# Лабораторная работа №11

# Методы защиты информации. Шифр простой перестановки.

**Цель работы**: Выполнить шифрование заданного сообщения простейшим шифром перестановок и выполнить проверку правильности шифрования.

# Теоретические сведения

Шифр (cipher) – совокупность алгоритмов или отображений открытой информации, представленной в формализованном виде, в недоступный для восприятия шифрованный текст (также представленный в формализованном виде), который зависит от внешнего параметра (ключа). Не зная ключа, невозможно по шифрованной информации определить открытую информацию, а по шифрованной и открытой информации – ключ.

Ключ (key) – некоторый неизвестный параметр шифра, позволяющий выбрать для шифрования и расшифрования конкретное преобразование из всего множества преобразований, составляющих шифр.

Открытый текст (plain text) – массив незашифрованных данных.

Шифртекст (ciphertext) – массив зашифрованных данных.

Шифрование (Encoding) – процесс создания шифрованного текста при наличии ключа.

Шифратор – аппарат или программа, реализующая шифр.

СКЗИ – средство криптографической защиты информации.

Дешифрование (Decoding) – восстановление открытого текста или ключа из шифрованнного текста.

Существует два основных способа, с помощью которых взламываются системы шифрования:

brute force (грубая сила);

статистический анализ (statistical analysis).

Атаки типа brute force являются самыми простыми по реализации, но требуют больших затрат времени. Они сводятся к попыткам перебрать все возможные ключи шифрования до тех пор, пока данные не будут расшифрованы. По существу это отгадывание значения ключа шифрования.

Шифр блочный (block cipher) – данные шифруются порциями одинакового размера, называемыми блоками, и результат зашифрования очередного блока зависит только от значения этого блока и от значения ключа шифрования, и не зависит от расположения блока в шифруемом массиве и от других блоков массива.

Шифр потоковый (stream cipher, general stream cipher) – результат зашифрования очередной порции данных зависит от самой этой порции и от всех предыдущих данных шифруемого массива.

В важном частном случае он зависит от самой порции данных и от ее позиции в массиве и не зависит от значения предшествующих и последующих порций данных.

Иногда данное условие дополняют требованием, что за один шаг шифруется элементарная структурная единица данных – бит, символ текста или байт.

# Шифр перестановок

Шифр перестановок – заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр /P - permutation/.

Шифр простой перестановки является одним из простейших блочных шифров. Исходное сообщение (открытый текст) разбивается на блоки равного размера.

Если размер текста не кратен размеру блока, в конец сообщения дописывают пробелы, чтобы число знаков в сообщении было кратно размеру блока.

Далее в каждом из блоков (независимо от остальных блоков) символы открытого текста меняются местами. Правило выполнения перестановки и является ключом к шифру.

Данный вариант шифра не является стойким, поскольку размер ключа существенно меньше размера текста.

Кроме того, в зашифрованном тексте сохраняются статистические зависимости между символами. Например, частота появлений отдельных символов в открытом тексте и шифртексте остается постоянной, что облегчает подбор ключа (т.е. взлом шифра).

# Пример использования шифра перестановок

Исходное сообщение "МАМА МЫЛА РАМУ"

Перестановка:

|  |  |
| --- | --- |
| Вместо | Подставить |
| 1 | 2 |
| 2 | 4 |
| 3 | 1 |
| 4 | 3 |

Размер блока: 4 символа (в перестановке участвуют 4 последовательных символа).

Длина текста: 14 символов (размер сообщения не является кратным размеру блока). Разбиение открытого текста на блоки (с добавлением пробелов, для наглядности пробелы изображены символами подчеркивания):

М А М А \_ М Ы Л А \_ Р А М У\_ \_

(блок 1) (блок 2) (блок 3) (блок 4)

***Перестановка в блоке 1:***

Открытый текст: Символ М А М А

Позиция 1 2 3 4

Шифртекст: Символ А А М М

Позиция 2 4 1 3

Перестановка:

А А М М М Л \_ Ы \_ А А Р У \_ М \_

(блок 1) (блок 2) (блок 3) (блок 4)

***Шифртекст:***

«ААМММЛ\_Ы\_ААРУ\_М\_»

Для расшифровки сообщения необходимо применить обратную перестановку.

Прямая перестановка: 1→2, 2→4, 3→1, 4→3

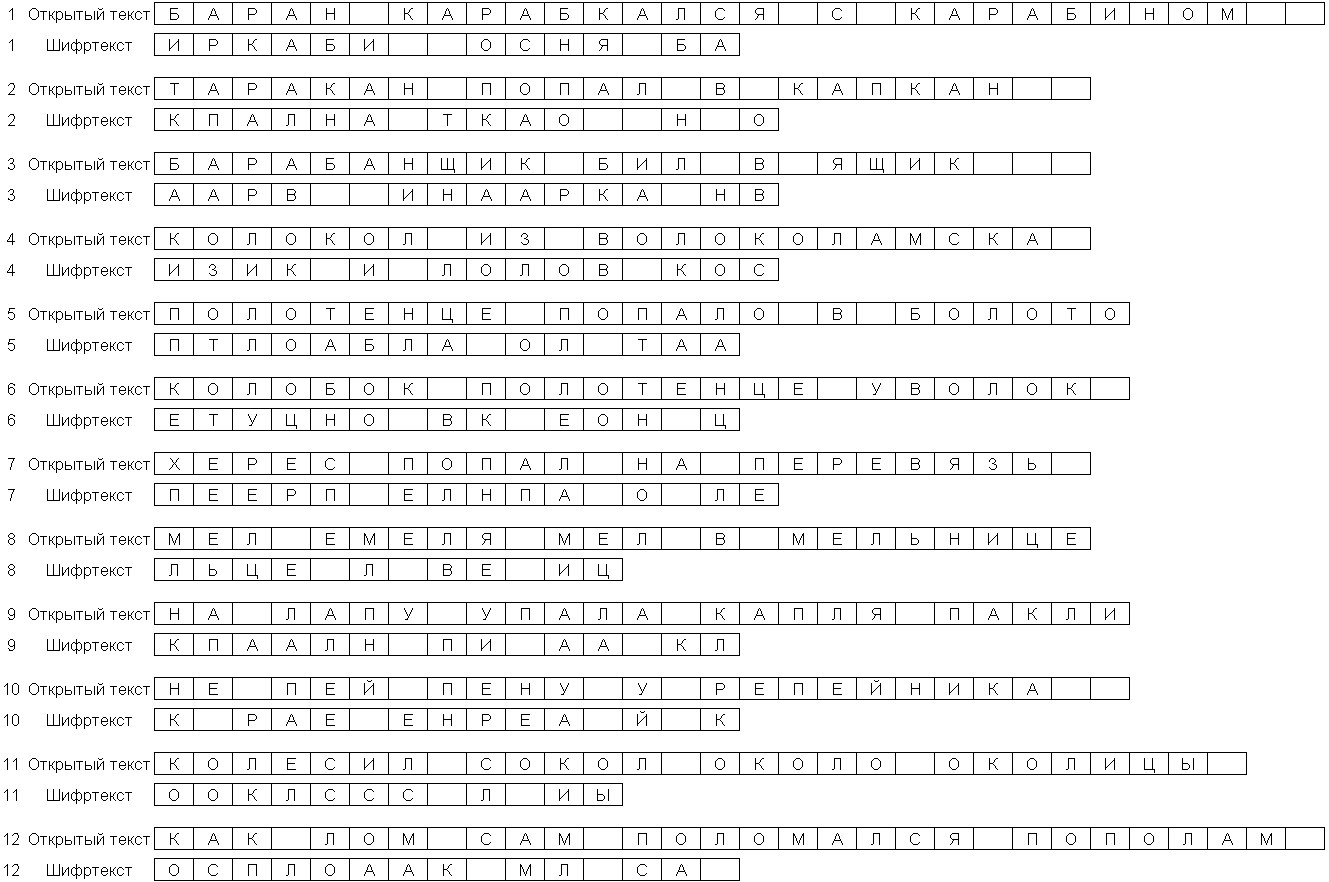
Обратная перестановка: 1→3, 2→1, 3→4, 4→2

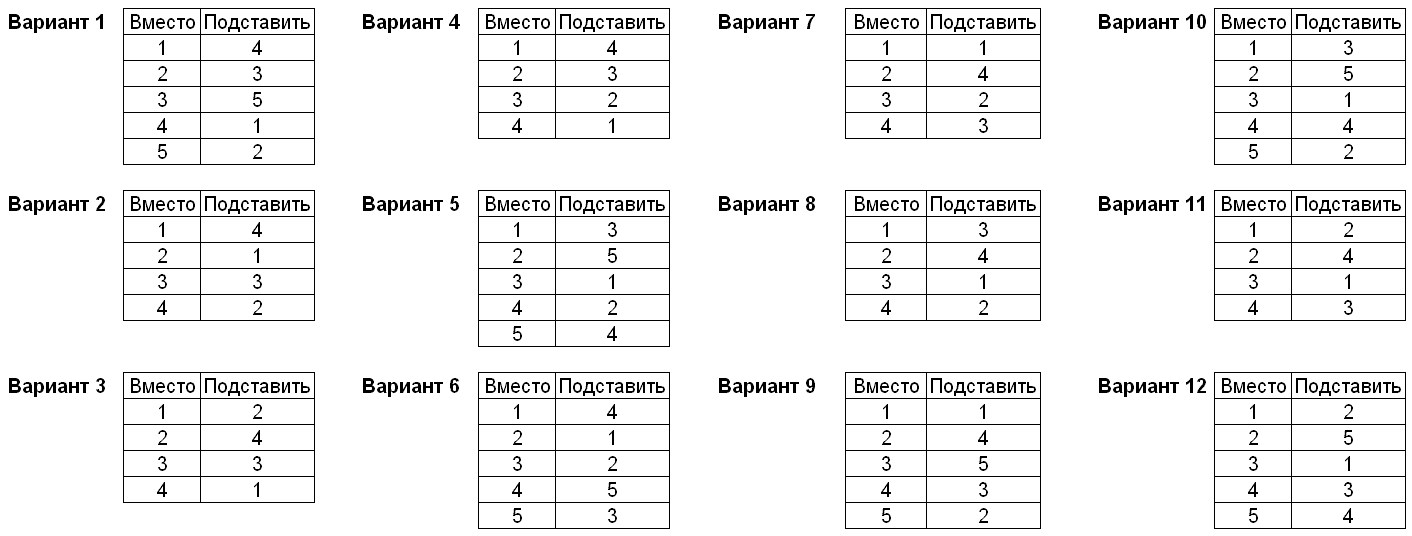
Например, для шифртекста «УААРУА М» = «УААР» (блок 1) + «УА\_М» (блок 2) Можно получить исходный открытый текст «АУРА УМА»

# Порядок выполнения лабораторной работы

1. Выбрать язык программирования.
2. До начала написания кода зашифровать сообщение в тетради.
3. Определить размер открытого текста и размер блока.
4. Дополнить, при необходимости, сообщение пробелами до размера, кратного блоку.
5. Переставить символы в блоках местами согласно варианта таблицы перестановок.
6. Составить шифртекст исходного сообщения.
7. Сравнить частоту появления отдельных символов в открытом тексте и шифртексте.
8. Расшифровать заданный шифртекст с использованием таблицы перестановки.

**Варианты заданий**

1. ***Открытый текст зашифровать.***
2. ***Шифртекст расшифровать.***
3. ***Варианты заданий и перестановок представлены на рисунках.***



# Содержание отчета о лабораторной работе:

* номер группы, ФИО, дата выполнения работы;
* исходное сообщение;
* ключ шифра (правило перестановки);
* шифртекст;
* сравнение частоты появление символов в открытом тексте и шифртексте;
* расшифровка заданного шифртекста.

# Пример

Исходное сообщение "МАМА МЫЛА РАМУ" Перестановка:

|  |  |
| --- | --- |
| Вместо | Подставить |
| 1 | 2 |
| 2 | 4 |
| 3 | 1 |
| 4 | 3 |

Размер открытого текста: 14 символов

Размер блока: 4 символа

Необходимо дополнить открытый текст двумя пробелами

(14 символов + 2 пробела = 16 символов = 4 блока \* 4 символа/блок ) Шифртекст для исходного сообщения:

"ААМММЛ Ы ААР У М "

Сравнение частот символов в открытом тексте и шифртексте:

Открытый текст Шифртекст

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Символ | Частота |  | Символ | Частота |
| А | 4 | А | 4 |
| М | 4 | М | 4 |
| " " | 2 | " " | 2 |
| Л | 1 | Л | 1 |
| Р | 1 | Р | 1 |
| У | 1 | У | 1 |
| Ы | 1 | Ы | 1 |