Лабораторная работа №8

Элементы криптографии. Шифрование различных исходных текстов одним ключом

Кувшинова К.О. группа НФИ-02-19

Содержание

# 1 Цель работы

Целью данной лабораторной работы является освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 2 Указания к работе

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой: (fig. 1)

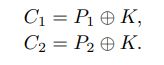


Figure 1: Схема однократного гаммирования одним ключом двух видов открытого текста

# 3 Задание к лабораторной работе

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

# 4 Выполнение лабораторной работы

1. Импортируем необходимые для работы библиотеки (fig. 2)

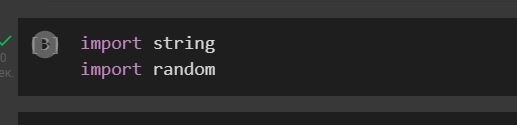


Figure 2: Импорт библиотек

1. Напишем функции формирования ключа, перевода данных в 16 систему и шифрования текста. (fig. 3)

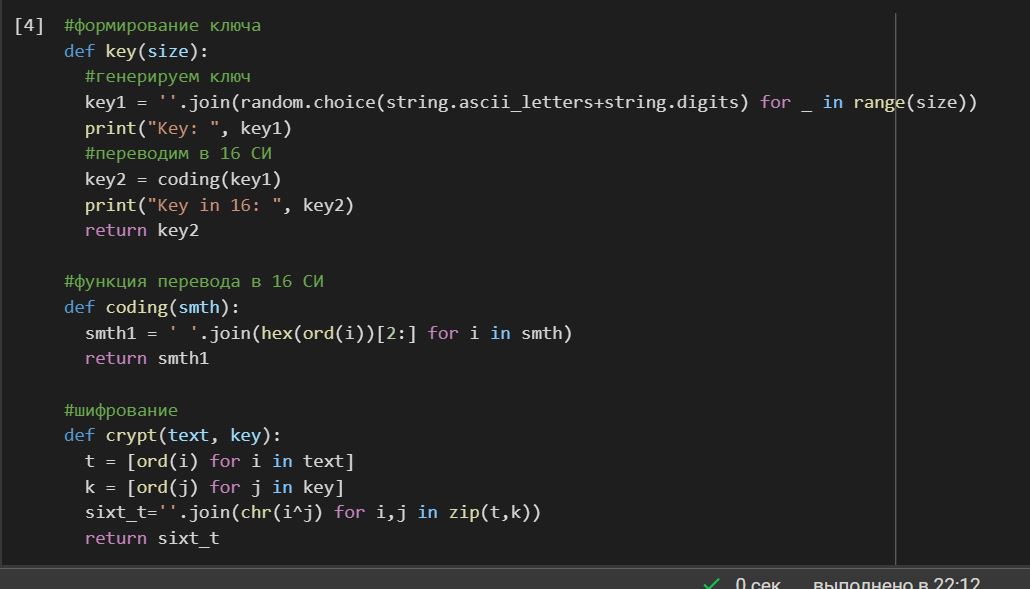


Figure 3: Функции формирования ключа, перевода данных в 16 систему и шифрования

1. Зашифруем и дешифруем тексты P1 и P2 2 в режиме однократного гаммирования. (fig. 4)

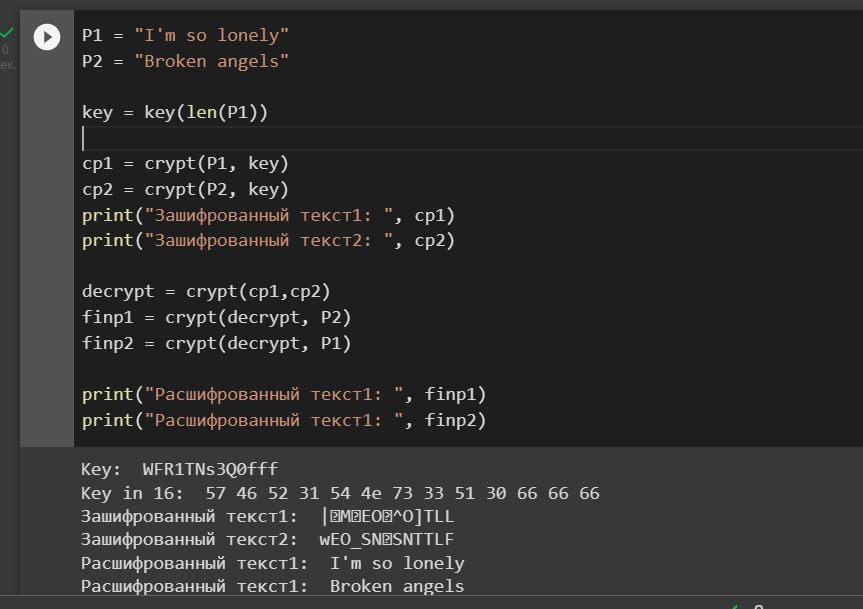


Figure 4: Шифрование и дешифрование текстов

# 5 Вывод

В ходе выполнения лабораторной работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 6 Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 3 с. [^1]: Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.