве ключевой информации используются особенности структуры таблицы.

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Пример магического квадрата и его заполнения сообщением ПРИЛЕТАЮ ВОСЬМОГО:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 3 | 2 | 13 |  | О | И | Р | М |
| 5 | 10 | 11 | 8 |  | Е | О | С | Ю |
| 9 | 6 | 7 | 12 |  | В | Т | А | Ь |
| 4 | 15 | 14 | 1 |  | Л | Г | О | П |

Шифротекст, получаемый при считывании содержим правой таблицы по строкам, имеет вполне загадочный вид:

ОИРМ ЕОСЮ ВТАЬ ЛГОП

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3х3 (если не учитывать его повороты). Количество магических квадратов 4х4 состав­ляет уже 880, а количество магических квадратов 5х5 - около 250000.

Магические квадраты средних и больших размеров могли служить хорошей базой для обеспечения нужд шифрования того времени, поскольку практически нереально выполнить вручную пepe6op всех вариантов для такого шифра.

Шифрующие таблицы с двойной перестановкой.

Для обеспечения дополнительной стойкости можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровывании порядок перестановок должен быть обратным.

Табличные шифры замены.

Полибианский квадрат.

Относится к шифрам простой замены, в которых буквы исходного текста заменяются по определенному правилами другими буквами того же алфавита. Одним из первых шифров простой замены считается так называемый полибианский квадрат. За два века до нашей эры греческий полководец и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5х5, заполненную буквами алфавита в случайном порядке.

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывалась в нижней строке таблицы, то для шифротекста брали самую верхнюю букву из того же столбца. Концепция полибианского квадрата оказалась плодотворной и нашла применение в криптосистемах последующего времени.

Шифрующие таблицы Трисемуса.

В 1508 г. аббат из Германии Иоганн Трисемус напи­сал пе­чатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шиф­рующих таблиц, заполненных алфави­том в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово. В таблицу сначала вписывалось по строкам ключевое слово, при­чем повторяющиеся буквы отбрасывались. Затем эта таблица до­полнялась не вошедшими в нее буквами алфавита по порядку.

При шифровании находят в этой таблице очередную букву открытого текста и запи­сывают в шифротекст букву, располо­женную ниже ее, в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифротекста берут самую верхнюю букву из того же столбца.

*Пример.* Для русско­го алфавита шифрующая таблица может иметь размер 4x8. Вы­бе­рем в качестве ключа слово БАНДЕРОЛЬ. Шифрующая таблица примет вид:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Б | А | Н | Д | Е | Р | О | Л |
| Ь | В | Г | Ж | 3 | И | И | К |
| М | П | С | Т | У | Ф | X | Ц |
| Ч | Ш | Щ | Ы | Ъ | Э | Ю | Я |

При шифровании с помощью этой таблицы

со­общения В Ы Л Е Т А Е М П Я Т О Г О

получаем шифротекст П Д К З Ы В З Ч Ш Л Ы Й С Й

Шифр Уинстона.

В 1854 г. англичанин Чарльз Уитстон разработал новый метод шиф­ро­вания биграммами, который называют "двойным квадра­том". Свое название этот шифр получил по аналогии с полибианским квадратом. В отличие от полибианского шифр "двой­ной квадрат" использует сразу две таблицы, размещенные по од­ной горизонтали, а шифрование идет биграммами (парами). Эти не столь сложные модификации привели к появ­лению на свет качественно новой криптографической систе­мы ручного шифрования. Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы вто­рой мировой войны.

Перед шифрованием исход­ное сообщение разбивают на биграммы. Каждая биграмма шиф­руется отдельно. Первую букву биграммы находят в левой табли­це, а вторую букву - в правой таблице. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противо­положных вершинах. Другие две вершины этого прямоу­гольника дают буквы биграммы шифротекста.

Если обе буквы биграммы сообщения лежат в одной стро­ке, то и буквы шифротекста берут из этой же строки. Первую букву биграммы шифротекста берут из левой таблицы в столбце, соот­ветствующем второй букве биграммы сообщения. Вторая же буква биграммы шифротекста берется из правой таблицы в столбце, со­ответствующем первой букве биграммы сообщения.

*Пример.* Пусть имеются две таблицы размером со случайно расположен­ными в них русскими алфавитами.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ж | Щ | Н | Ю | Р |  | И | Ч | Г | Я | Т |
| И | Т | Ь | Ц | Б |  | 1 | Ж | Ь | М | О |
| Я | М | Е | . | С |  | 3 | Ю | Р | В | Щ |
| В | Ы | П | Ч |  |  | Ц | : | П | Е | Л |
| : | Д | У | О | К |  | Ъ | А | Н | . | X |
| 3 | Э | Ф | Г | Ш |  | Э | К | С | Ш | Д |
| X | А | 1 | Л | Ъ |  | Б | Ф | У | Ы |  |

Рис. Две таблицы со случайно расположенными символами русского алфавита для шифра "двойной квадрат

Предположим, что шифруется биграмма исходного текста ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифротекста входят буква О, расположенная в столб­це 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифротекста ОВ.

Если обе буквы биграммы сообщения лежат в одной стро­ке, например ТО, то биграмма сообщения ТО превращается в биграмму шифротекста ЖБ. Аналогичным образом шифруются все биграммы сообщения:

Сообщение ПР ИЛ ЕТ АЮ \_Ш ЕС ТО ГО

Шифротекст ПЕ ОВ ЩН ФМ ЕШ РФ БЖ ДЦ

Шифрование методом "двойного квадрата" дает весьма устой­чивый к вскрытию и простой в применении шифр. Взламывание шифротекста "двойного квадрата" требует больших усилий, при этом длина сообщения должна быть не менее тридцати строк.

Порядок выполнения работы:

1. Разработать алгоритмы шифрования и дешифрования блока (потока) открытого текста заданной длины из алфавита Z на заданном ключе с помощью метода, указанного в варианте.
2. Определить алфавит криптосистемы (открытого текста и шифротекста). Если алфавит не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII.
3. Написать программу/модуль, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифротекст должны быть представлены отдельными файлами.
4. Написать программу/модуль для реализации алгоритма расшифрования полученного файла шифротекста при известном ключе.
5. Провести тестирование программы на коротких и длинных тестовых примерах

Контрольные вопросы:

1. Что такое ключ?
2. Объясните понятие алфавит?
3. Нарисуйте общую схему системы, использующей симметричное шифрование;
4. Перечислите основные методы шифрования с закрытым ключом;
5. В чём заключается суть режима работы блочного шифра «сцепление блоков шифра»?

# Лабораторная работа №2

Исследование методов криптоанализа симметричных систем шифрования

Цель работы: сформировать практические навыки применения методов криптоанализа симметричных систем шифрования.

Задачи: Изучить способы оценки практической стойкости алгоритма. Разработать алгоритмы и реализовать программы, использующие алгоритмы криптоанализа для определения параметров алгоритма шифрования, необходимые для оценки практической криптостойкости.

Требования к отчету.

Отчет по лабораторной работе должен содержать:

1. Титульный лист установленного образца.
2. Постановку задачи.
3. Описание хода выполнения работы
4. Вывод

Длительность работы:8 академических часов.

Защита работы: собеседование с преподавателем по контрольным вопросам.

Задание: Разработать и реализовать алгоритмы криптоанализа для оценки практической стойкости алгоритма, разработанного в лабораторной работе №1.

Теоретические сведения

Способность шифра противостоять всевозможным атакам на него называют стойкостью шифра. Понятие стойкости шифра является центральным для криптогра­фии. Важнейшим для развития криптографии был результат К. Шен­нона о существовании и единственности абсолютно стойкого шифра. Но абсолютно стойкий шифр на практике, как правило, неприменим, поэтому для защиты своей информа­ции законные пользователи вынуждены применять не абсолютно стой­кие шифры. Такие шифры, по крайней мере теоретически, могут быть вскрыты, то есть противник с неогра­ниченными ресурсами может вскрыть любой не­ абсолютно стойкий шифр. Вопрос толь­ко в том, хватит ли у него сил, средств и времени для разработки и реализации соответствующих ал­горитмов.

В этой ситуации желательно, получить теоретическую оценку стойкости, то есть, например, дока­зать, что никакой противник не сможет вскрыть выбранный шифр, ска­жем, за 24 часа. К сожалению, математическая теория ещё не даёт нужных теорем — они относятся к нерешённой проблеме нижних оценок вычислительной сложности задач.

Поэтому у пользователя остаётся единственный путь — получение практических оценок стойкости. Этот путь состоит в том, чтобы определить от какого противника мы соби­раемся защищать информацию, а также какие силы и средства он сможет применить для его вскрытия. Затем, мысленно стать в положение противника и пытаться с его позиций атаковать шифр, т.е. разрабатывать различные алгоритмы вскрытия шифра, а наилучший из этих алгоритмов использовать для прак­тической оценки стойкости шифра. В общем случае все оценки стойкости системы должны вестись в предпо­ложении, что криптоаналитику известен алгоритм шифрования, но он не знает ключа, на котором зашифровано конкретное сообщение. Противник также может знать некоторые характери­стики открытых текстов, например, общую те­матику сообщений, некоторые стандарты, форматы и т. д.

Итак, стойкость конкретного шифра оценивается только путём все­возможных попыток его вскрытия и зависит от квалификации криптоана­литиков, атаку­ющих шифр. Такую процедуру иногда называют проверкой стойкости. Имеется несколько показателей криптостойкости, среди кото­рых основные:

количество всех возможных ключей;

среднее время, необходимое для криптоанализа.

В данной работе мы будем защищаться от пассивной атаки с известной шифрограммой, когда противник может перехватывать все шифрованные сообщения, но не имеет соответствующих им открытых текстов. Задача криптоаналитика заключается в том, чтобы раскрыть исходные тексты и вычислить ключ.

Для этого рекомендуется использовать один из двух простейших мето­дов вскрытия шифра

1. Статистическую атаку.
2. Силовую атаку.

Силовая атака

Силовая атака заключается в подборе ключа шифрования путем перебора подряд всех возможных ключей вплоть до нахождения истинного. В отличие от всех других методов эта атака применима для всех типов шифров, но она имеет максимальную сложность реализации и, соответственно, требует максимальных затрат времени и средств.

Алгоритм криптоанализа заключается в следующем: определяется множество всех возможных ключей шифрования для данной криптосистемы и для каждого ключа выполняются шаги:

1. Дешифрование известного шифротекста на этом ключе;
2. Анализ «осмысленности» полученного предполагаемого открытого текста, например, путем поиска соответствующих слов в словаре возможных сообщений;
3. Принятие решения об истинности найденного ключа на основе результатов предыдущих шагов дешифрования.

Данный метод работает тем медленнее, чем больше длина шифротекста, используемого для криптоанализа.

Криптоаналитическая статистическая атака

Криптоаналитическая статистическаяатака применима только против систем одноалфавитной замены, главным недостатком которых является возможность взлома шифротекста на основе анализа частот появления букв. Такая атака начинается с подсчета частот появления символов:

1. определяется число появлений каждой буквы в шифротексте.
2. полученное распределение частот букв в шифротексте сравнивается с распределением частот букв в алфавите исходных сообщений, например в английском.
3. буква с наивысшей частотой появления в шифротексте заменяется на букву с наивысшей частотой появления в английском языке и т.д.

По закону больших чисел вероятность успешного вскрытия системы шифрования повыша­ется с увеличением длины шифротекста.

Таблица вероятностей букв в русских текстах.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| буква | пробел | о | е или ё | а | и | н | т | с | р | в | л |
| вер-ть | 0,175 | 0,090 | 0,072 | 0,062 | 0,062 | 0,053 | 0,053 | 0,045 | 0,040 | 0,038 | 0,035 |
| буква | к | м | д | п | у | я | з | ы | б | ь или ъ | г |
| вер-ть | 0,028 | 0,026 | 0,025 | 0,023 | 0,021 | 0,018 | 0,016 | 0,016 | 0,014 | 0,014 | 0,013 |
| буква | ч | й | х | ж | ш | ю | ц | щ | э | ф |  |
| вер-ть | 0,012 | 0,010 | 0,009 | 0,007 | 0,006 | 0,006 | 0,004 | 0,003 | 0,003 | 0,002 |  |

Таблица вероятностей букв в английских текстах.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| буква | пр-л | **е** | **t** | **а** | **о** | **n** | **i** | **s** | **r** |
| вер-ть | 0,185 | 0,097 | 0,076 | 0,064 | 0,062 | 0,057 | 0,056 | 0,052 | 0,047 |
| буква | **h** | **l** | **d** | **с** | **u** | **p** | **f** | **м** | **w** |
| вер-ть | 0,04 | 0,031 | 0,028 | 0,025 | 0,018 | 0,018 | 0,018 | 0,017 | 0,016 |
| буква | **y** | **в** | **g** | **v** | **к** | **q** | **x** | **j** | **z** |
| вер-ть | 0,015 | 0,013 | 0,013 | 0,007 | 0,039 | 0,002 | 0,002 | 0,001 | 0,001 |



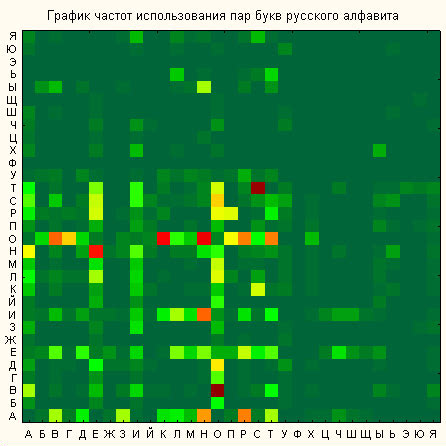


Устойчивыми являются также частотные характеристики биграмм, триграмм и четырехграмм осмысленных текстов.

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравномерность k-грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО   
СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.



Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве.

Порядок выполнения работы:

Считать, что противнику известен алгоритм шифрования. Выбрать наилучший с его точки зрения алгоритм подбора ключа и обосновать свой выбор. Использовать методы:

1. анализа статистических свойств шифротекста (частот появления букв).
2. силовую атаку (полный перебор ключей).
3. другие (если есть более эффективные)

С помощью программы, реализующей выбранный алгоритм крип­тоана­лиза провести эксперимент по вскрытию шифротекс­тов различного размера.

При использовании статистического криптоанализа исполь­зовать табли­цы, приведенные выше или подсчитать частоты появления букв используемого алфавита в тексте, частью которого является текст примера.

Для проверки на «осмысленность» полученного текста создать мини-словарь из части слов, встречающихся в тексте примера.

В результате эксперимента определить параметры алгоритма шифрования (размер передаваемого текста, размер и характеристи­ки ключа, объем ключевого пространства и другие параметры алгоритма шифрования), необходимые для оценки практической криптостойкости разработанного в лабораторной работе №1 алгоритма шифрования.

Построить графики зависимости времени криптоанализа от параметров ал­горитма шифрования (длины или других параметров ключа, размера шифротекста или др., в зависимости от алгоритмов шифрования и криптоанализа).

Практической криптостойкостью в данной работе будем считать невозможность взлома шифра противником, имеющим в распоряжении один ПК мощности, равной мощности компьютера, на котором делалась работа и 30 минут времени.

Контрольные вопросы:

1. Перечислите виды криптографических атак?
2. Объясните понятие активная криптографическая атака?
3. Какие существуют методы вскрытия шифров?
4. Что называется криптостойкостью?
5. В каких случаях наиболее эффективной является статистическая атака?