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.

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.

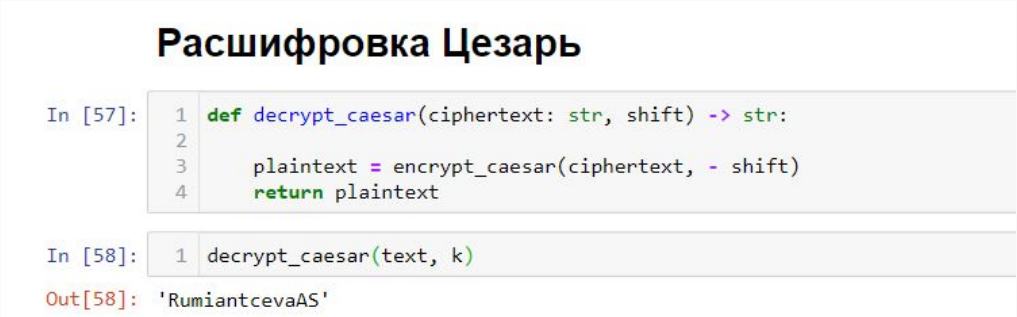

Figure 2: рис. 2. Разшифровка текста шифром Цезаря.

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 Абташ.

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

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

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

Расшифровка Атбаш

```
In [65]:
def decrypt_atbash(ciphertext: str) -> str:
    letters = string.ascii_letters      #abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
    abc = letters[:len(letters)//2]     #abcdefghijklmnopqrstuvwxyz
    ABC = letters[len(letters)//2:]     #ABCDEFGHIJKLMNOPQRSTUVWXYZ

    cipher_letters = abc[::-1]+ ABC[::-1]
    table = str.maketrans(cipher_letters, letters)

    text = ciphertext.translate(table)
    return text

In [66]:
decrypt_atbash(text)

Out[66]: 'RumiantcevaAS'
```

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

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

```
In [67]:
text = encrypt_atbash("RumiantcevaAS")
print(text)
text_ = encrypt_atbash(text)
print(text_)

IfnrzmgxvezZH
RumiantcevaAS
```

Figure 5: рис. 5. Повторное шифрование текста шифром Атбаш = дешифрование.

Выводы

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