МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В. Г. ШУХОВА»

(БГТУ им. В.Г. Шухова)

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Лабораторная работа №1

по дисциплине «Криптографические интерфейсы»

тема: «Основы работы с CNG»

Выполнил: ст. группы КБ-41

Зотова А.И.

Проверил: ст. пр. Смакаев А.В.

Белгород,

2021 г.

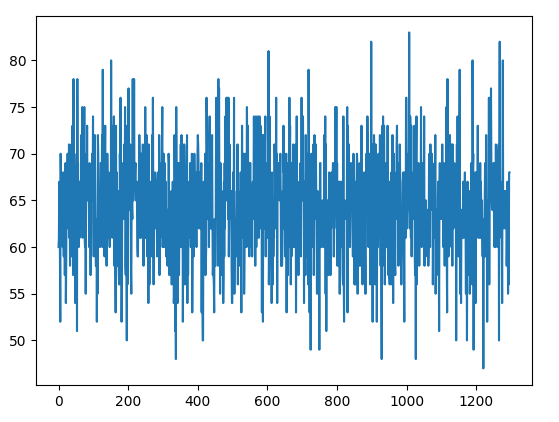
Цель работы: ознакомится с криптографическим API операционных систем семейства Windows. Разработать консольное приложение, использующее CNG для генерации ключа и шифрования/дешифрования файлов. Исследовать лавинный эффект при разных режимах сцепления блоков.

Задание:

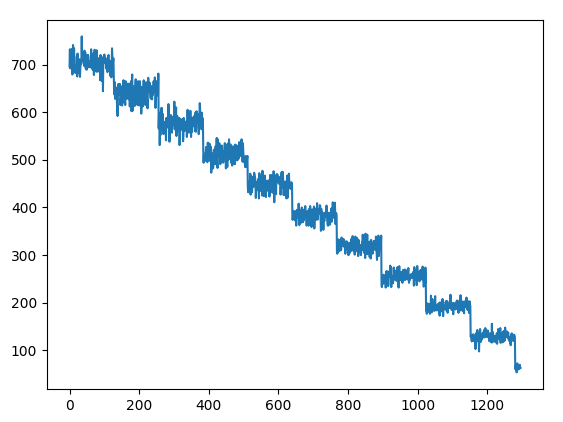
1. Разработать консольное приложение, позволяющее генерировать ключи шифрования и шифровать/дешифровать файлы симметричным шифром AES с использованием криптографического API CNG.
2. Исследовать лавинный эффект при разных режимах сцепления блоков (ECB, CBC, CFB). В ходе исследования нужно изменить один бит в открытом тексте и построить график.

Программа берет исходный текст из файла *plainText.txt,* ключ из файла *key.txt,* и вектор инициализации из файла *IV.txt* и шифрует исходный текст шифром AES. Исходный шифрованный текст сравнивается с шифрованными текстами с допущенной ошибкой в исходном тексте. Номер ошибочного бита и количество отличающихся битов в новом шифрованном тексте записывается в файл *exp.txt*.

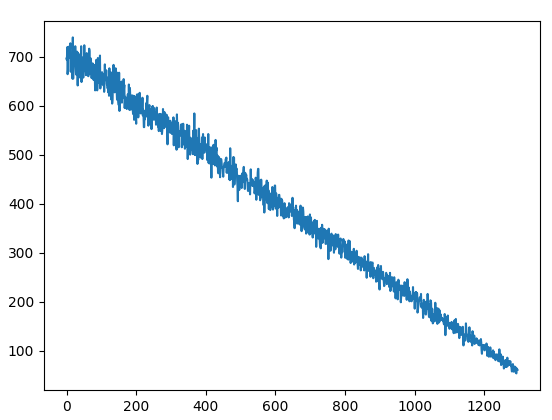
По данным из файла строится график, в котором ось X это номер измененного бита, а ось Y количество измененных битов в шифрованном тексте.

**

*Рис. 1 – График при режиме сцепления ECB.*

**

*Рис. 2 – График при режиме сцепления CBC.*

**

*Рис. 3 – График при режиме сцепления CFB.*

Вывод:

ECB – изменение бита в одном из блоков текста никак не влияет на процесс шифрования остальных блоков текста. Поэтому в число измененных битов во всем шифрованном тексте, входят лишь биты от блока, в котором совершена ошибка.

CBC – изменение бита в одном из блоков текста влияет на процесс шифрования последующих блоков текста. Поэтому в число измененных битов во всем шифрованном тексте, входят биты от блока, в котором совершена ошибка и следующих за ним блоков.

CFB – аналогично CBC. С отличием лишь в том, что измененный бит подмешивается уже после процесса шифрования вектора инициализации, а значит график будет более плавным.