Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование.

Казакова Виктория Алексеевна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 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.

# 3 Ход работы

1. Импорт необходимых модулей, создание функций для перевода данных в 16ричный формат, функции для ключа и функцию кодирования и декодирования (рис. [1](#fig:001)).

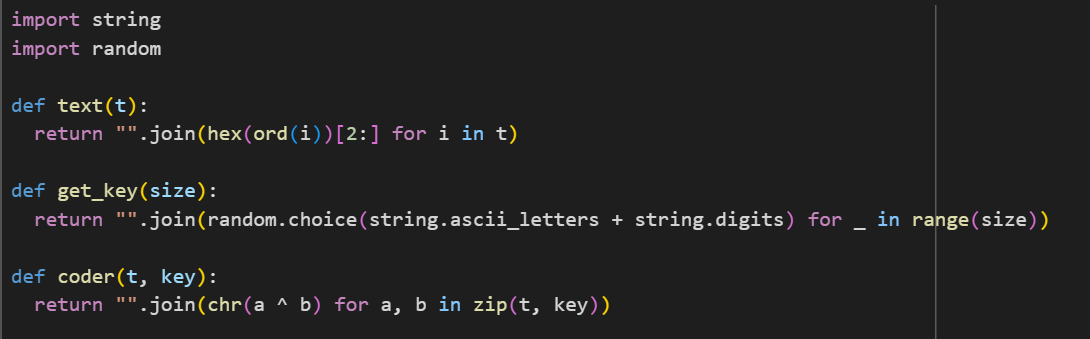


Figure 1: Подготовка необходимых функций

1. Прописываю основной код, в котором используются все написанные ранее функции (рис.@fig:002).

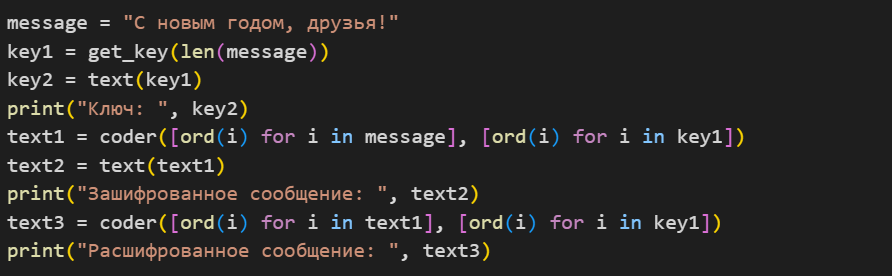


Figure 2: Кодирование и декодирование строки

1. Результат работы программы: ([3](#fig:003)).

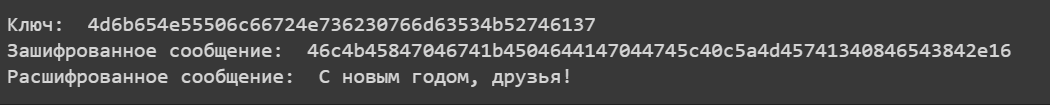


Figure 3: Результат

# 4 Выводы

В ходе работы было освоено на практике применение режима однократного гаммирования.

# 5 Список литературы

1. [Методический материал] [https://esystem.rudn.ru/pluginfile.php/2090284/mod\_resource/content/2/007-lab\_crypto-gamma.pdf]
2. [Сайт для поиска команд] [https://www.ibm.com/]
3. [Google Colab] [https://colab.research.google.com/?hl=ru]