Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Тарусов Артём Сергеевич

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 (fig. 1).

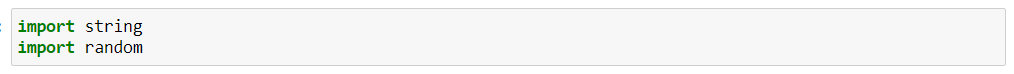


Рис. 1: Импорт

1. Создадим функцию для преобразования данных в шестнадцатеричный формат (fig. 2).

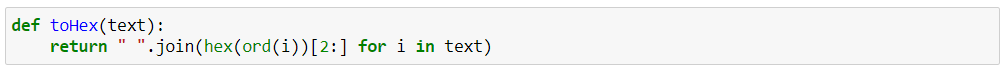


Рис. 2: Функция toHex

1. Напишем функцию, генерирующую ключ (fig. 3).

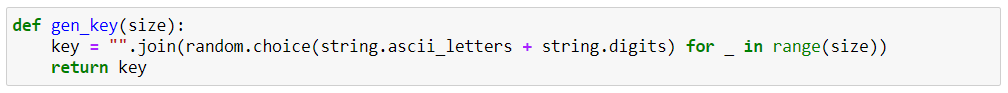


Рис. 3: Функция gen\_key

1. Реализуем функцию для кодирования и декодирования данных (fig. 4).

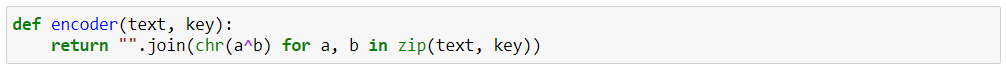


Рис. 4: Функция encoder

1. Закодируем и декодируем строку “С Новым годом, друзья!” (fig. 5).

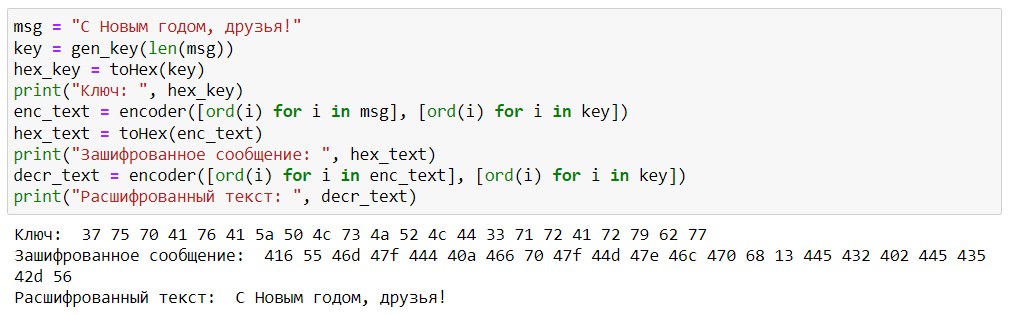


Рис. 5: Кодирование и декодирование строки

1. Получим ключ, с помощью которого получим сообщение “С Новым годом, коллега”, вместо “С Новым годом, друзья!” при декодировании. Воспользуемся симметричностью кодирования(fig. 6).

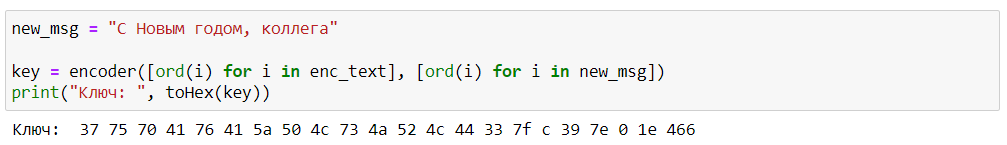


Рис. 6: Получение ключа для другого прочтения открытого текста

# Выводы

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

# Список литературы

[1] https://www.kaspersky.ru/resource-center/definitions/encryption

[2] https://xakep.ru/2019/07/18/crypto-xor/