Отчет по лабораторной работе №8

Информационная безопасность

Чекалова Лилия Руслановна

Содержание

# 1 Цель работы

* Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 2 Задание

* Написание программы
* Зашифровка текстов по открытым текстам и известному ключу
* Расшифровка текстов без использования ключа

# 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 представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста.

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 две функции — для генерации ключа по размеру сообщения (выбор случайных букв в кодировке ASCII) и для шифрования (поэлементный XOR) (рис. [1](#fig:001)).

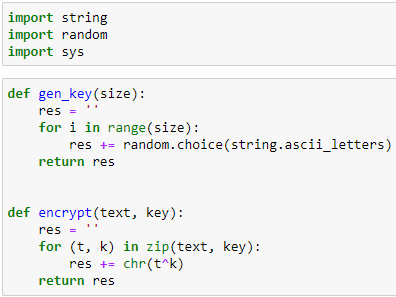


Figure 1: Программа, 1

Далее я задала два открытых сообщения одинаковой длины, сгенерировала ключ и закодировала сообщения с помощью этого ключа. После этого я ввела промежуточную переменную temp, в которой сохранила результат поэлементного XOR между двумя зашифрованными сообщениями. Чтобы расшифровать первый текст, я произвела поэлементный XOR temp и второго открытого сообщения, а для расшифровки второго сообщения — поэлементный XOR temp и первого сообщения (рис. [2](#fig:002)).

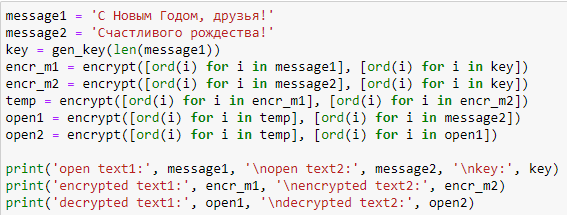


Figure 2: Программа, 2

Полученные сообщения я вывела на экран (рис. [3](#fig:003)). Сообщения были успешно закодированы с помощью заданного ключа и раскодированы без использования этого ключа.

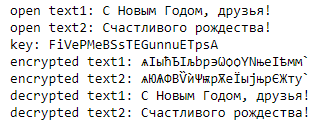


Figure 3: Результат запуска программы

# 5 Выводы

В результате лабораторной работы я закрепила знания о базовых элементах криптографии и освоила на примере шифрования двух текстов одним ключом применение режима однократного гаммирования, написав программу, позволяющую зашифровывать тексты и расшифровывать их, даже не зная ключа.

# Список литературы

1. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом [Электронный ресурс]. URL: <https://esystem.rudn.ru/pluginfile.php/2090286/mod_resource/content/2/008-lab_crypto-key.pdf>.