# Лабораторная работа №1

Шифры простой замены

Яковлев Артём Александрович, НФИмд-01-22

# Содержание

# Список таблиц

# Список иллюстраций

# Цель работы

Цель данной работы — изучить и программно реализовать шифры простой замены.

# Задание

Заданием является:

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

# Теоретическое введение

Шифр простой замены представляет собой замену каждой буквы в исходном слове на определенное число, которому соответствует данная буква. 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

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

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

где $m$ - длина алфавитаа, $j$ - произвольный ключ (величина сдвига от изначальной позиции буквы), $a$ - текущая позиция буквы в алфавите.

Для латинского алфавита длина составляет 26 символов, а формулу можно привести к виду:

$$T^k(i) = (i + k) \mod 26,$$

где $i, k$ соответствуют $a, j$, а $m = 26$.

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 $k$

Шифр Цезаря реализуем в виде функции ceasar следующего вида:

```
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
```

Рис. 0.1: функция шифра Цезаря

На вход она принимает переменные t (текст для шифрования), key (произвольный

ключ), alphabet (алфавит в виде списка).

В ходе обработке мы работаем с индексами элементов массива-строки, предварительно проверяя, является ли символ частью передаваемого алфавита. Если да, то мы вызываем вложенную функцию для расчета сдвига и выполняем к ней операцию деления с остатком (исходя из формулы в теоретическом введении).

## Реализация шифра Атбаша

Шифр Атбаш реализуем в виде функции atbash следующего вида:

```
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
```

Рис. 0.2: функция шифра Атбаш

На вход она принимает те же переменные, что и функция Шифра Цезаря, исключая произвольный ключ.

Шифруется символ засчет вычитания из длины алфавита индекс символа, над которым производится шифрование.

Возвращается также зашифрованный символ.

# Тестирование

Запустив наш программный код, получим следующие результаты:

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

```
jxkgs zkgs
```

Рис. 0.3: результат Цезаря

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

```
dream team
```

Рис. 0.4: результат Атбаш

Видим, что шифрование проведено корректно.

# Выводы

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