Отчёт по лабораторной работе 1

Шрифты простой замены

Румянцева Александра Сергеевна

Содержание

Список иллюстраций

Список таблиц

Цель работы

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

Задание

Лабораторная работа подразумевает реализацию шифра Цезоря с произвольным ключом k и шифра Атбаш.

Теория

Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. Он является моноалфавитным, то есть имеет подстановочный тип, где каждая буква в открытом тексте заменяется на другую букву, смещенную на определенное количество позиций в алфавите.

Шифр Цезаря называется так благодаря Юлию Цезарю, который использовал его со сдвигом 3, чтобы защищать военные сообщения. Несмотря на то, что Цезарь считается первым зафиксированным человеком, использующим эту схему, другие шифры подстановки, как известно, использовались и раньше.

Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Пример шифрования со сдвигом 5:

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер п/п	12	18	10	17	20	16	4	18	1	22	10	33
Номер п/п +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное

приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$y = (x + k) \bmod n$ $x = (y - k + n) \bmod n$

где: x — символ открытого текста, y — символ шифрованного текста, n — мощность алфавита, k — ключ.

Шифр Атбаш

Шифр простой замены Атбаш использовался для еврейского алфавита и оттуда же получил свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю. (алеф(первая буква) заменяется на тау(последнюю), бет(вторая) заменяется на шин(предпоследняя) из этих сочетаний шифр и получил свое название).

Шифр Атбаш для английского алфавита:

Исходный алфавит: A B C D E F G H Я J K L M N O P Q R S T U V W X Y Z

Алфавит замены: Z Y X W V U T S R Q P O N M L K J Я H G F E D C B A

Правило шифрования состоит в замене i-й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

Выполнение лабораторной работы

1. Реализация шифра Цезаря на языке Python для английского алфавита

Мною был написан код для шифрования текста (рис. 1) и разшифровки (рис. 2) шифром Цезаря.

Рис. 1: рис. 1. Шифрование текста шифром Цезаря.

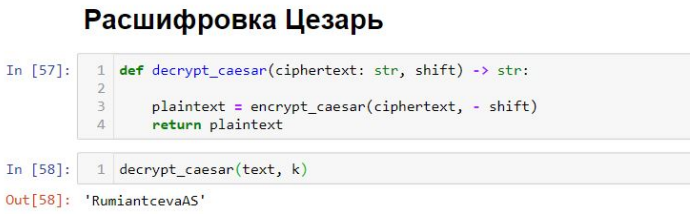

Рис. 2: рис. 2. Разшифровка текста шифром Цезаря.

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

2. Реализация шифра Атбаш на языке Python для английского алфавита

Был написан код для шифрования текста (рис. 3) и разшифровки (рис. 4) шифром Абташ.

Шифр Атбаш

In [62]:
```
def encrypt_atbash(plaintext: 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]  #новый "перевернутый" алфавит для шифра
    table = str.maketrans(letters, cipher_letters)

    ciphertext = plaintext.translate(table)
    return ciphertext
```

In [64]:
```
text = encrypt_atbash("RumiantcevaAS")
text
```

Out[64]: 'IfnrzmgxvezZH'

Рис. 3: рис. 3. Шифрование текста 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'

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

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

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
```

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

Библиография

1. ТУИС РУДН

2. Статья “Шифр Атбаш” https://ru.wikipedia.org/wiki/Атбаш

Выводы

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