Лабораторная работа №1

Шифры простой замены

Ли Т.А.

17 сентября 2022

Российский университет дружбы народов, Москва, Россия

Докладчик

- Ли Тимофей Александрович
- студент группы НФИмд-02-22, студ. билет 1132223452
- Российский университет дружбы народов
- 1132223452@rudn.ru

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

In [14]:
```
def ceasar(letter: chr, key: int, alphabet: list):
    def ceasar(letter:chr, key:int):
        return alphabet.index(letter)+key
    if letter.lower() not in alphabet:
        return letter
    t_letter=alphabet[ceasar(letter.lower(),key)%len(alphabet)]
    if letter.isupper():
        t_letter=t_letter.upper()
    return t_letter
```

Рис. 1: функция шифра Цезаря

Реализация шифра Атбаша

```
def atbash(letter:chr, alphabet:list):
    if letter.lower() not in alphabet:
        return letter
    t_letter=alphabet[len(alphabet)-alphabet.index(letter.lower())-1]
    if letter.isupper():
        t_letter=t_letter.upper()
    return t_letter
```

Рис. 2: функция шифра Атбаш

Для тестирования мы создали следующие функции:

```
In [16]: def run_ceasar(message: str, key:int, alphabet:list):
             a=list(map(lambda letter: ceasar(letter,key,alphabet),message))
             return "".join(a)
```

```
In [20]: def run_atbash(message: str, alphabet:list):
             a=list(map(lambda letter: atbash(letter,alphabet),message))
             return "".join(a)
```

Рис. 3: функции запуска шифрования

```
In [17]: run_ceasar("lessss go first try",3,eng)
Out[17]: 'ohvvvv jr iluvw wub'

In [18]: run_ceasar("ohvvvv jr iluvw wub",23,eng)
Out[18]: 'lessss go first try'
```

Рис. 4: результат Цезаря

```
In [26]: run_atbash("abcdefghijklmnopqrstuvwxyz ",eng2)
Out[26]: ' zyxwvutsrqponmlkjihgfedcba'
```

Рис. 5: 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.