Лабораторная работа 1

Шифры простой замены

Греков Максим Сергеевич

Содержание

# Цель работы

Ознакомиться с шифрами простой замены.

Реализовать шифр Цезаря с произвольным ключом *k*.

Реализовать шифр Атбаш.

# Описание реализации

Для реализации алгоритмов использовались средства языка Python.

Был предложен функционал генерации алфавитов и их добавления. (рис. 1)

Были реализованы как шифраторы, так и дешифраторы рассматриваемых алгоритмов.

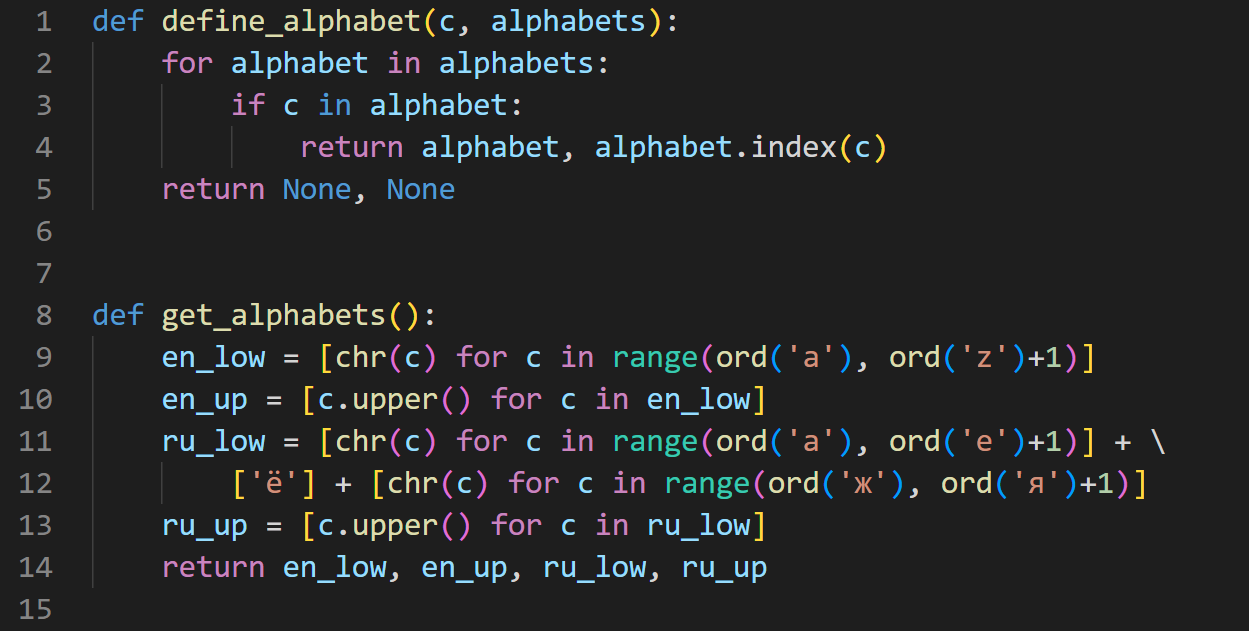


Figure 1: Код генерации алфавитов

# Реализация

## Шифр Цезаря с произвольным ключом k

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. (рис. 2)

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

где — символ открытого текста, — символ шифрованного текста, — мощность алфавита, а — ключ.

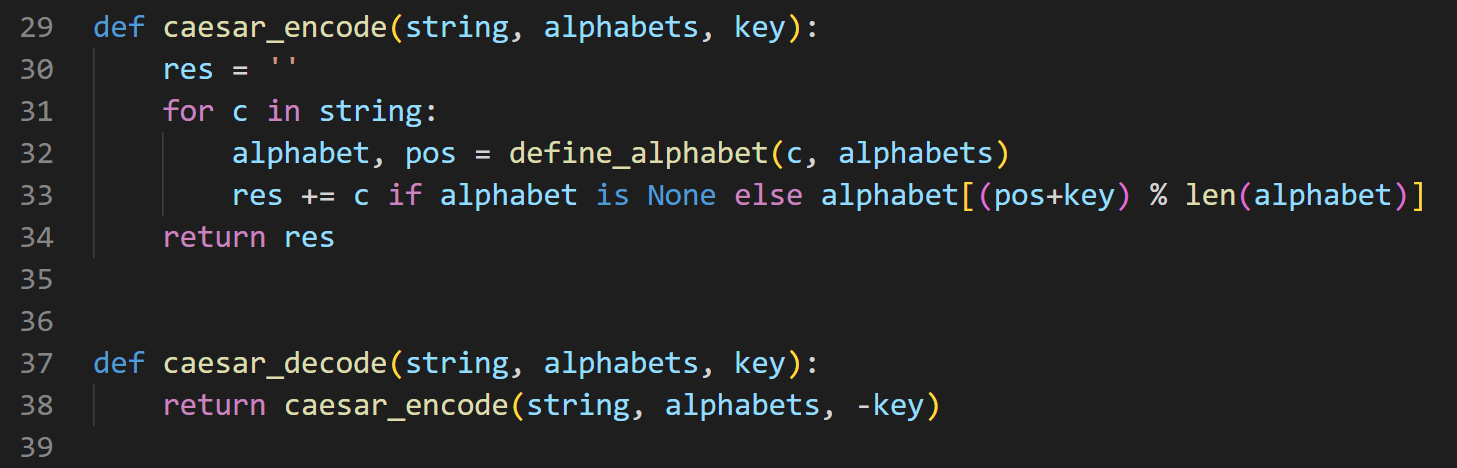


Figure 2: Код Шифра Цезаря

## Шифр Атбаш

Шифр Атбаш — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене -й буквы алфавита буквой с номером , где — число букв в алфавите. (рис. 3)

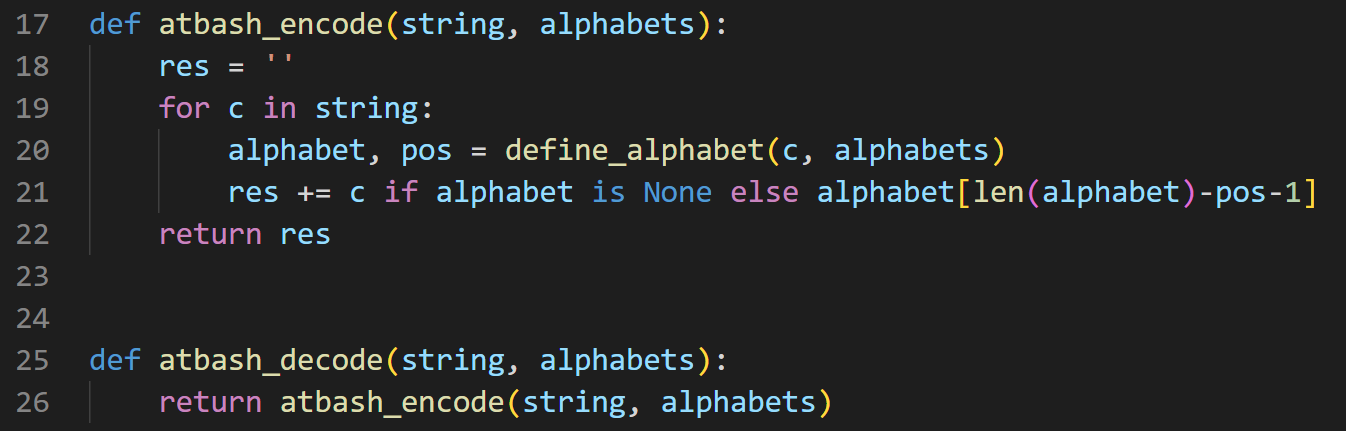


Figure 3: Код Шифра Атбаш

# Вывод

Ознакомились с шифрами простой замены.

Реализовали шифр Цезаря с произвольным ключом *k*.

Реализовали шифр Атбаш.