Отчёт по лабораторной работе №7

Попов Олег Павлович

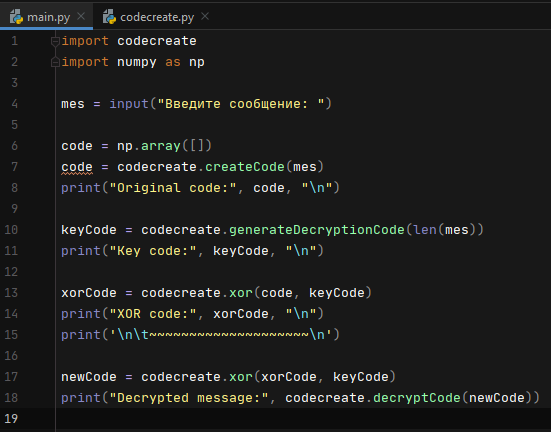
Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Выполнение лабораторной работы

Ниже представлен код консольного приложения для работы с шестнадцатеричными кодами символов.



Выше указан main файл программы, в котором находится исключительно реализация всех функций, написанных в файле createcode.

Порядок выполнения команд в файле main следующий: на вход программе дается ввод mes; все символы mes обрабатываются через функцию createCode(), которая создает массив шестнадцатеричных кодов; генерируется рандомный ключ через функцию generateDecryptionCode(); сообщение кодируется через функцию однократного гаммирования xor(); все вышеперечисленное выводится на экран; и под конец сообщение xorCode дешифруется через функцию xor() [newCode] и выводится на экран.



Данный код представляет собой файл createcode. Здесь, как уже было сказано ранее, записаны все функции.

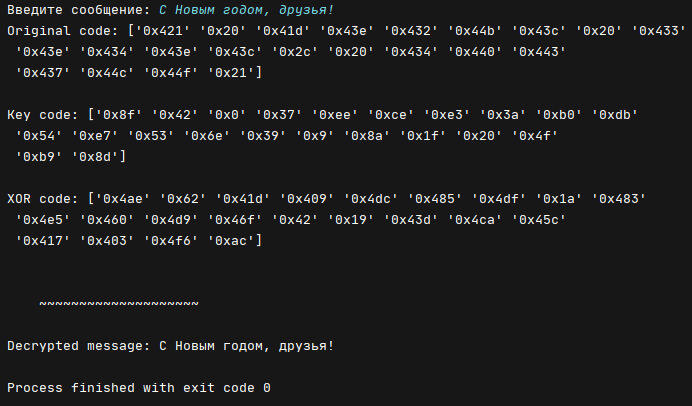
Функция createCode(): берет на вход сообщение типа string и для каждого символа сообщения генерирует его шестнадцатеричный код ascii.

Функция generateDecryptionCode(): создает рандомный ключ определенного размера s.

Функция xor(): реализует “исключающее или” для code1 и code2 и выводит зашифорованное сообщение в виде массива кодов.

Функция decryptCode(): нужна для расшифровки кодов code и вывода сообщения. Для реализации данной функции пришлось отдельно записывать символы кириллицы и создавать для них массив кодов, так как функция bytes.fromhex() не распознает трехзначные шестнадцатеричные коды (все коды кириллицы трехзначные). В итоге, функция проверяет, есть ли код в массиве кириллицы, и выводит символы.

В итоге, вывод программы выглядит так:



# Выводы

В ходе данной работы я ознакомился с однократным гаммированием и реализовал его в приложении командной строки.