Лабораторная работа №1

Дисциплина: Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

Содержание

List of Tables

List of Figures

1 Цель работы

Изучить шифр Цезаря и шифр Атбаш, научиться реализации данных шифров программным путём.

2 Задание

1. Реализовать шифр Цезаря с произвольным ключом k
2. Реализовать шифр Атбаш

3 Выполнение лабораторной работы

1)Перед тем как выполнять лабораторную работу, нужно понять, каким образом её мы будем выполнять. В силу незнания языка Julia, первую лабораторную работу я буду выполнять с помощью языка программирования Python.

Нам нужно реализовать два шифра. Начнём с первого(Рисунок 3.1).

```
def caesar(text, k):
    result = ""
    for char in text:
        if char.isalpha():
            if 97 <= ord(char) <= 122 or 65 <= ord(char) <= 90:
                start = ord('A') if char.isupper() else ord('a')
                result += chr((ord(char) - start + k) % 26 + start)
            if 1040 <= ord(char) <= 1103:
                start = ord('A') if char.isupper() else ord('a')
                result += chr((ord(char) - start + k) % 32 + start)
        else:
            result += char
    return result

text = "АБВГДЕЭЮЯ aBCDEfgHxyZ"
k = 3
encrypted_text = caesar(text, k)
print(encrypted_text)
```

Figure 3.1: Код программы шифра Цезаря

В шифре Цезаря на вход мы получаем текст и число смещения. Делаем цикл, который поменяет каждую букву нашего предложения на соответствующую букву шифроалфавита. Стоит отметить, что используем мы кодировку ASCII, поэтому нам нужно отличать латиницу и кириллицу. Для этого мы вводим дополнительные условия. Также стоит учесть тот факт, что буква ‘ё’ из кириллицы выходит за границы кодировки простых букв. Поэтому в наших текстах эта буква не будет

использоваться. Вывод программы представлен на рисунке 3.2.

```
C:\Users\tidaa\PycharmProjects\InfoBez\venv\Scripts\python.exe C
ГДЕЖЗИАБВ dEFGHijKabC

Process finished with exit code 0
```

Figure 3.2: Вывод программы

2)Похожим образом реализуется шифр Атбаш, который зеркалит алфавит. В этом шифроалфавите мы не будем использовать пробел из-за таких же проблем, как и с буквой ‘ё’. Код представлен на рисунке 3.3.

```
def atbash(text):
    result = ""
    for char in text:
        if char.isalpha():
            if 97 <= ord(char) <= 122 or 65 <= ord(char) <= 90:
                start = ord('A') if char.isupper() else ord('a')
                result += chr(start + (25 - (ord(char) - start)))
            if 1040 <= ord(char) <= 1103:
                start = ord('A') if char.isupper() else ord('a')
                result += chr(start + (31 - (ord(char) - start)))
        else:
            result += char
    return result

text = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ abcDEFxYz"
encrypted_text = atbash(text)
print(encrypted_text)
```

Figure 3.3: Код программы шифра Атбаш

Вывод программы представлен на рисунке 3.4.

```
C:\Users\tidaa\PycharmProjects\InfoBez\venv\Scripts\python.exe
ЯЮЭЬЫЪЩШЧЦХФУТСРПОНМЛКЙИЗЖЕДГВБА zyxWVUcBa

Process finished with exit code 0
```

Figure 3.4: Вывод программы

4 Выводы

- Я изучил шифр Цезаря и шифр Атбаш, научился реализации данных шифров программным путём.

5 Список литературы

- Шифры простой замены [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/