

Лабораторная работа 1. Простые шифры

1.1. Цель работы

Ознакомление с простыми симметричными криптографическими шифрами на основе методов подстановок, перестановок и гаммирования.

1.2. Общие сведения

1.2.1. Классификация шифров

1.2.1.1. Классификация по ключевой информации

Первым принципиальным признаком, позволяющим произвести разделение шифров, является объем информации, неизвестной третьей стороне. В том случае, когда злоумышленнику полностью неизвестен алгоритм выполненного над сообщением преобразования, шифр называется *тайнописью*.

В отличие от тайнописи *криптографией с ключом* называют сегодня алгоритмы шифрования, в которых сам алгоритм преобразований широко известен и доступен для исследований каждому желающему, но шифрование производится на основе небольшого объема информации — *ключа*, известного только отправителю и получателю ключа.

В некоторых (наиболее простых) случаях ключ формирует человек, отправляющий сообщение, в отдельных ключ создается автоматически с помощью программного обеспечения или даже запрашивается у удаленной базы данных ключей. В современной криптографии в зависимости от методик размер ключа составляет от 56 до 4096 бит. Запоминать ключ, который является на самом деле просто большой последовательностью чисел, обычному человеку довольно сложно хоть в двоичной, хоть в десятичной записи. Поэтому все современные системы предлагают пользователю вводить не ключ — набор цифр, а пароль — произвольную текстовую фразу. Пароль может состоять из одного или нескольких слов, быть осмысленным или нет, главное — чтобы он легко запоминался пользователем.

1.2.1.2. Симметричное/асимметричное шифрование

Все криптоалгоритмы с ключом делятся на *симметричные* и *асимметричные*. В *симметричных криптоалгоритмах* ключи, используемые на передающей и приёмной сторонах, полностью идентичны. Такой ключ несет в себе всю информацию о засекречивании сообщения и поэтому не должен быть известен никому, кроме двух участвующих в

разговоре сторон. Поэтому в отношении ключа симметричных систем часто называются *шифрами на секретном ключе*.

Симметричное шифрование можно применять как при отправке сообщений между двумя пользователями, разделенными большим расстоянием, так и при отправке «последний» одним и тем же пользователем самому себе, но во времени. Примером подобных отправок является шифрование файлов на жестких дисках и сменных носителях с тем, чтобы другие пользователи тех же ЭВМ не могли считать информацию в отсутствие владельца.

В асимметричном шифровании для шифрования применяется один ключ, а для дешифрования — другой. Дело в том, что процедура шифрования в асимметричных системах устроена таким образом, что ни одно постороннее лицо не может, зная зашифрованный таким способом текст и ключ шифрования, восстановить исходный текст. Прочитать зашифрованный текст можно, только зная ключ дешифрования. А раз так, то ключ шифрования может быть известен всем пользователям сети — его раскрытие не нанесет никакого урона переписке. Поэтому ключ шифрования в асимметричных системах называется *открытым ключом*. Ключ дешифрования необходимо держать в строгом секрете, как и секретный ключ симметричных систем. Поэтому он носит название *закрытого ключа*, а сами асимметричные системы получили еще одно название — *шифры на открытом ключе*.

1.2.1.3. Поточное/блочное шифрование

Следующим критерием классификации шифров является схема обработки ими потока информации. Согласно ему, симметричные криптоалгоритмы делятся на *поточные* и *блочные* шифры. *Поточный шифр* способен обрабатывать информацию побитно, т. е. подобная схема может, получив порцию из произвольного количества бит (может быть, даже одного), зашифровать/дешифровать ее и передать для дальнейшей обработки другим модулям. Подобная схема очень удобна в каналах последовательной связи, где сам процесс передачи информации может обрываться в произвольный момент и затем через некоторый промежуток времени продолжаться дальше.

Однако побитовая обработка информации является очень медленной в тех случаях, когда вычислительная техника имеет возможности для параллельной обработки (то есть программной реализации). Разрядность основной массы современных процессоров равна 32 битам, существуют 64- и 80-разрядные аппаратные платформы. В этих условиях, особенно тогда, когда информация все равно переносится в буфер в том или ином объеме (пакеты в компьютерных сетях, файлы на носителях), гораздо выгоднее применять совершенно другие принципы криптографических преобразований, называемые *блочными шифрами*.

В блочных шифрах преобразования могут применяться только над

информацией строго определенного объема. Размер блока на сегодняшний день равен 64, 126 или 256 битам. Частичное шифрование (например, попытка обработать 177 бит) невозможно. Блочное шифрование получило гораздо более широкое распространение из-за развития современной вычислительной техники, и, если поточные шифры одинаково часто реализуются как программно, так и аппаратно, то блочные шифры в подавляющем большинстве реализуются программно.

1.2.2. Используемые операции

1.2.2.1. Подстановочные шифры

Подстановочным шифром называется шифр, который каждый символ открытого текста в шифротексте заменяет другим символом. Получатель инвертирует подстановку шифротекста, восстанавливая открытый текст. В классической криптографии существует четыре типа подстановочных шифров:

- простой подстановочный шифр, или моноалфавитный шифр, — это шифр, который каждый символ открытого текста заменяет соответствующим символом шифротекста. Простыми подстановочными шифрами являются криптограммы в газетах;
- одновзвучный подстановочный шифр похож на простую подстановочную криптосистему за исключением того, что один символ открытого текста отображается на несколько символов шифротекста. Например, «А» может соответствовать 5, 13, 25 или 56, «В» — 7, 19, 31 или 42 и так далее;
- полиграммный подстановочный шифр — это шифр, который блоки символов шифрует по группам. Например, «АВА» может соответствовать «RTQ», «АВВ» может соответствовать «SLL» и так далее;
- полиалфавитный подстановочный шифр состоит из нескольких простых подстановочных шифров. Например, могут быть использованы пять различных простых подстановочных фильтров; каждый символ открытого текста заменяется с использованием одного конкретного шифра.

Знаменитый шифр Цезаря, в котором каждый символ открытого текста заменяется символом, находящегося тремя символами правее по модулю 26 («А» заменяется на «D», «В» — на «Е», «W» — на «Z», «X» — на «A», «Y» — на «B», «Z» — на «C»), представляет собой простой подстановочный фильтр. Он действительно очень прост, так как алфавит шифротекста представляет собой смещённый, а не случайно распределённый алфавит открытого текста.

1.2.2.2. Перестановочные шифры

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется шифром перестановки (ШП). Рассмотрим преобразование из ШП, предназначенное для шифрования сообщения длиной n символов. Его можно представить с помощью таблицы

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix} \quad (1.1)$$

где i_1 – номер места шифротекста, на которое попадает первая буква исходного сообщения при выбранном преобразовании, i_2 – номер места для второй буквы и т. д.

В верхней строке таблицы выписаны по порядку числа от 1 до n , а в нижней те же числа, но в произвольном порядке. Такая таблица называется подстановкой степени n .

Зная подстановку, задающую преобразование, можно осуществить как шифрование, так и расшифрование текста. Например, если для преобразования используется подстановка

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 1 & 4 & 6 \end{bmatrix}$$

и в соответствии с ней зашифровывается слово МОСКВА, то получится КОСВМА.

Попробуйте расшифровать сообщение НЧЕИУК, полученное в результате преобразования с помощью указанной выше подстановки.

Зная метод математической индукции, легко убедиться в том, что существует $n!$ вариантов заполнения нижней строки таблицы (1.1). Таким образом, число различных преобразований шифра перестановки, предназначенного для зашифрования сообщений длины n , меньше либо равно $n!$.

Примером ШП, предназначенного для шифрования сообщений длины n , является шифр, в котором в качестве множества ключей взято множество всех подстановок степени n , а соответствующие им преобразования шифра задаются, как было описано выше. Число ключей такого шифра равно $n!$

Для использования на практике такой шифр неудобен, так как при больших значениях n приходится работать с длинными таблицами.

Широкое распространение получили фигуры перестановки, использующие некоторую геометрическую фигуру. Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называется *маршрутной перестановкой*. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав

такой маршрут: по горизонтали, начиная с левого верхнего поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, указанным способом фразу:

ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

используя прямоугольник размера 4×7

| | | | | | | |
|---|---|---|---|---|---|---|
| П | Р | И | М | Е | Р | М |
| Н | Т | У | Р | Ш | Р | А |
| О | Й | П | Е | Р | Е | С |
| И | К | В | О | Н | А | Т |

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.

Для использования шифра, называемого *поворотной решёткой*, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера $2m \times 2k$ клеток. В трафарете вырезано $m \times k$ клеток так, что при наложении его на лист чистой бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Пример шифрования. Пусть в качестве ключа используется решётка 6×10 (рис. 1.1).

Зашифруем с ее помощью текст

ШИФРРЕШЁТКАЯВЛЯЕТСЯ ЧАСТНЫМЛУЧАЕМШИФРАМАРШРУТНОЙ ПЕРЕСТАНОВКИ

Наложив решетку на лист бумаги, вписываем первые 15 (по числу вырезов) букв сообщения ШИФРРЕШЁТКАЯВЛЯ. Сняв решетку, мы увидим текст, представленный на рис. 1.2. Поворачиваем решётку на 180° . В окошечках появятся новые, еще не заполненные клетки. Вписываем в них следующие 15 букв. Получится запись, приведенная на рис. 1.3. Затем поворачиваем решетку на другую сторону и зашифровываем остаток текста аналогичным образом (рис. 1.4, 1.5).

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифротекст по порядку четырьмя способами. Можно доказать, что число возможных

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| × | | × | × | × | × | × | × | × | × |
| | × | × | × | | × | | | × | × |
| × | | × | × | × | | × | × | × | |
| × | × | × | | × | × | × | | × | × |
| × | | × | × | × | × | × | × | × | × |
| × | × | | × | × | | | × | × | |

Рис. 1.1. Поворотная решётка

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| × | Ш | × | × | × | × | × | × | × | × |
| И | × | × | × | Ф | × | Р | Р | × | × |
| × | Е | × | × | × | Ш | × | × | × | Ё |
| × | × | × | Т | × | × | × | К | × | × |
| × | А | × | × | × | × | × | × | × | × |
| × | × | Я | × | × | В | Л | × | × | Я |

Рис. 1.2. Первая итерация

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | × | Т | С | × | × | × | × | × |
| И | × | × | × | Ф | × | Р | Р | Ч | × |
| × | Е | А | × | × | Ш | С | × | × | Ё |
| × | × | × | Т | × | × | × | К | × | × |
| × | А | × | × | × | × | × | × | × | × |
| × | × | Я | × | × | В | Л | × | × | Я |

Рис. 1.3. Вторая итерация

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | А | Т | С | Е | М | Я | × | Ш |
| И | И | × | × | Ф | × | Р | Р | Ч | × |
| × | Е | А | Ф | × | Ш | С | Р | × | Ё |
| Т | А | × | Т | Н | М | × | К | Ы | А |
| Р | А | М | С | Ш | Л | Р | У | × | У |
| × | Т | Я | × | × | В | Л | × | Ч | Я |

Рис. 1.4. Третья итерация

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | А | Т | С | Е | М | Я | Н | Ш |
| И | И | О | Й | Ф | П | Р | Р | Ч | Е |
| Р | Е | А | Ф | Е | Ш | С | Р | С | Ё |
| Т | А | Т | Т | Н | М | × | К | Ы | А |
| Р | А | М | С | Ш | Л | Р | У | Н | У |
| О | Т | Я | В | К | В | Л | И | Ч | Я |

Рис. 1.5. Четвёртая итерация

трафаретов, то есть количество ключей шифра «решётка», составляет $= 4^{mk}$. Этот шифр предназначен для сообщений длины $n = 4mk$. Число всех перестановок в тексте такой длины составит $(4mk)!$, что во много раз больше числа. Однако, уже при размере трафарета 8×8 число возможных решеток превосходит 4 миллиарда.

Шифром вертикальной перестановки (ШВП) называется широко распространенная разновидность шифра маршрутной перестановки. В нем используется прямоугольник, в котором сообщение вписывается обычным способом (по строкам слева направо). Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом. Пусть, например, этот ключ таков: $(5, 1, 4, 7, 2, 6, 3)$, и с его помощью надо зашифровать сообщение:

ВОТПРИМЕРШИФРАВЕРТИКАЛЬНОЙПЕРЕСТАНОВКИ

Впишем сообщение в прямоугольник, столбцы которого пронумерованы в соответствии с ключом:

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 1 | 4 | 7 | 2 | 6 | 3 |
| В | О | Т | П | Р | И | М |
| Е | Р | Ш | И | Ф | Р | А |
| В | Е | Р | Т | И | К | А |
| Л | Ь | Н | О | Й | П | Е |
| Р | Е | С | Т | А | Н | О |
| В | К | И | - | - | - | - |

Теперь, выбирая столбцы в порядке, заданном ключом и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

ОРЕЪЕРФИЙА-МААЕО-ТШРНСИВЕВЛРВРКПН-ПИТОТ-

Число ключей ШВП не более $m!$, где m — число столбцов таблицы. Как правило, m гораздо меньше, чем длина текста n (сообщение

укладывается в несколько строк по m букв), а значит, и $m!$ много меньше $n!$.

В случае, когда ключ ШВП не рекомендуется записывать, его можно извлекать из какого либо запоминающегося слова или предложения. Для этого существует много способов. Наиболее распространенный состоит в том, чтобы приписывать буквам числа в соответствии с обычным алфавитным порядком букв. Например, пусть ключевым словом будет ПЕРЕСТАНОВКА. Присутствующая в нем буква А получает номер 1. Если какая-то буква входит несколько раз, то ее появление нумеруется последовательно слева направо. Поэтому второе вхождение буквы А получает номер 2. Поскольку буквы Б в этом слове нет, то буква В получает номер 3 и так далее. Процесс продолжается до тех пор, пока все буквы не получают номера. Таким образом, мы получаем следующий ключ:

| | | | | | | | | | | | |
|---|---|----|---|----|----|---|---|---|---|---|---|
| П | Е | Р | Е | С | Т | А | Н | О | В | К | А |
| 9 | 4 | 10 | 5 | 11 | 12 | 1 | 7 | 8 | 3 | 6 | 2 |

1.2.2.3. Гаммирование

Гаммирование также является широко применяемым криптографическим преобразованием. Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым образом (например, используя сложение по модулю 2).

Процесс дешифрования данных сводится к повторной генерации гаммы шифра при известном ключе и обращении процесса наложения такой гаммы на зашифрованные данные.

Для программной генерации гаммы шифра необходимо воспользоваться датчиком псевдослучайных чисел. Наиболее простым для реализации является генератор линейной конгруэнтной последовательности:

$$T_{i+1} = (AT_i + C) \bmod m.$$

Такой датчик ПСЧ генерирует псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений A и C . Значение m обычно устанавливается равным $2n$, где n — длина машинного слова в битах. Датчик имеет максимальный период M до того, как генерируемая последовательность начнет повторяться. По причине, отмеченной ранее, необходимо выбирать числа A и C такие, чтобы период M был максимальным. Как показано Д. Кнудом, линейный конгруэнтный датчик ПСЧ имеет максимальную длину тогда и только тогда, когда C — нечётное, и $A \bmod 4 = 1$.

1.3. Порядок выполнения лабораторной работы

Порядок выполнения лабораторной работы заключается в следующем:

1. Ознакомиться с разделами методических указаний к данной лабораторной работе.
2. Получить у преподавателя вариант (варианты) заданий на исследование описанных выше шифров.
3. Составить контрольный пример.
4. Разработать и реализовать заданный(е) алгоритм(ы) шифрования/дешифрования.
5. На контрольном примере проверить правильность работы алгоритмов шифрования и дешифрования.
6. Составить отчёт.

1.4. Содержание отчета о выполненной работе

Отчёт должен содержать следующие разделы:

1. Название и цель работы.
2. Описание алгоритма.
3. Реализация алгоритма (псевдокод и код программы).
4. Результаты работы программы с различными исходными текстами, ключами и другими параметрами.
5. Ответы на контрольные вопросы.

1.5. Варианты заданий

Реализовать следующих варианты алгоритмов шифрования/дешифрования:

1. Шифр Цезаря. Аффинная система перестановок Цезаря.
2. Квадрат Полибия (5×5 , 5×6 , 4×7 , 6×6 , 5×7 и т. д.). Квадрат Кардано ($N \times N$).
3. Шифр многоалфавитной замены (Вижинера).
4. Шифр маршрутной перестановки.
5. Шифр поворотной решётки.
6. Шифр вертикальной перестановки.
7. Поточные шифры. Шифры гаммирования. Линейные регистры сдвига.
8. Шифр Вернама.

1.6. Контрольные вопросы

1. Какой шифр называется шифром подстановки?

-
2. Какой шифр называется шифром перестановки?
 3. Какой шифр называется поворотной решёткой?
 4. Какой шифр называется шифром вертикальной перестановки?
 5. К какому классу шифров относится шифр Цезаря?