Отчёт по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Кондрашина Мария Сергеевна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования

# 2 Теоретические сведения

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.[1]

# 3 Выполнение лабораторной работы. Создание программы

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. (fig. 1) - (fig. 2)

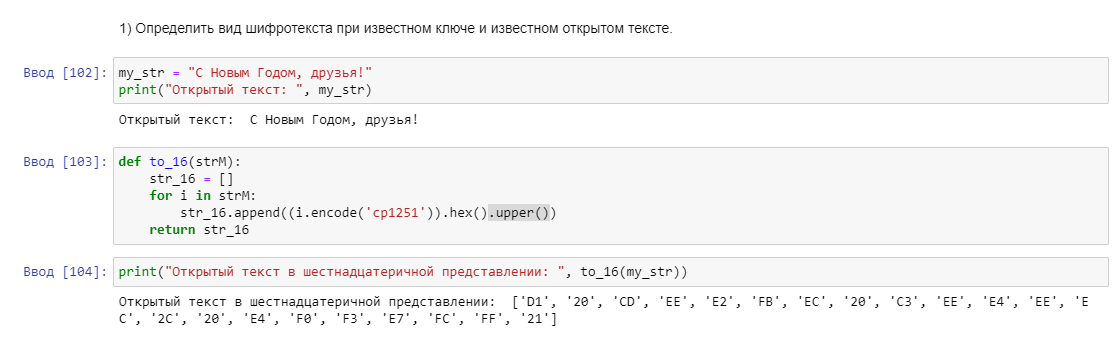


Figure 1: Работа с открытым текстом. Перевод в шестнадцатеричное представление.



Figure 2: Создание ключа и шифрование текста

1. Оределить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста,представляющий собой один из возможных вариантов прочтения открытого текста.(fig. 3)

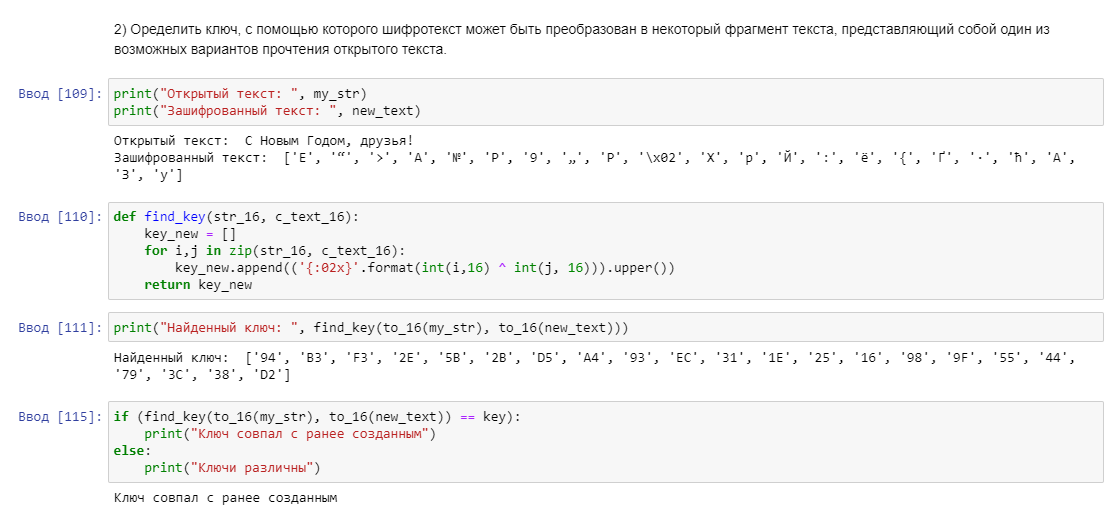


Figure 3: Определение ключа по отрытому и зашифрованному тексту

# 4 Выводы

* Выполнила лабораторную работу №7.
* Освоила на практике применение режима однократного гаммирования

# 5 Список литературы

1. Методические материалы курса. “Информационная безопасность компьютерных сетей” Кулябов Д. С., Королькова А. В., Геворкян М. Н.