Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Банникова Екатерина Алексеевна

Содержание

# 1 Цель работы

1. Ознакомление с двумя методами шифрования: шифр Цезаря с произвольным ключем k и шифр Атбаш.
2. Их реализация на произвольном языке программирования.

# 2 Задание

1. Реализовать шифр Цезаря с произвольным ключем
2. Реализовать шифр Атбаша.

# 3 Теоретическое введение

Шифр = криптосистема. Закрытый текст = зашифрованный текст. Криптоаналитик — человек, который пытается вскрыть зашифрованное сообщение, которое не ему предназначено. Атака, взлом, вскрытие — попытка узнать исходный текст сообщения без ключа. Дешифровка — взлом или расшифровка самая обычная и законная.

Шифр простой замены — класс методов шифрования, которые сводятся к созданию таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется.

# 4 Выполнение лабораторной работы

## 4.1 Шифр Цезаря

В соответсвии с заданием, была написана программа для шифра Цезаря. Код представлен ниже.

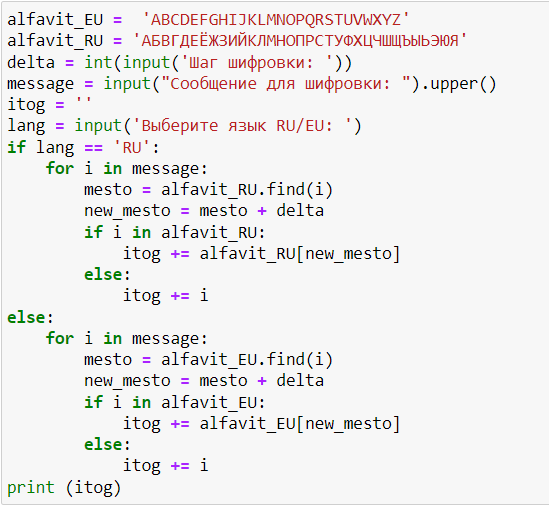


Рис. 1: Код шифра Цезаря

Результаты выполнения программы прдеставленны ниже.

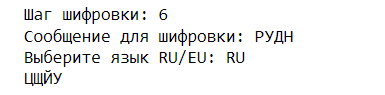


Рис. 2: Результат шифрования

## 4.2 Шифр Атбаш

В соответсвии с заданием, была написана программа для шифра Атбаш. Код представлен ниже.

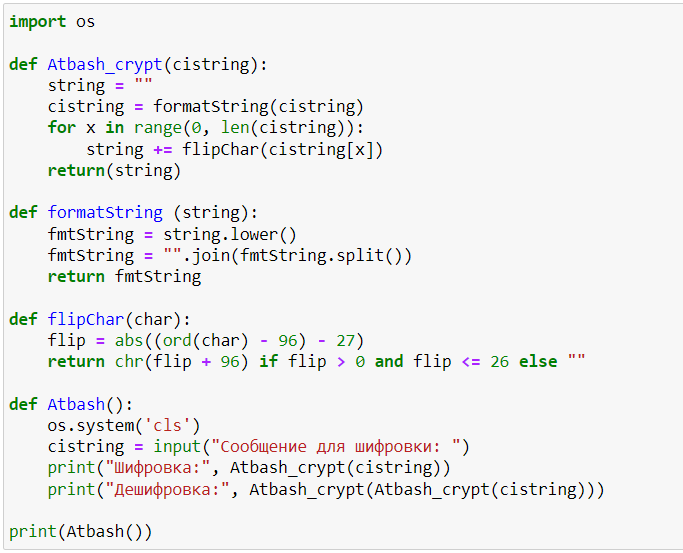


Рис. 3: Код шифра Атбаш

Результаты выполнения программы прдеставленны ниже.

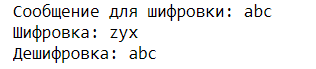


Рис. 4: Результат шифрования

# 5 Выводы

1. Я ознакомилась с помощью питона с двумя методами шифровки: Цезарь и Атбаш.
2. Реализовала эти шифры на питоне.

# 6 Список литературы

1. Википедия. Шифр простой замены. https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80\_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9\_%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D1%8B#:%7E:text=%D0%A8%D0%B8%D1%84%D1%80%20%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9%20%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D1%8B%2C%20%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9%20%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BE%D1%87%D0%BD%D1%8B%D0%B9%2C%D1%81%D0%BE%D0%BF%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%B5%D0%B9%20%D0%B1%D1%83%D0%BA%D0%B2%D0%B0%20%D1%88%D0%B8%D1%84%D1%80-%D1%82%D0%B5%D0%BA%D1%81%D1%82%D0%B0
2. Википедия. Шифр Цезаря.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#:%7E:text=%D0%A8%D0%B8%D1%84%D1%80%20%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F%20%E2%80%94%20%D1%8D%D1%82%D0%BE%20%D0%B2%D0%B8%D0%B4%20%D1%88%D0%B8%D1%84%D1%80%D0%B0%2C%D1%81%D1%82%D0%B0%D0%BD%D0%B5%D1%82%20%D0%94%2C%20%D0%B8%20%D1%82%D0%B0%D0%BA%20%D0%B4%D0%B0%D0%BB%D0%B5%D0%B5
3. Википедия. Шифр Атбаш. https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%D1%88