Отчет по лабораторной работе №1

Дисциплина: Математические основы защиты информации и информационной безопасности

Выполнила Дяченко Злата Константиновна, НПМмд-02-22

Содержание

# 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. 1)

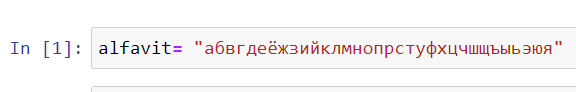


Figure : Figure 1: Создание переменной, содержащей алфавит

## 3.2 Шаг 2

Написала функцию, выполняющую шифрование с помощью шифра Цезаря. Код функции и результат ее использования представлен на Рисунке 2 (рис. -fig. 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.

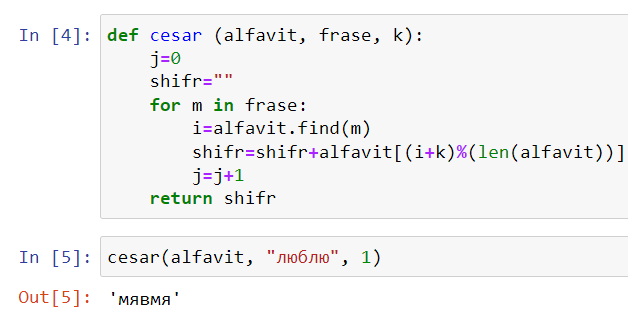


Figure : Figure 2: Реализация шифра Цезаря

## 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) представлена новая функция и результат ее использования для шифрования фразы.

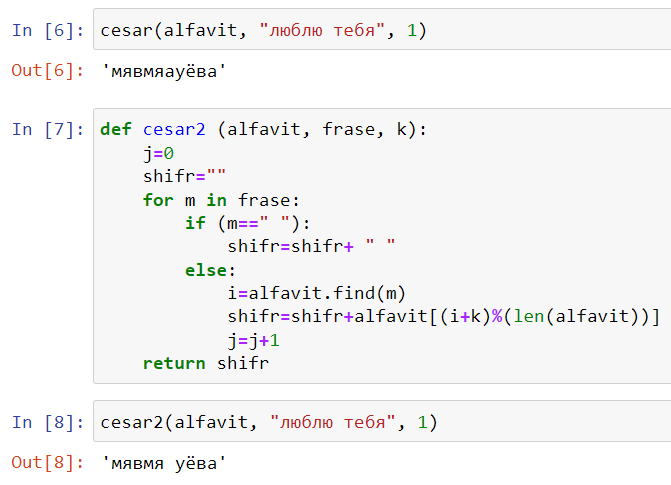


Figure : Figure 3: Изменение функции шифра Цезаря

## 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. 4).

Figure 4: Создание переменной, содержащей алфавит и символ пробел

Figure : Figure 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. 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.

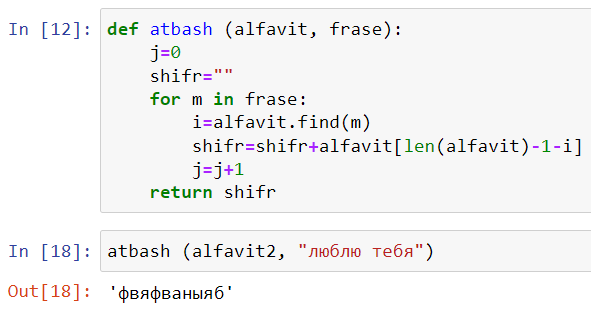


Figure : Figure 5: Реализация шифра Атбаш

# 4 Выводы

Я ознакомилась с двумя типами шифров простой замены и реализовала их. Результаты работы находятся в [репозитории на GitHub](https://github.com/ZlataDyachenko/workD), а также есть [скринкаст выполнения лабораторной работы](https://youtu.be/75rpMm6mq3Y).