

# Лабораторная работа №1

## Шрифты простой замены

---

Румянцева Александра Сергеевна

17 сентября, 2022

## Цели и задание на лабораторную работу

Цель: Приобретение практических навыков шифрования и дешифрования текстов методом простой замены. Изучение шифра Цезаря и Атбаша.

Задание: Лабораторная работа подразумевает реализацию шифра Цезаря с произвольным ключом  $k$  и шифра Атбаш.

# Выполнение лабораторной работы

1. Изучила теорию и указание к лабораторной работе.
2. Реализация шифра Цезаря на языке Python для английского алфавита

Мною был написан код для шифрования текста (рис. 1) и шифром Цезаря.

**Шифр Цезаря**

```
In [55]: 1 import string
2 def encrypt_caesar(plaintext: str, shift) -> str:
3     letters = string.ascii_letters #abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
4     abc = letters[:len(letters)//2] #abcdefghijklmnopqrstuvwxyz
5     ABC = letters[len(letters)//2:] #ABCDEFGHIJKLMNOPQRSTUVWXYZ
6
7     cipher_letters = abc[shift:] + abc[:shift] + ABC[shift:] + ABC[:shift] #a b c d e f g h i j k l m n o p q r s t u v w x y z
8     table = str.maketrans(letters, cipher_letters)
9
10    ciphertext = plaintext.translate(table)
11    return ciphertext

In [56]: 1 k=3
2 text = encrypt_caesar("Run!antcovaAS", k)
3 print(text)

Ur!p!dqpfhydBV
```

**Figure 1:** рис. 1. Шифрование текста шифром Цезаря.

Как можно заметить, для шифра Цезаря использовался ключ шифрования  $k=3$ .

Код для разшифровки текста (рис. 2) шифром Цезаря.

**Расшифровка Цезарь**

```
In [57]: 1 def decrypt_caesar(ciphertext: str, shift) -> str:
          2
          3     plaintext = encrypt_caesar(ciphertext, - shift)
          4     return plaintext

In [58]: 1 decrypt_caesar(text, k)

Out[58]: 'RumiantcevaAS'
```

**Figure 2:** рис. 2. Разшифровка текста шифром Цезаря.

Для расшифровки шифра Цезаря аналогично использовался ключ шифрования  $k=3$ .

## 2. Реализация шифра Атбаш на языке Python для английского алфавита

Был написан код для шифрования текста (рис. 3) шифром Атбаш.

**Шифр Атбаш**

```
In [62]: 1 def encrypt_atbash(plaintext: str) -> str:
2         letters = string.ascii_letters      #abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
3         abc = letters[:len(letters)//2]      #abcdefghijklmnopqrstuvwxyz
4         ABC = letters[len(letters)//2:]      #ABCDEFGHIJKLMNOPQRSTUVWXYZ
5
6         cipher_letters = abc[::-1] + ABC[::-1] #исходный "перевернутый" алфавит для шифра
7         table = str.maketrans(letters, cipher_letters)
8
9         ciphertext = plaintext.translate(table)
10        return ciphertext

In [64]: 1 text = encrypt_atbash("RuniantcevaAS")
2         text

Out[64]: 'IfnrzngxvezZH'
```

**Figure 3:** рис. 3. Шифрование текста шифром Атбаш.

Для шифра Атбаш уже не использовался ключ шифрования, поскольку сам шифр не подразумевает его присутствие.

Код для разшифровки текста (рис. 4) шифром Атбаш.

**Расшифровка Атбаш**

```
In [65]: 1 def decrypt_atbash(ciphertext: str) -> str:
2         letters = string.ascii_letters #abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
3         abc = letters[:len(letters)//2] #abcdefghijklmnopqrstuvwxyz
4         ABC = letters[len(letters)//2:] #ABCDEFGHIJKLMNOPQRSTUVWXYZ
5
6         cipher_letters = abc[::-1]+ABC[::-1]
7         table = str.maketrans(cipher_letters, letters)
8
9         text = ciphertext.translate(table)
10        return text

In [66]: 1 decrypt_atbash(text)

Out[66]: 'RumiantcevaAS'
```

**Figure 4:** рис. 4. Разшифровка текста шифром Атбаш.

Можно заметить что сама шифровка шифром Атбаш является и дешифровкой при повторном применении шифрования (рис. 5).

```
In [67]: 1 text = encrypt_atbash("RumiantcevaAS")
2         print(text)
3         text_ = encrypt_atbash(text)
4         print(text_)

IfnrzmgxvezZH
RumiantcevaAS
```

**Figure 5:** рис. 5. Повторное шифрование текста шифром Атбаш = дешифрование. 6/7

Мною были приобретены практические навыки шифрования и дешифрования текстов методом простой замены. Успешно освоены шифры Цезаря и Атбаша.