Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Банникова Екатерина Алексеевна

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

НФИмд-02-23

Шифры простой замены. Шифр Цезаря и шифр Атбаш

Цель лабораторной работы

1. Ознакомление с двумя методами шифрования: шифр Цезаря с произвольным ключем k и шифр Атбаш.
2. Их реализация на произвольном языке программирования.

Задачи лабораторной работы

1. Реализовать шифр Цезаря с произвольным ключем
2. Реализовать шифр Атбаша.

Выполнение

В соответсвии с заданием, была написана программа для шифра Цезаря. Код представлен ниже.

```
alfavit_EU =  'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
alfavit_RU = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ'
delta = int(input('Шаг шифровки: '))
message = input("Сообщение для шифровки: ").upper()
itog = ''
lang = input('Выберите язык RU/EU: ')
if lang == 'RU':
    for i in message:
        mesto = alfavit_RU.find(i)
        new_mesto = mesto + delta
        if i in alfavit_RU:
            itog += alfavit_RU[new_mesto]
        else:
            itog += i
else:
    for i in message:
        mesto = alfavit_EU.find(i)
        new_mesto = mesto + delta
        if i in alfavit_EU:
            itog += alfavit_EU[new_mesto]
        else:
            itog += i
print (itog)
```

Figure 1: Код шифра Цезаря

Выполнение

Результаты выполнения программы прдеставленны ниже.

```
Шаг шифровки: 6
Сообщение для шифровки: РУДН
Выберите язык RU/EU: RU
ЦЩЙУ
```

Figure 2: Результат шифрования

Выполнение

В соответсвии с заданием, была написана программа для шифра Атбаш. Код представлен ниже.

```
import os

def Atbash_crypt(cistring):
    string = ""
    cistring = formatString(cistring)
    for x in range(0, len(cistring)):
        string += flipChar(cistring[x])
    return(string)

def formatString (string):
    fmtString = string.lower()
    fmtString = "".join(fmtString.split())
    return fmtString

def flipChar(char):
    flip = abs((ord(char) - 96) - 27)
    return chr(flip + 96) if flip > 0 and flip <= 26 else ""

def Atbash():
    os.system('cls')
    cistring = input("Сообщение для шифровки: ")
    print("Шифровка:", Atbash_crypt(cistring))
    print("Дешифровка:", Atbash_crypt(Atbash_crypt(cistring)))

print(Atbash())
```

Figure 3: Код шифра Атбаш

Результаты выполнения программы прдеставленны ниже.

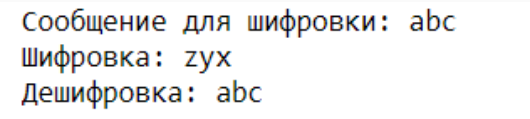

Figure 4: Результат шифрования

Выводы

- Я ознакомилась с помощью питона с двумя методами шифровки: Цезарь и Атбаш.
- Реализовала эти шифры на питоне.