

# **Лабораторная работа №1**

**Математические основы защиты информации и информационной  
безопасности**

Леонтьева Ксения Андреевна | НПМмд-02-23

# Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
4	Выводы	9

# Список иллюстраций

3.1	Реализация шифра Цезаря . . . . .	7
3.2	Реализация шифра Атбаш . . . . .	8

# 1 Цель работы

Реализовать на языке программирования шифр Цезаря с произвольным ключом  $k$  и шифр Атбаш.

## 2 Теоретическое введение

Шифр Цезаря (является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка).

Математически процедуру шифрования можно описать следующим образом:  $T_m = \{T^j\}, j = 0, 1, \dots, m - 1, T^j(a) = (a + j) \bmod(m)$ , где  $(a + j) \bmod(m)$  - операция нахождения остатка от целочисленного деления  $a + j$  на  $m$ , а  $T_m$  - циклическая группа. Обобщение шифра Цезаря на случай произвольного ключа  $k$  для латинского алфавита:  $(i + k) \bmod(26)$ .

Шифр Атбаш является шифром сдвига на всю длину алфавита. Для реализации шифра целесообразно пользоваться таблицей ASCII и функциями работы с ней: `ord` и `char`.

### 3 Выполнение лабораторной работы

Начнем с реализации шифра Цезаря. Переменные `phrase` и `k` соответствуют введенным с клавиатуры тексту и ключу, необходимому для шифрования. Переменная `alphabet` представляет собой список, состоящий из строчных латинских букв. `New_alphabet` - пустой список, который с помощью цикла мы заполняем, делая сдвиг в исходном алфавите (`alphabet`) на введенные `k` букв влево. Затем заполняем пустой список (`encrypted_phrase`), соответствующий зашифрованному слову. Для этого последовательно, с помощью цикла по переменной `j`, “берем” буквы из исходного текста (`phrase`), находим индекс `j`-той буквы из текста в исходном алфавите (`alphabet`), а далее в новом алфавите (`new_alphabet`) находим букву с найденным только что индексом. Наконец, выводим полученный зашифрованный текст на экран.

Код программы (рис. 3.1).

```
import string
```

```
phrase = input('Введите текст без пробелов: ')\nphrase = list(phrase)
```

```
k = input('Введите ключ: ')\nk = int(k)
```

```
Введите текст без пробелов: abcdefg\nВведите ключ: 3
```

```
alphabet = string.ascii_lowercase
```

```
new_alphabet = list()\nfor i in range(len(alphabet)):\n    new_alphabet.append(alphabet[(i+k)%26])
```

```
encrypted_phrase = list()\nfor j in range(len(phrase)):\n    encrypted_phrase.append(new_alphabet[alphabet.index(phrase[j])])
```

```
print(''.join(encrypted_phrase))
```

```
defghij
```

Рис. 3.1: Реализация шифра Цезаря

Далее реализовываем шифр Атбаш. Аналогично шифру Цезаря вводим текст `phrase`. Заполняем список `alphabet` русскими строчными буквами и пробелом с помощью кодов из таблицы ASCII и операции `chr`. Затем заполняем пустой список (`encrypted_phrase`), соответствующий зашифрованному слову. Для этого находим в исходном алфавите индекс, соответствующий зашифрованной букве по формуле: `длина_алфавита - индекс_буквы_исходного_текста - 1`. Наконец, выводим полученный зашифрованный текст на экран.

Код программы (рис. 3.2).

```
phrase = input('Введите текст: ')\nphrase = list(phrase)
```

Введите текст: привет

```
alphabet = list()\nfor i in range(1072,1104):\n    alphabet.append(chr(i))\nalphabet.append(chr(32))\n\nencrypted_phrase = list()\nfor j in range(len(phrase)):\n    number = len(alphabet) - alphabet.index(phrase[j]) - 1\n    encrypted_phrase.append(alphabet[number])
```

```
print(''.join(encrypted_phrase))
```

сршьюю

Рис. 3.2: Реализация шифра Атбаш



## 4 Выводы

В ходе выполнения данной лабораторной работы были реализованы шифры Цезаря и Атбаш на языке программирования Python.