Отчёт по лабораторной работе №1

Шифр простой замены

Фань Яньцзе

Содержание

List of Figures

1 Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

2 Теоретические сведения

2.1 Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

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, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

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) mod n
x = (y - k + n) mod n
```

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

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

2.2 Шифр Атбаш

Атбаш — простой шифр подстановки, изначально придуманный для иврита. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n − i + 1, где n — число букв в алфавите.

3 Выполнение работы

3.1 Реализация шифра Цезаря на языке Python

Блок шифрования

```
def cesar(text, step=3, w=0):
    liters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    res = ''
    if w==0:
        for i in text:
            index = liters.find(i)
            new_index = index + step
            if i in liters:
                res += liters[new_index]
            else:
                res += i
    if w==1:
        for i in text:
            index = liters.find(i)
            new_index = index - step
            if i in liters:
                res += liters[new_index]
            else:
                res += i
```

```
    return res
```

3.2 Реализация шифра Атбаш на языке Python

Блок шифрования

```
def atbash(text, w=0):
    liters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ '
    liters_r = [x for x in liters]
    liters_r.reverse()
    res = ''
    if w == 0:
        for i in text:
            for j,l in enumerate(liters):
                if i==l:
                    res += liters_r[j]
    if w == 1:
        for i in text:
            for j,l in enumerate(liters_r):
                if i==l:
                    res += liters[j]
    return res
```

3.3 Контрольный пример

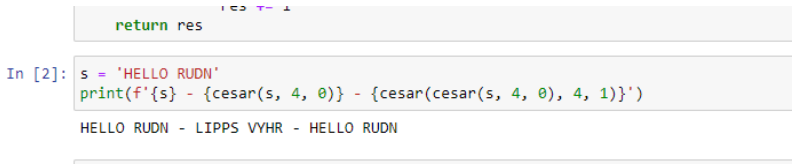

Figure 3.1: шифр Цезаря

```
    if w == 1:
        for i in text:
            for j,l in enumerate(liters_r):
                if i==l:
                    res += liters[j]
    return res
```

In [13]:
```
s = 'HELLO RUDN'
print(f'{s} - {atbash(s, 0)} - {atbash(atbash(s, 0), 1)}')
```

```
HELLO RUDN - TWPPMAJGXN - HELLO RUDN
```

Figure 3.2: шифр Атбаш

4 Выводы

Изучили алгоритмы шифрования Цезаря и Атбаш.

Список литературы

1. Шифр Цезаря
2. Шифр Атбаш