Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Леонтьева К. А., НПМмд-02-23

17 сентября 2023

Российский университет дружбы народов

Москва, Россия

Цель лабораторной работы

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

Задачи лабораторной работы

1) Изучить теоретическую часть лабораторной работы по методичке
2) Написать соответствующие программы

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.

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.

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

Математически процедуру шифрования (для Python) можно описать следующим образом: $N - j - 1$, где N - количество букв в алфавите, j - номер заменяемой буквы в алфавите.

Ход выполнения лабораторной работы

- Реализуем шифр Цезаря

```
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
```

Figure 1: Рис.1: Шифр Цезаря

Ход выполнения лабораторной работы

- Реализуем шифр Атбаш

```
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
```

Figure 2: Рис.2: Шифр Атбаш

Вывод

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