Лабораторная работа №1

Шифры простой замены

Дугаева Светлана Анатольевна

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

```
def cesar (text, k):
    encr = ""
    for c in text:
        c1 = c.lower()
        c_ind=ord(c1) - ord("a")
        c_sh= (c_ind+k) % 26 + ord("a")
        c_new = chr(c_sh)
        if c.islower():
            encr += c_new
        elif c.isupper():
            encr += c_new.upper()
        else:
            encr += c
    return(encr)
```

Создание алфавита для шифра Атбаш

```
# --- Alphabet ---
alphab = list(map(chr, range(97, 123)))
alphab.append(chr(32))
```

Реализация шифра Атбаш

```
# --- Atbash 's Cipher ---
def atbash(text, a):
    encr = ""
    for c in text:
        c1 = c.lower()
        if c1 not in a:
            encr += c
            break
        c_new = a[len(a)-1-a.index(c1)]
        if c.isupper():
            c_new = c_new.upper()
        encr += c_new
    return(encr)
```

Тестирование

```
# --- Tests ---
print("Шифр Цезаря:")
print("Исходный текст: Hello world!\nЗашифрованный текст: ", cesar("Hello world!", 4

print("Шифр Атбаш:")
print("Исходный текст: Twppmaemjpx!\nЗашифрованный текст: ", atbash("Twppmaem
```

Результаты тестирования

Для шифра Цезаря с ключом $k = 4$ получаем следующий результат:

CEASAR'S CIPHER TEST

Шифр Цезаря:

Исходный текст: Hello world!

Зашифрованный текст: Lipps asvph!

Результаты тестирования

Для шифра Атбаш получаем следующий результат:

```
ATBASH'S CIPHER TEST
-----------
Шифр Атбаш:
Исходный текст: Twppmaemjpx!
Зашифрованный текст:  Hello world!
-----------
```

Выводы

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