Лабораторная работа №8

Дисциплина: Информационная безопасность

Боровикова Карина Владимировна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 2 Задание

* Написать программу для шифровки и дешифровки текстов
* Произвести работу по шифровке и дешифровке текстов

# 3 Теоретическое введение

**Шифрование** – это такое преобразование исходного сообщения, которое не позволит всяким нехорошим людям прочитать данные, если они это сообщение перехватят.

**Исходное сообщение** – это, собственно, то, что мы хотим зашифровать. Классический пример — текст.

**Шифрованное сообщение** – это сообщение, прошедшее процесс шифрования.

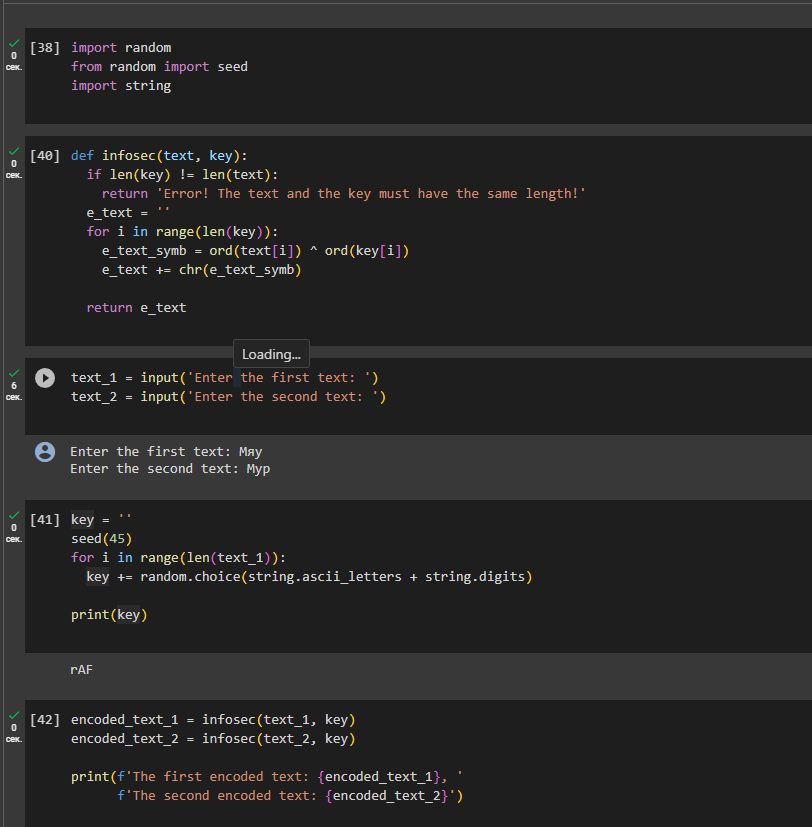
**Шифр** — это сам алгоритм, по которому мы преобразовываем сообщение.

**Ключ** — это компонент, на основе которого можно произвести шифрование или дешифрование.

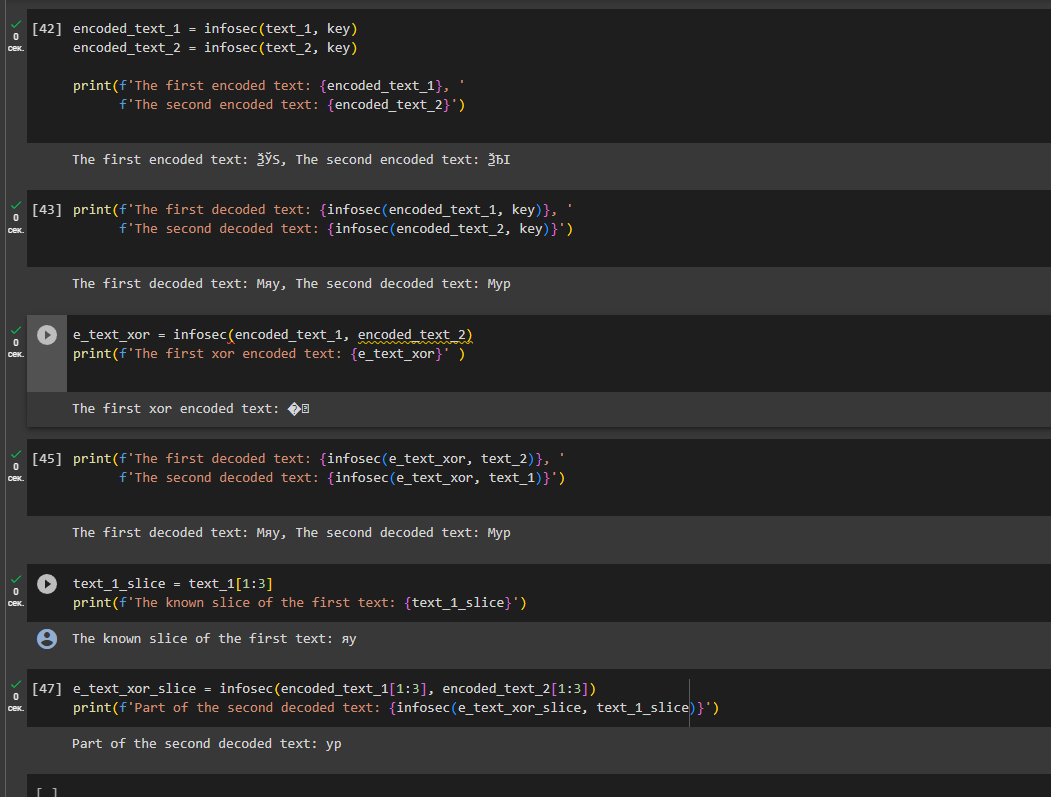
**Алфавит** – это перечень всех возможных символов в исходном и зашифрованном сообщении. Включая цифры, знаки препинания, пробелы, отдельно строчные и заглавные буквы и т.д.

# 4 Выполнение лабораторной работы

1. Пишем код на языке Python: (риc. ?? - ??):



Первая часть кода



Вторая часть кода

* созданной ранее
* при условии, что известны оба шифротекста и один из открытых текстов
* [47]: получение части второго текста (на тех позициях, на которых расположены символы части первого открытого текста) с помощью функции, созданной ранее, при условии, что известны оба шифротекста и часть первого открытого текста

# 5 Выводы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы