**Лабораторная работа №11**

**Тема: «Методы шифрования с закрытым ключом»**

**Цель: получить практические навыки работы по шифрованию методами с закрытым ключом**

Известны разные методы шифрования с закрытым ключом рис. 1. На практике часто используются алгоритмы перестановки, подстановки, а также комбинированные методы.

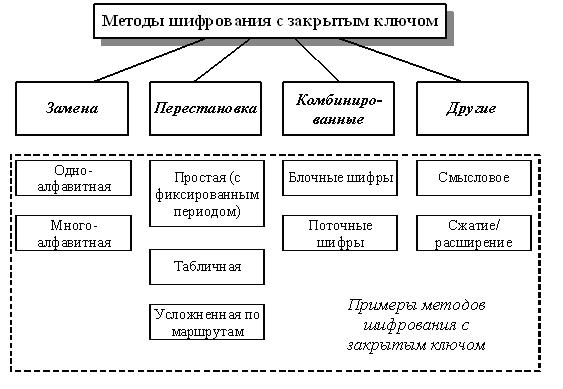


Рис. 1. Методы шифрования с закрытым ключом

В методах перестановки символы исходного текста меняются местами друг с другом по определенному правилу. В методах замены (или подстановки) символы открытого текста заменяются некоторыми эквивалентами шифрованного текста. С целью повышения надежности шифрования, текст, зашифрованный с помощью одного метода, может быть еще раз зашифрован с помощью другого метода. В этом случае получается комбинированный или композиционный шифр. Применяемые на практике в настоящее время блочные или поточные симметричные шифры также относятся к комбинированным, так как в них используется несколько операций для зашифрования сообщения.

Основное отличие современной криптографии от криптографии "докомпьютерной" заключается в том, что раньше криптографические алгоритмы оперировали символами естественных языков, например, буквами английского или русского алфавитов. Эти буквы переставлялись или заменялись другими по определенному правилу. В современных криптографических алгоритмах используются операции над двоичными знаками, то есть над нулями и единицами. В настоящее время основными операциями при шифровании также являются перестановка или подстановка, причем для повышения надежности шифрования эти операции применяются вместе (комбинируются) и помногу раз циклически повторяются.

**Методы замены**

Методы шифрования заменой (подстановкой) основаны на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.

**Одноалфавитная замена**

Одним из важных подклассов методов замены являются одноалфавитные (или моноалфавитные) подстановки, в которых устанавливается однозначное соответствие между каждым знаком ai исходного алфавита сообщений A и соответствующим знаком ei зашифрованного текста E. Одноалфавитная подстановка иногда называется также простой заменой, так как является самым простым шифром замены.

Примером одноалфавитной замены является шифр Цезаря, рассмотренный ранее. В рассмотренном в "Основные понятия криптографии" примере первая строка является исходным алфавитом, вторая (с циклическим сдвигом на k влево) – вектором замен.

В общем случае при одноалфавитной подстановке происходит однозначная замена исходных символов их эквивалентами из вектора замен (или таблицы замен). При таком методе шифрования ключом является используемая таблица замен.

**Методы перестановки**

При использовании шифров перестановки входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов. Перестановки в классической "докомпьютерной" криптографии получались в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры.

Простейшим примером перестановки является перестановка с фиксированным периодом d. В этом методе сообщение делится на блоки по d символов и в каждом блоке производится одна и та же перестановка. Правило, по которому производится перестановка, является ключом и может быть задано некоторой перестановкой первых d натуральных чисел. В результате сами буквы сообщения не изменяются, но передаются в другом порядке.

Например, для d=6 в качестве ключа перестановки можно взять 436215. Это означает, что в каждом блоке из 6 символов четвертый символ становится на первое место, третий – на второе, шестой – на третье и т.д. Пусть необходимо зашифровать такой текст:

ЭТО\_ТЕКСТ\_ДЛЯ\_ШИФРОВАНИЯ

Количество символов в исходном сообщении равно 24, следовательно, сообщение необходимо разбить на 4 блока. Результатом шифрования с помощью перестановки 436215 будет сообщение

\_ОЕТЭТ\_ТЛСКДИШР\_ЯФНАЯВОИ

Теоретически, если блок состоит из d символов, то число возможных перестановок d!=1\*2\*...\*(d-1)\*d. В последнем примере d=6, следовательно, число перестановок равно 6!=1\*2\*3\*4\*5\*6=720. Таким образом, если противник перехватил зашифрованное сообщение из рассмотренного примера, ему понадобится не более 720 попыток для раскрытия исходного сообщения (при условии, что размер блока известен противнику).

Для повышения криптостойкости можно последовательно применить к шифруемому сообщению две или более перестановки с разными периодами.

Другим примером методов перестановки является перестановка по таблице. В этом методе производится запись исходного текста по строкам некоторой таблицы и чтение его по столбцам этой же таблицы. Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом.

**Вопросы для самопроверки**

1. Поясните общую схему симметричного шифрования.
2. Что общего имеют все методы шифрования с закрытым ключом?
3. Назовите основные группы методов шифрования с закрытым ключом.
4. Приведите примеры шифров перестановки.
5. Сформулируйте общие принципы для методов шифрования подстановкой.
6. В чем заключаются многоалфавитные подстановки?
7. Приведите пример шифра одноалфавитной замены.
8. Опишите алгоритм любого метода шифрования перестановкой. Приведите пример шифрования некоторого сообщения этим методом. Каков алгоритм расшифрования в этом методе?
9. К какой группе методов шифрования с закрытым ключом относится метод с использованием таблицы Вижинера? Каковы алгоритмы шифрования и расшифрования в этом методе? Приведите пример шифрования некоторого сообщения этим методом.
10. Каким образом можно зашифровать и расшифровать сообщение методом табличной перестановки, если размер шифруемого сообщения не кратен размеру блока?
11. Что такое монофонические шифры?

**Практические задания**

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.



Расшифруйте сообщения, зашифрованные с помощью шифра №1

* И.РЮУ.ЪФОБГНО
* CЛХГ.ЪЛХО.ФОО.ЩВ

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.



Расшифруйте сообщения, зашифрованные с помощью шифра №2:

\bigtriangledown * ! ( \infty \blacklozenge № > \sharp \oplus

@ \spadesuit - \heartsuit \infty \bigtriangledown * ! (-) \sharp *\Delta

1. Пусть исходный алфавит содержит следующие символы:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:

КРИПТОСТОЙКОСТЬ

ГАММИРОВАНИЕ

1. Пусть исходный алфавит состоит из следующих знаков (символ "\_" (подчеркивание) будем использовать для пробела):

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ\_

Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:

ШВМБУЖНЯ

ЯБХЪШЮМХ

1. Первый байт фрагмента текста в шестнадцатеричном виде имеет вид А5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде). Что получится после шифрования?
2. Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9А. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Какой ключ использовался при шифровании?
3. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:

ЖЕЛТЫЙ\_ОГОНЬ

МЫ\_НАСТУПАЕМ

1. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:

СЛПИЬНАЕ

РОИАГДВН

1. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:

МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР

СИГНАЛ БОЯ – НИСАГО ЛЯБ

1. Зашифруйте сообщения методом перестановки по таблице 5\*5. Ключ указывает порядок считывания столбцов при шифровании.

ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235)

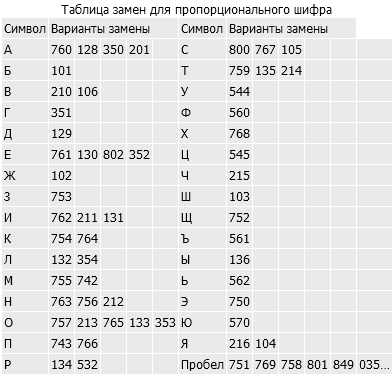
ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)

1. Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4\*4 (символ подчеркивания заменяет пробел). Ключ указывает порядок считывания столбцов при шифровании.

ЕАУПД\_КЕАЗАРЧВ (ключ: 4123)

А\_НСЫИЛБСАЛЙГ (ключ: 3142)

1. Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен:



Расшифруйте указанные сообщения.

* 353214764134136759136762849754128212350354035767106216753211
* 351 761756130532128759353134758105757213101752352763211762