Отчет по лабораторной работе №7

Информационная безопасность

Байрамгельдыев Довлетмурат

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

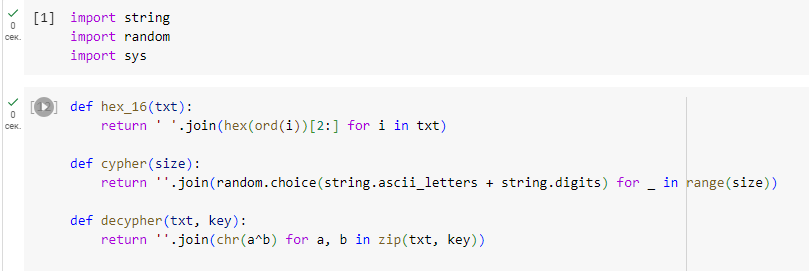
Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами 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 [**lab-theory?**].

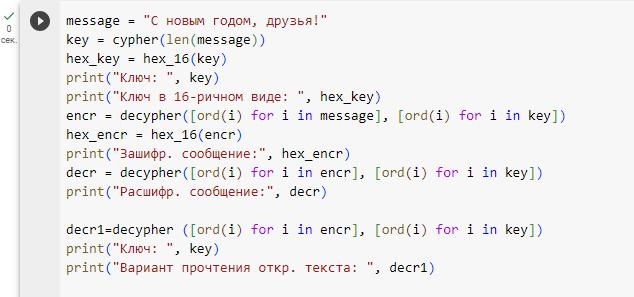
# 4 Выполнение лабораторной работы

Для выполнения лабораторной работы я написал функции для перевода в 16-ричный вид, шифрования и дешифрования, а также импортировал нужные библиотеки (рис. ??).



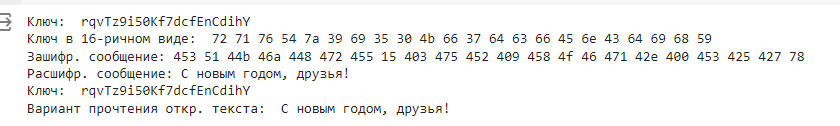
Программа, 1

Далее я задал изначальное открытое сообщение, сгенерировал ключ, закодировал сообщение с помощью этого ключа, а также перевел все в 16-ричную систему. После этого раскодировал закодированное сообщение, чтобы проверить правильность работы программы, и определил используемый ключ по открытому сообщению и закодированному сообщению (рис. ??).



Программа, 2

Полученные сообщения и ключи вывел на экран (рис. ??). Сообщение было успешно закодировано и раскодировано, а найденный ключ совпадает с тем, который был сгенерирован для кодирования.



Результат запуска программы

# 5 Выводы

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

# Список литературы

1. Элементыкриптографии.Однократноегаммирование[Электронныйресурс].URL: https://esystem.rudn.ru/pluginfile.php/2090284/mod\_resource/content/2/007 lab\_crypto-gamma.pdf.