Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования шифр Цезаря с произвольным ключом k и шифр Атбаш.

# 2 Теоретическое введение

Шифр Цезаря (является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка).

Математически процедуру шифрования можно описать следующим образом: , где - операция нахождения остатка от целочисленного деления на , а - циклическая группа. Обобщение шифра Цезаря на случай произвольного ключа k для латинского алфавита: .

Шифр Атбаш является шифром сдвига на всю длину алфавита. Для реализации шифра целесообразно пользоваться таблицей ASCII и функциями работы с ней: ord и char.

Более подробно см. в [1] и [2].

# 3 Выполнение лабораторной работы

Начнем с реализации шифра Цезаря. Переменные phrase и k соответствуют введенным с клавиатуры тексту и ключу, необходимому для шифрования. Переменная alphabet представляет собой список, состоящий из строчных латинских букв. New\_alphabet - пустой список, который с помощью цикла мы заполняем, делая сдвиг в исходном алфавите (alphabet) на введенные k букв влево. Затем заполняем пустой список (encrypted\_phrase), соответствующий зашифрованному слову. Для этого последовательно, с помощью цикла по переменной j, “берем” буквы из исходного текста (phrase), находим индекс j-той буквы из текста в исходном алфавите (alphabet), а далее в новом алфавите (new\_alphabet) находим букву с найденным только что индексом. Наконец, выводим полученный зашифрованный текст на экран.

Код программы (рис. 1).

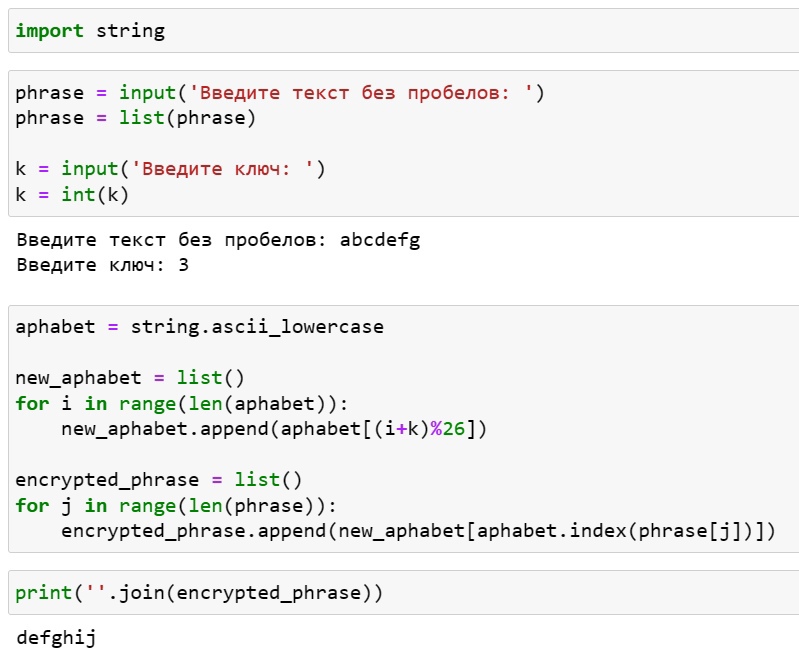


Рис. 1: Реализация шифра Цезаря

Далее реализовываем шифр Атбаш. Аналогично шифру Цезаря вводим текст phrase. Заполняем список alphabet русскими строчными буквами и пробелом с помощью кодов из таблицы ASCII и операции chr. Затем заполняем пустой список (encrypted\_phrase), соответствующий зашифрованному слову. Для этого находим в исходном алфавите индекс, соответствующий зашифрованной букве по формуле: длина\_алфавита - индекс\_буквы\_исходного\_текста - 1. Наконец, выводим полученный зашифрованный текст на экран.

Код программы (рис. 2).

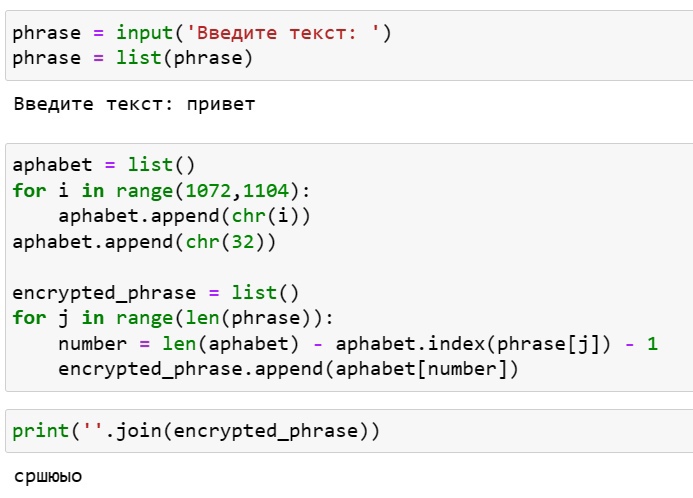


Рис. 2: Реализация шифра Атбаш

# 4 Выводы

В ходе выполнения данной лабораторной работы были реализованы шифры Цезаря и Атбаш на языке программирования Python.

# Список литературы

1. Шифр Цезаря [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F>.

2. Шифр Атбаш [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%D1%88>.