Отчет по лабораторной работе №1

Дисциплина: Математические основы защиты информации и информационной безопасности

Выполнила Дяченко Злата Константиновна, НПМмд-02-22

Содержание

Список иллюстраций

1 Цель работы

Ознакомится и реализовать шифры простой замены.

2 Задание

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

3 Выполнение лабораторной работы

3.1 Шаг 1

Ознакомилась с предоставленными теоретическими данными. Для выполнения задания решила использовать язык Python. Создала переменную типа строка, содержащую русский алфавит, что видно на Рисунке 1 (рис. -fig. 3.1)

```
In [1]: alfavit= "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
```

Рис. 3.1: Создание переменной, содержащей алфавит

3.2 Шаг 2

Написала функцию, выполняющую шифрование с помощью шифра Цезаря. Код функции и результат ее использования представлен на Рисунке 2 (рис. -fig. 3.2). Функция принимает на вход алфавит, фразу, которую нужно зашифровать, и величину сдвига k. Для каждого символа сообщения сначала производится поиск его порядкового номера в алфавите, обозначаемый i. Затем по формуле $(i+k)\ mod\ l$, где l - число символов в алфавите, определяется на символ с каким номером будет заменен данный. Этот символ добавляется к уже зашифрованным ранее символам. Функция возвращает получившуюся строку.

```
In [4]: def cesar (alfavit, frase, k):
            j=0
            shifr=""
            for m in frase:
                i=alfavit.find(m)
                shifr=shifr+alfavit[(i+k)%(len(alfavit))]
                j=j+1
            return shifr

In [5]: cesar(alfavit, "люблю", 1)

Out[5]: 'мявмя'
```

Рис. 3.2: Реализация шифра Цезаря

3.3 Шаг 3

При использовании данной функции для шифрования фразы символ пробела заменяется буквой “а”. Чтобы пробел при шифровании сохранялся, в функцию было добавлено новое условие. На Рисунке 3 (рис. -fig. 3.3) представлена новая функция и результат ее использования для шифрования фразы.

```
In [6]: cesar(alfavit, "люблю тебя", 1)

Out[6]: 'мявмяауёва'

In [7]: def cesar2 (alfavit, frase, k):
            j=0
            shifr=""
            for m in frase:
                if (m==" "):
                    shifr=shifr+ " "
                else:
                    i=alfavit.find(m)
                    shifr=shifr+alfavit[(i+k)%(len(alfavit))]
                    j=j+1
            return shifr

In [8]: cesar2(alfavit, "люблю тебя", 1)

Out[8]: 'мявмя уёва'
```

Рис. 3.3: Изменение функции шифра Цезаря

3.4 Шаг 4

Для реализации шифра Атбаш добавила создала переменную, содержащую все символы русского алфавита и символ пробела в конце, что видно на Рисунке 4 (рис. -fig. 3.4).

```
In [17]: alfavit2= "абвгдеёжзийклмнопрстуфхцчшщъыьэюя "
```

Рис. 3.4: Создание переменной, содержащей алфавит и символ пробел

3.5 Шаг 5

Написала функцию, реализующую шифр Атбаш, код которой и пример выполнения показан на Рисунке 5 (рис. -fig. 3.5). Функция принимает на вход алфавит, фразу, которую нужно зашифровать. Для каждого символа сообщения сначала производится поиск его порядкового номера в алфавите, обозначаемый *i*. Поиск номера нового символа осуществляется по формуле *l -1 -i*, где *l* - число символов в алфавите.

```
In [12]: def atbash (alfavit, frase):
             j=0
             shifr=""
             for m in frase:
                 i=alfavit.find(m)
                 shifr=shifr+alfavit[len(alfavit)-1-i]
                 j=j+1
             return shifr

In [18]: atbash (alfavit2, "люблю тебя")
Out[18]: 'фвяфваныяб'
```

Рис. 3.5: Реализация шифра Атбаш

4 Выводы

Я ознакомилась с двумя типами шифров простой замены и реализовала их. Результаты работы находятся в репозитории на GitHub, а также есть скринкаст выполнения лабораторной работы.