# ЛАБОРАТОРНАЯ РАБОТА №1
# “ШИФРОВАНИЕ ДАННЫХ МЕТОДОМ ПОДСТАНОВКИ”

## Цель работы

Целью работы является знакомство с классическим криптографическим алгоритмом - алгоритмом шифрования данных при помощи подстановки.

## Основные сведения

В современной криптографии рассматриваются два типа криптографических алгоритмов. Это классические криптографические алгоритмы, основанные на использовании секретных ключей, и новые криптографические алгоритмы с открытым ключом, основанные на использовании ключей двух типов: секретного (закрытого) и открытого.

В классической криптографии ("криптографии с секретным ключом" или "одноключевой криптографии") используется только одна единица секретной информации - ключ, знание которого позволяет отправителю зашифровать информацию в шифртекст, а получателю - расшифровать его. Операция шифрования/дешифрования с большой вероятностью невыполнима без знания секретного ключа. Поскольку при использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются симметричными.

Подстановочное шифрование основывается на использовании некоторой взаимно однозначной функции $C_V : V^m \to V^m$, где $V$ - алфавит шифруемых сообщений, $m$ - длина блока открытого текста и блока

шифрограммы. В процессе шифрования открытый текст X разбивается на $m$-символьные блоки $x_1$, $x_2$, ..., $x_l$, каждый из которых заменяется $m$-символьным блоком $y_i = C_V(x_i), i = \overline{1,l}$. Дешифрование сводится к обратной замене $m$-символьных блоков $y$ на $m$-символьные блоки $C_V^{-1}(y_i), i = \overline{1,m}$.

Например, пусть алфавит $V$ = {0,1, .., 9, <пробел>, A, B, .., Z, a, b, .., z, А, Б, .., Я, а, б, .., я}, длина блока шифрограммы и блока открытого текста $m$ = 3. Допустим, что необходимо зашифровать открытый текст X = “Произвольный блок открытого текста”. Разобьем открытый текст X на $m$-символьные (трехсимвольные в нашем примере) блоки: “Про”, “изв”, “оль”, “ный”, “_бл”, “ок_“, “отк”, “рыт”, “ого”, “_те”, “кст”, “а__”. Пробелы обозначены символом _, при необходимости последний блок может быть дополнен с правой стороны необходимым количеством пробелов. Если пробел не входит в алфавит языка, то его функцию (функцию разделительного элемента) может выполнять любой другой символ алфавита, если стороны, обменивающиеся сообщениями, достигли соответствующей договоренности.

Для шифрования необходимо иметь функцию $C_V$, ставящую каждому трехсимвольному блоку открытого текста трехсимвольный блок шифртекста. Такая функция может быть задана, например, при помощи таблицы:

| $x_i$ | Про | изв | оль | ный | _бл | ок_ | отк | рыт | ого | _те | кст | а__ | … |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_V(x_i)$ | Атр | ф7ы | нрв | св_ | ркк | ыт0 | мкф | ц_й | 1ся | щн_ | ы34 | вхш | … |

Каждый блок открытого текста заменяется при помощи функции $C_V$ соответствующим блоком шифртекста. Таким образом, для

рассматриваемого примера шифртекст будет выглядеть следующим образом: “Атрф7ынрвсв_ркkыт0мкфц_й1сящн_ы34вхш”.

Поскольку функция $C_V$ является взаимно однозначной, эта же таблица используется и для дешифрации шифртекста.

Очевидно, что приведенные в этом примере алфавит и принятый размер блока открытого текста требуют очень большой таблицы, задающей функцию шифрования: эта таблица должна задавать все возможные трехсимвольные сочетания из русских и латинских букв, а также цифр. Если в качестве алфавита рассматривать двоичный алфавит {0, 1}, а размер блока открытого текста принять равным 7 (как это имеет место в случае обычного ASCII-кода), то для задания функции шифрования требуется таблица со 128 столбцами. В общем случае, требуется определить $|V|^m$ значений функции, где $|V|$ - мощность множества $V$, то есть количество элементов алфавита. Разумеется, если заранее известно, что некоторые комбинации символов открытого текста являются недопустимыми, то указанное значение может быть уменьшено.

## Индивидуальные задания

Задания выбираются студентами из нижеприведенной таблицы в соответствии со своими номерами по списку (по модулю 10).

| Задание | | | Для информации | |
|---|---|---|---|---|
| № п.п. | $V$ | $m$ | $\|V\|$ | $\|V\|^m$ |
| 1 | {0,1} | 5 | 2 | 32 |
| 2 | {0,1,2} | 3 | 3 | 27 |
| 3 | {0,1,2,3,4} | 2 | 5 | 25 |
| 4 | {0,1,2,3,4,5} | 2 | 6 | 36 |
| 5 | {A,B,..,Z} | 1 | 26 | 26 |

| Задание | | | Для информации | |
|---|---|---|---|---|
| № п.п. | $V$ | $m$ | $\|V\|$ | $\|V\|^m$ |
| 6 | {А,Б,..,Я} | 1 | 33 | 33 |
| 7 | {x,y} | 5 | 2 | 32 |
| 8 | {x,y,z} | 3 | 3 | 27 |
| 9 | {a,b,c,d,e} | 2 | 5 | 25 |
| 10 | {а,б,в,г,д,е} | 2 | 6 | 36 |

## Порядок выполнения

1. Изучить основы шифрования данных методом подстановки.

2. В соответствии с индивидуальным заданием разработать алгоритм и написать программу, обеспечивающую ввод произвольного открытого текста и выдачу шифрограммы, полученную изучаемым методом, а также дешифрацию - получение открытого текста из шифрограммы.

Примечание. Функцию шифрования, основываясь на данных индивидуального задания, определить самостоятельно.

## Содержание отчета

1. Цель работы.
2. Индивидуальное задание.
3. Функция шифрования.
4. Текст программы, реализующей индивидуальное задание.
5. Пример открытого текста и соответствующей ему шифрограммы.
6. Выводы по работе.