

# Лабораторная работа №1

## Шифры простой замены

---

ВОЛКОВА ДАРЬЯ АЛЕКСАНДРОВНА НПММД-02-21

# Цель работы

---

Изучение шифров простой замены:

1. шифр Цезаря
2. шифр Атбаш

# Задачи

---

Программная реализация шифров простой замены:

1. шифр Цезаря
2. шифр Атбаш

# Теоретические сведения

---

В шифре простой замены выбирается нормативный алфавит т.е. набор символов, которые будут использоваться для составления сообщений. В качестве нормативного алфавита может применяться, например, русский алфавит, исключая буквы «ъ» и «ё». Затем выбирается алфавит шифрования (шифр-алфавит).

Шифрование заключается в замене каждого символа открытого текста на соответствующие символы шифр-алфавита. В шифре простой замены каждый символ исходного текста заменяется символами шифр-алфавита одинаково на всем протяжении текста.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3, А была бы заменена на Г.

«Атбáш» — один из самых древних методов шифрования. Шифрование заключается в замене каждой буквы исходного текста на «симметричную» ей букву алфавита, то есть первая алфавита заменялась на последнюю и наоборот, вторая буква — на предпоследнюю и наоборот и т.д.

# Результаты

---

```
: # 1. Шифр Цезаря

: alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя '

: message = input('Введите строку: ').lower()
: key = int(input('Введите ключ: '))

Введите строку: привет
Введите ключ: 4

: encrypted = ''

: for letter in message:
:     if letter in alphabet:
:         t = alphabet.find(letter)
:         new_key = (t + key) % len(alphabet)
:         encrypted += alphabet[new_key]
:     else:
:         encrypted += letter

: print('Криптограмма:', encrypted)

Криптограмма: уфмёиц
```

Пример работы алгоритма Цезаря

# Результаты

---

```
# 2. Шифр Атбаш
```

```
alphabet = 'абвгдежзийклмнопрстуфхцшщъыьэюя '
```

```
alphabet_revers= alphabet[::-1]
```

```
message = input('Введите строку: ').lower()
```

Введите строку: привет

```
encrypted = ''
```

```
for i in message:
    for j, l in enumerate(alphabet):
        if i == l:
            encrypted = encrypted+alphabet_revers[j]
```

```
print('Криптограмма:', encrypted)
```

Криптограмма: рпчюын

Пример работы алгоритма Атбаш

# Выводы

---

В ходе выполнения работы удалось изучить шифры простой замены:

1. шифр Цезаря
2. шифр Атбаш

А также реализовать данные алгоритмы программно на языке Python.