Отчёт по лабораторной работе №1

Шифр простой замены

Студент: Гонсалес Ананина Луис Антонио, 1032175329

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 Цель работы

Цель данной лабораторной работы- изучить теорию и реализовать шифры простой замены (Шифр Цезаря и Шифр Атбаш)

# 2 Теоретические сведения

**Шифр Цезаря**

Также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования [1].

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

Математическая модель:

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

Формула

Формула

Формула

Формула

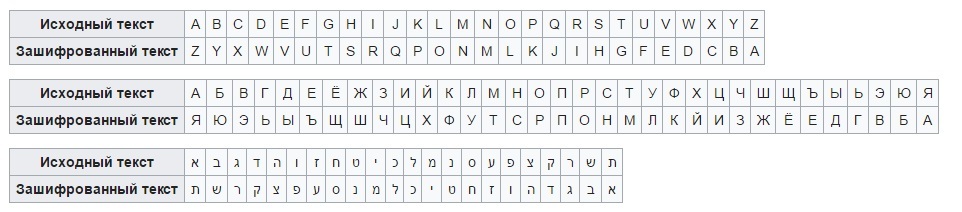
где ~x — символ открытого текста, ~y — символ шифрованного текста, ~n — мощность алфавита, а ~k — ключ.

Шифр Цезаря со сдвигом на 3 (английский алфавит):

A заменяется на D, B заменяется на E, Z заменяется на C и так далее.

**Шифр Атбаш**

Шифр простой замены, использованный для еврейского алфавита и получивший оттуда свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю [2].

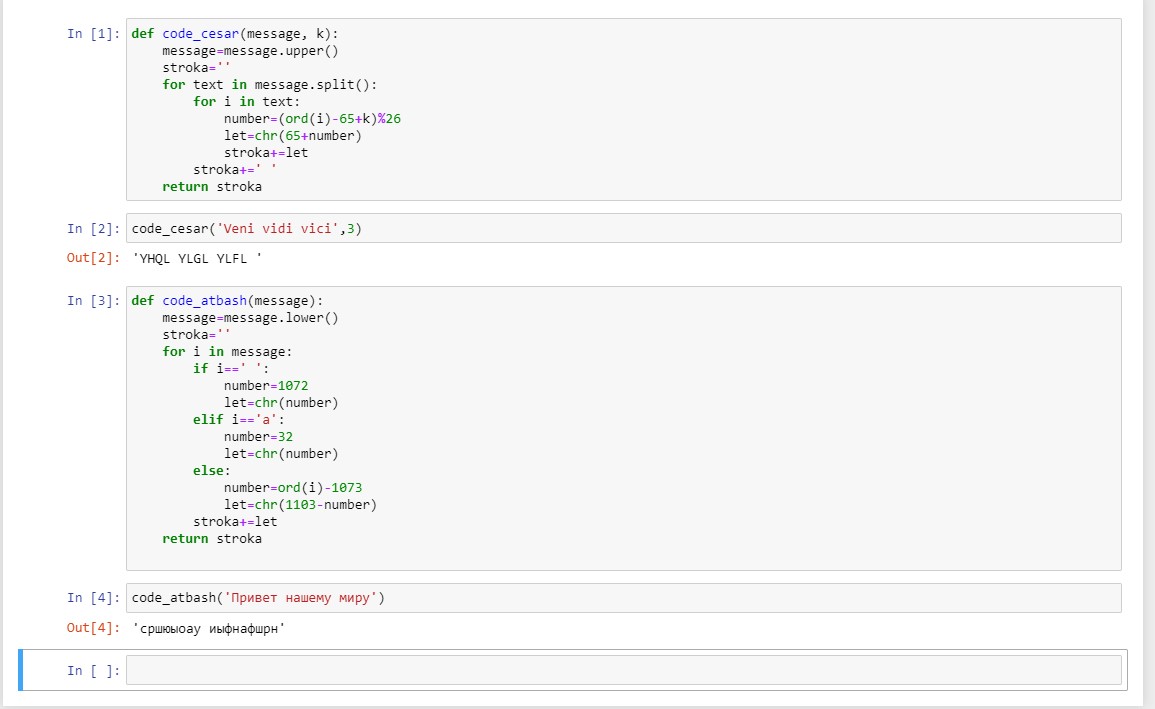


Атбаш

# 3 Выполнение работы

​ Шифр Цезарь:

1. Для начала начал разбирать шифр Цезаря, для этого написал функцию code\_cesar с двумя нужными параметрами (message, к) где message это сам текст который будем зашифровывать, а к это наш произвольный ключ, моем случае 3.
2. Далее написал нужный алгоритм который взял с файла пдф и с интернета.
3. Потом написал само сообщения и вышло оно зашифровано.

* Шифр Атбаш:
  1. Написал функцию code\_atbash с параметром message.
  2. Далее написал нужный алгоритм.
  3. Потом написал само сообщения и вышло оно зашифровано.
* 
* Код

# 4 Выводы

В итоге в данной лабораторной работы я изучил теорию и реализовал шифры простой замены (Шифр Цезаря и Шифр Атбаш)

# Список литературы

1. Шифр Цезаря [Электронный ресурс]. Википедия, 2021. URL: <https://calculatorium.ru/cryptography/caesar-cipher>.

2. Шифр Атбаш [Электронный ресурс]. Википедия, 2021. URL: <http://kriptografea.narod.ru/atbash.html>.