Лабораторная работа №1

Шифры простой замены

Яковлев А.А.

17 сентября 2022

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Цель работы — изучить и программно реализовать шифры простой замены.

Задачами являются:

- Реализовать шифр Цезаря с произвольным ключом k;
- Реализовать шифр Атбаш.

В основе функционирования шифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

Шифр Цезаря

Шифр Цезаря является моноалфавитной подстановкой, т.е. каждой букве открытого текста ставится соответствие одна буква шифротекста.

Математическая процедура шифрования описывается как

$$T_m = \left\{ T^j \right\}, j = 0, 1, \cdots, m-1,$$

$$T^j(a) = (a + j) \mod m,$$

Сам же Цезарь обычно использовал подстановку T^3.

Шифр Атбаш

Шифр Атбаш является сдвигом на всю длину алфавита. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

Выполнение лабораторной работы

Для реализации шифров мы будем использовать Python, так как его синтаксис позволяет быстро реализовать необходимые нам алгоритмы.

Реализация шифра Цезаря с произвольным ключом k

```
alphabet1= list(map(chr, range(97,123)))
print(alphabet1)
```

```
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm'
'y', 'z']
```

```
def ceaser(t,alphabet1,key):
    res = ""

    for c in t:
        if c not in alphabet1:
            res += c
        else:
            c_index = ord(c) - ord('a')
            c_shifted = (c_index+key)%26 + ord('a')
            c_new = chr(c_shifted)
            res+=c_new
    return res
print(ceaser("dream team",alphabet1, 6))
```

```
jxkgs zkgs
```

Реализация шифра Атбаша

```
alphabet2 = list(map(chr, range(97,123)))
alphabet2.append(chr(32))
print(alphabet2)
```

```
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n',
'y', 'z', ' ']
```

```
def atbash(t,alphabet2):
    res = ""
    for c in t:
        if c not in alphabet2:
            res +=c
        else:
            c_new = alphabet2[len(alphabet2)-1-alphabet2.index(c)]
            res += c_new
    return(res)
print(atbash("xjw oahw o", alphabet2))
```

```
dream team
```

```
print(ceaser("dream team",alphabet1, 6))
```

```
jxkgs zkgs
```

Рис. 3: результат Цезаря

```
print(atbash("xjw oahw o", alphabet2))
```

```
dream team
```

Рис. 4: результат Атбаш

Выводы

В рамках выполненной лабораторной работы мы изучили и реализовали следующие шифры простой замены: шифр Цезаря (с произвольным ключом k) и шифр Атбаш.