Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | НПМмд-02-23

Содержание

Список иллюстраций

1 Цель работы

Реализовать на языке программирования шифр Цезаря с произвольным ключом k и шифр Атбаш.

2 Теоретическое введение

Шифр Цезаря (является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка).

Математически процедуру шифрования можно описать следующим образом: $T_m = \{T^j\}, j = 0, 1, ..., m-1, T^j(a) = (a+j)mod(m)$, где $(a+j)mod(m)$ - операция нахождения остатка от целочисленного деления $a+j$ на m, а T_m - циклическая группа. Обобщение шифра Цезаря на случай произвольного ключа k для латинского алфавита: $(i+k)mod(26)$.

Шифр Атбаш является шифром сдвига на всю длину алфавита. Для реализации шифра целесообразно пользоваться таблицей ASCII и функциями работы с ней: ord и char.

Более подробно см. в [1] и [2].

3 Выполнение лабораторной работы

Начнем с реализации шифра Цезаря. Переменные phrase и k соответствуют введенным с клавиатуры тексту и ключу, необходимому для шифрования. Переменная alphabet представляет собой список, состоящий из строчных латинских букв. New_alphabet - пустой список, который с помощью цикла мы заполняем, делая сдвиг в исходном алфавите (alphabet) на введенные k букв влево. Затем заполняем пустой список (encrypted_phrase), соответствующий зашифрованному слову. Для этого последовательно, с помощью цикла по переменной j, “берем” буквы из исходного текста (phrase), находим индекс j-той буквы из текста в исходном алфавите (alphabet), а далее в новом алфавите (new_alphabet) находим букву с найденным только что индексом. Наконец, выводим полученный зашифрованный текст на экран.

Код программы (рис. 3.1).

```
import string
```

```
phrase = input('Введите текст без пробелов: ')
phrase = list(phrase)

k = input('Введите ключ: ')
k = int(k)
```

```
Введите текст без пробелов: abcdefg
Введите ключ: 3
```

```
aphabet = string.ascii_lowercase

new_aphabet = list()
for i in range(len(aphabet)):
    new_aphabet.append(aphabet[(i+k)%26])

encrypted_phrase = list()
for j in range(len(phrase)):
    encrypted_phrase.append(new_aphabet[aphabet.index(phrase[j])])
```

```
print(''.join(encrypted_phrase))
```

```
defghij
```

Рис. 3.1: Реализация шифра Цезаря

Далее реализовываем шифр Атбаш. Аналогично шифру Цезаря вводим текст phrase. Заполняем список alphabet русскими строчными буквами и пробелом с помощью кодов из таблицы ASCII и операции chr. Затем заполняем пустой список (encrypted_phrase), соответствующий зашифрованному слову. Для этого находим в исходном алфавите индекс, соответствующий зашифрованной букве по формуле: длина_алфавита - индекс_буквы_исходного_текста - 1. Наконец, выводим полученный зашифрованный текст на экран.

Код программы (рис. 3.2).

```
phrase = input('Введите текст: ')
phrase = list(phrase)
```

```
Введите текст: привет
```

```
aphabet = list()
for i in range(1072,1104):
    aphabet.append(chr(i))
aphabet.append(chr(32))

encrypted_phrase = list()
for j in range(len(phrase)):
    number = len(aphabet) - aphabet.index(phrase[j]) - 1
    encrypted_phrase.append(aphabet[number])
```

```
print(''.join(encrypted_phrase))
```

```
сршюыо
```

Рис. 3.2: Реализация шифра Атбаш

4 Выводы

В ходе выполнения данной лабораторной работы были реализованы шифры Цезаря и Атбаш на языке программирования Python.

Список литературы

1. Шифр Цезаря [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F.
2. Шифр Атбаш [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%D1%88.