Отчет по лабораторной работе №7

Информационная безопасность

Чекалова Лилия Руслановна

Содержание

# 1 Цель работы

* Освоить на практике применение режима однократного гаммирования.

# 2 Задание

* Написание программы
* Зашифровка текста по открытому тексту и известному ключу
* Определение ключа по открытому и зашифрованному тексту

# 3 Теоретическое введение

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.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Более подробно о см. в [1].

# 4 Выполнение лабораторной работы

Для выполнения лабораторной работы я написала программу для зашифрования и расшифровки текста. Импортировав необходимые библиотеки, я задала три функции — для генерации ключа по размеру сообщения (выбор случайных букв в кодировке ASCII), для перевода сообщения и ключей в 16-ричную систему (получение кода символа и перевод его в 16-ричную систему) и для шифрования (поэлементный XOR) (рис. [1](#fig:001)).

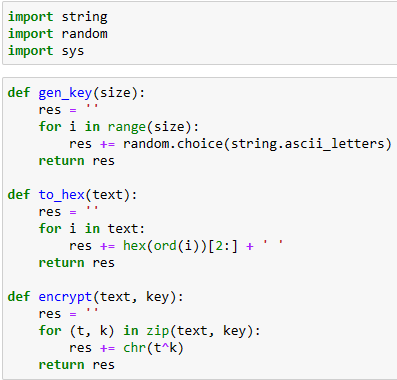


Figure 1: Программа, 1

Далее я задала изначальное открытое сообщение, сгенерировала ключ, закодировала сообщение с помощью этого ключа, а также перевела все в 16-ричную систему. После этого я раскодировала закодированное сообщение, чтобы проверить правильность работы программы, и определила используемый ключ по открытому сообщению и закодированному сообщению (рис. [2](#fig:002)).

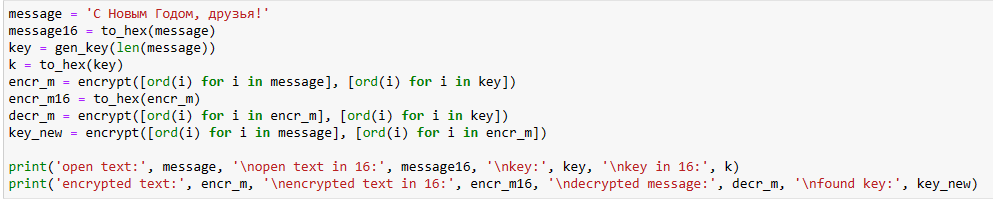


Figure 2: Программа, 2

Полученные сообщения и ключи я вывела на экран (рис. [3](#fig:003)). Сообщение было успешно закодировано и раскодировано, а найденный ключ совпадает с тем, который был сгенерирован для кодирования.

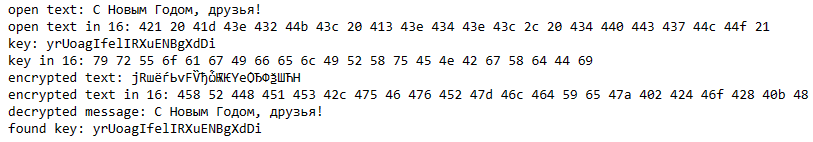


Figure 3: Результат запуска программы

# 5 Выводы

В результате лабораторной работы я получила представление о базовых элементах криптографии и освоила на практике применение режима однократного гаммирования, написав программу, позволяющую зашифровывать и расшифровывать тексты и определять использованные для этого ключи.

# Список литературы

1. Элементы криптографии. Однократное гаммирование [Электронный ресурс]. URL: <https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/content/2/007-lab_crypto-gamma.pdf>.