Отчет по лабораторной работе №7

по дисциплине: Информационная безопасность

Го Чаопэн

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Задание

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.

# Теоретическое введение

* Шифрование – это технология кодирования и раскодирования данных.Зашифрованные данные -это результат применения алгоритма для кодирования данных с целью сделать их недоступными для чтения. Данные могут быть раскодированы в исходную форму только путем применения специальный ключа [1].
* Гаммирование — это наложение (или снятие при расшифровке сообщений) на открытое (или зашифрованное) сообщение так называемой криптографической гаммы. Криптографическая гамма — это последовательность элементов данных, которая вырабатывается с помощью определенного алгоритма. [2].

# Выполнение лабораторной работы

1. Импортируем необходимые модули ([1](#fig:001)).

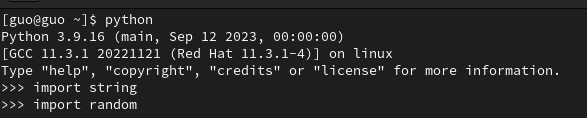


Figure 1: Импорт модулей

1. Создадим функции для преобразования данных в шестнадцатеричный формат, генерации ключа и кодирования, декодирования данных ([2](#fig:002)).

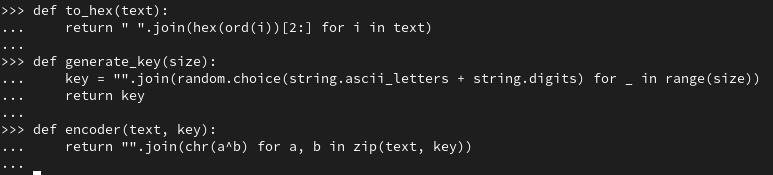


Figure 2: Функции

1. Закодируем и декодируем строку “С Новым годом, друзья!” ([3](#fig:003)).

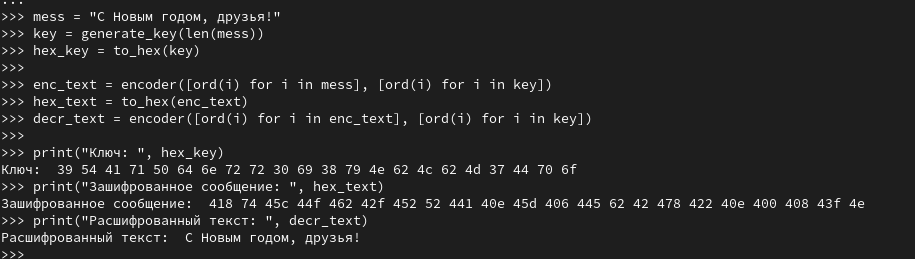


Figure 3: Кодирование и декодирование строки

1. Получим ключ, с помощью которого получим сообщения “С Новым годом, семья”, “С Новым годом, учителя” вместо “С Новым годом, друзья!” при декодировании. Воспользуемся симметричностью кодирования([4](#fig:004)).

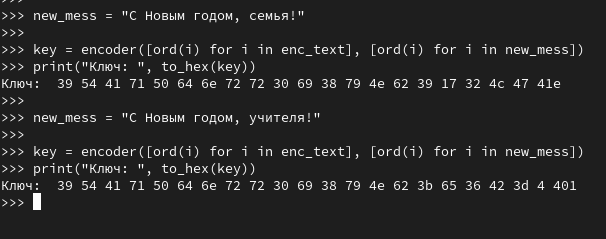


Figure 4: Получение ключа для другого прочтения открытого текста

# Выводы

В рамках данной лабораторной работы было освоено на практике применение режима однократного гаммирования.

# Список литературы

1. Шифрование информации: как защитить свои данные [Электронный ресурс]. URL: <https://gb.ru/blog/shifrovanie-informatsii/>.

2. Гаммирование [Электронный ресурс]. URL: <https://science.fandom.com/ru/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>.