Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Кувшинова К.О. группа НФИ-02-19

Содержание

# 1 Цель работы

Целью данной лабораторной работы является освоить на практике применение режима однократного гаммирования.

# 2 Указания к работе

*Гаммирование* представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежащего сокрытию текста.

# 3 Задание к лабораторной работе

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 4 Выполнение лабораторной работы

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

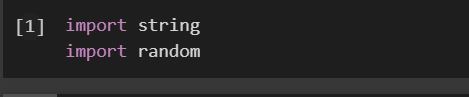


Figure 1: Импорт библиотек

1. Напишем функции формирования ключа, перевода данных в 16 систему и шифрования текста. (fig. 2)

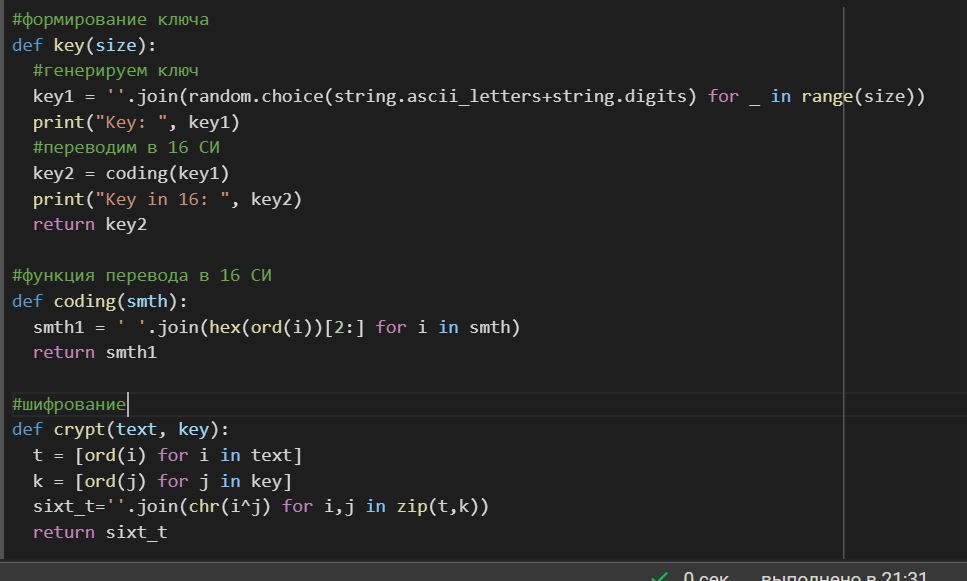


Figure 2: Функции формирования ключа, перевода данных в 16 систему и шифрования

1. Зашифруем и дешифруем предложенный текст с помощью сгенерированного ключа. (fig. 3)

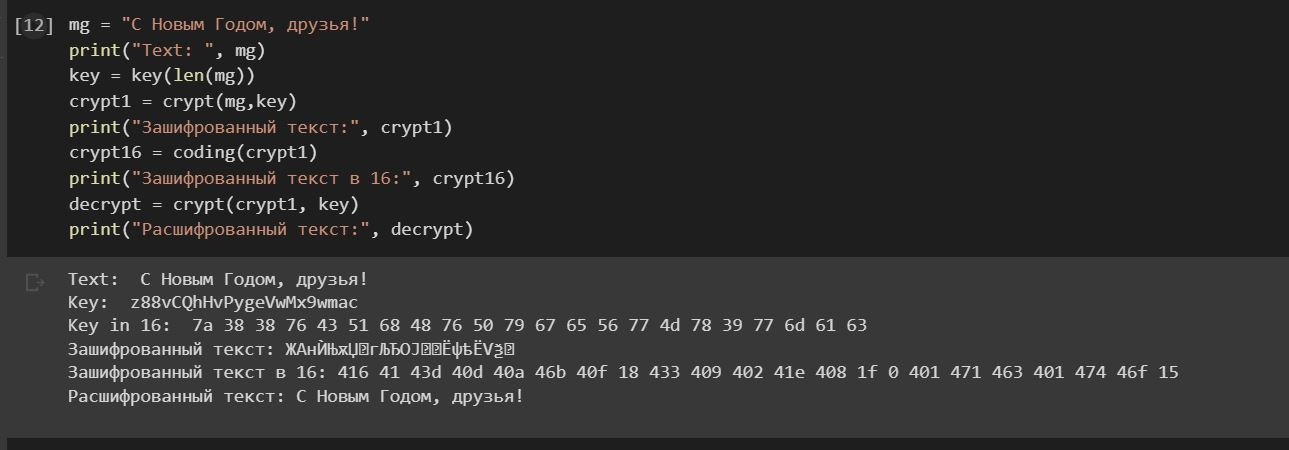


Figure 3: Шифрование и дешифрование текста

1. Определим ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. Из нового ключа предложенный текст дешифруется верно.(fig. 4)

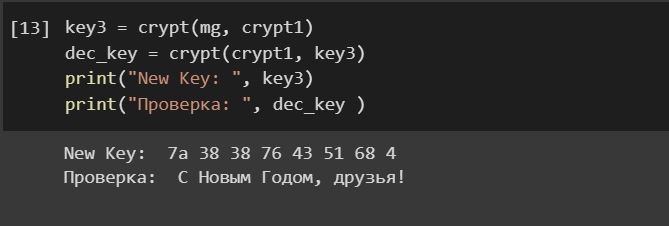


Figure 4: Шифрование и дешифрование текста

# 5 Вывод

В ходе выполнения лабораторной работы мы освоили на практике применение режима однократного гаммирования.

# 6 Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Элементы криптографии. Однократное гаммирование [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 3 с. [^1]: Элементы криптографии. Однократное гаммирование.