Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ОТЧЕТ

О ЛАБОРАТОРНОЙ РАБОТЕ

Лабораторная работа №3

по теме:

«Применение блочных шифров»

Исполнитель, студент группы 201-361 \_\_\_\_\_\_\_\_\_\_\_\_ Н.А. Фельдбуш

Москва, 2023

**Постановка задачи**:

Напишите программу, шифрующую изображение tux.png (формат не принципиален) с помощью шифра AES. Режимы шифрования: ECB, CBC, CFB и OFB (нужно получить четыре варианта зашифрованного изображения). В учебных целях заголовочную часть файла зашифровывать не нужно. Сравните скорости выполнения алгоритмов и результаты шифрования.

**Ход работы:**

Выполним поставленную задачу при помощи средств языка программирования Python. Для реализации используются две основных функции (рис.1).



Рисунок 1 – Основные функции

Функция “main” выполняет основную поставленную задачу. С помощью библиотеки “subprocess” и “openssl.exe” происходит шифрование файла четырьмя разными способами: “aes-256-ecb”, “aes-256-cbc”, “ aes-256-cfb”, “ aes-256-ofb”. Так же в функции измеряется время необходимое для шифрования, а также размер зашифрованных файлов.

Функция “decode” принимает в себя путь к файлу, а также режим шифрования с помощью, которого файл был зашифрован. С помощью этой информации файл дешифруется и создается новый расшифрованный файл.