Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Банникова Екатерина Алексеевна

Содержание

Список иллюстраций

List of Tables

1 Цель работы

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

2 Задание

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

3 Теоретическое введение

Шифр = криптосистема. Закрытый текст = зашифрованный текст. Криптоаналитик — человек, который пытается вскрыть зашифрованное сообщение, которое не ему предназначено. Атака, взлом, вскрытие — попытка узнать исходный текст сообщения без ключа. Дешифровка — взлом или расшифровка самая обычная и законная.

Шифр простой замены — класс методов шифрования, которые сводятся к созданию таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется.

4 Выполнение лабораторной работы

4.1 Шифр Цезаря

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

```
alfavit_EU =  'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
alfavit_RU = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'
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)
```

Рис. 4.1: Код шифра Цезаря

Результаты выполнения программы прдеставленны ниже.

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

Рис. 4.2: Результат шифрования

4.2 Шифр Атбаш

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

```python
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())
```

Рис. 4.3: Код шифра Атбаш

Результаты выполнения программы прдеставленны ниже.

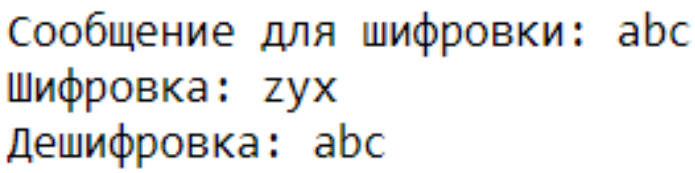

Рис. 4.4: Результат шифрования

5 Выводы

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

6 Список литературы

1. Википедия. Шифр простой замены. https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%
   %D1%82%D0%B5%D0%BA%D1%81%D1%82%D0%B0
2. Википедия. Шифр Цезаря.https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%
3. Википедия. Шифр Атбаш. https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%