Отчет по лабораторной работе 8

Радимов Игорь

Содержание

# Цель работы

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

# Задание

Лабораторная работа подразумевает использование языков программирования для создания программы для щифрования и дещифрования в режиме однократного гаммирования при известном ключе.

# Теория

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных.

# Выполнение работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования и расшифруем два текста, зная только один из них и не зная ключа.(рис 1-2)

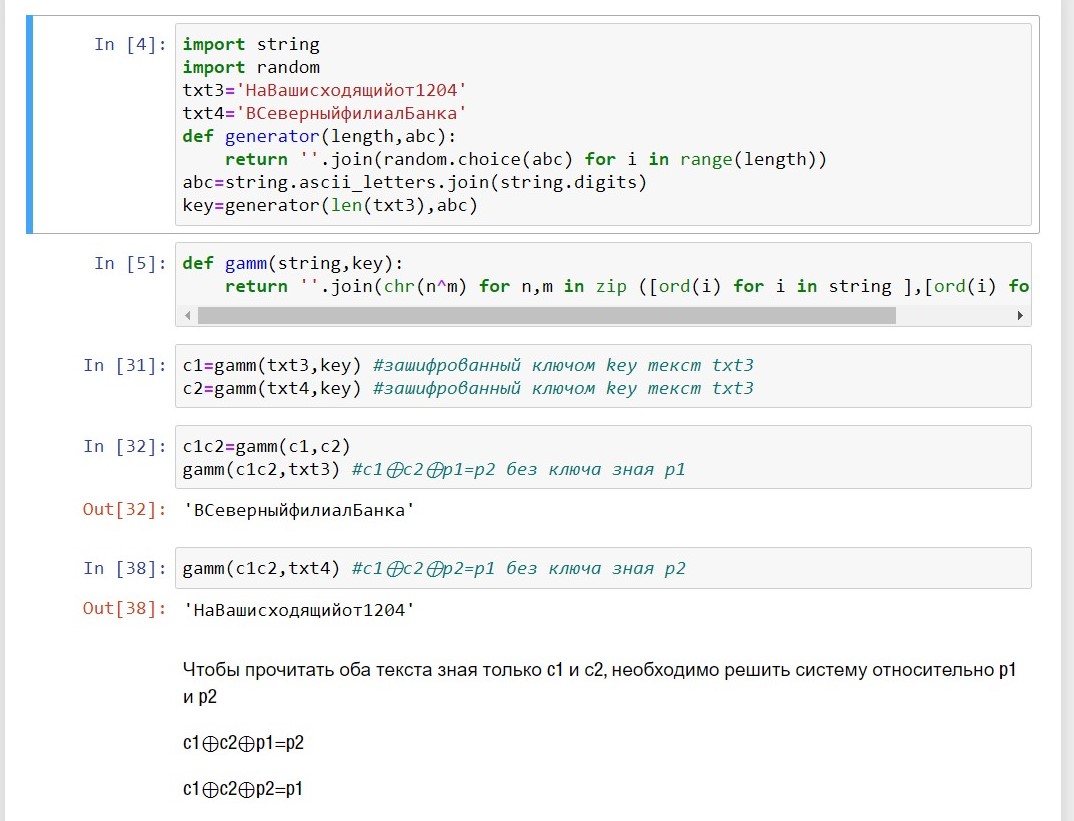


Figure 1: рис.1. Программа, часть 1.

# Библиография

1. ТУИС РУДН
2. Статья на сайте “https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5”

# Выводы

Во время выполнения лабораторной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.