ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ОТЧЕТ  
ПО ЛАБОРАТОРНОЙ РАБОТЕ

ПО ДИСЦИПЛИНЕ

«Защита информации»

Руководители \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.А. Харченко

Москва 2023

СПИСОК ИСПОЛНИТЕЛЕЙ

Студ. группы 201-361 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Е. Сильченко

**Ход работы:**

1. Генерируем ключ используя OpenSSSL и записываем его в файл рисунок 1.



Рисунок 1 – Генерация ключа.

1. Создаем 2 временных файла, для хранения тела изображения (без заголовка) и для хранения зашифрованного тела изображения, эти же файлы будут использоваться для расшифровки файла только наоборот, в первом будет хранится зашифрованное тело изображения, во втором расшифрованное. Также создаем два выходных файла для зашифрованного файла (создан ниже) и для расшифрованного. В метод для шифрования передаем следующие параметры: режим шифрования, исходное изображение, ключ, зашифрованное изображение и 2 временных файла рисунок 2.

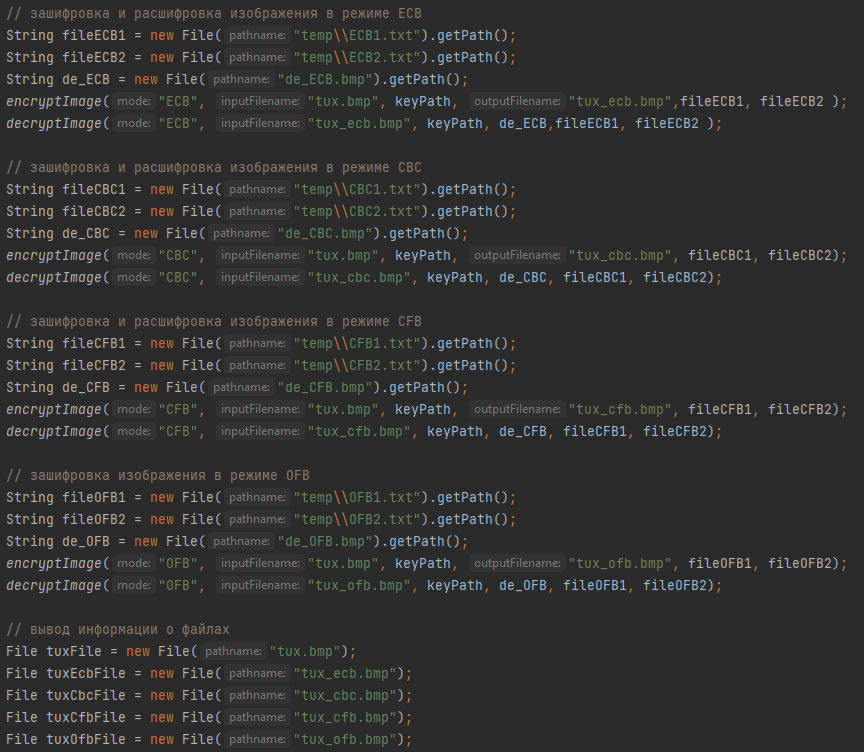


Рисунок 2 – Основная часть программы.

1. В методе для шифрования изображения мы получаем байты заголовка (в данном случае заголовок равен 110 байт) и тело изображения. Тело изображения записываем в первый временный файл. Далее в OpenSSL мы передаем режим шифрования который передается этому методу, первый временный файл в котором хранится тело изображения и файл в который будет помещено зашифрованное тело изображения и ключ. Далее мы считываем полученный файл и записываем зашифрованное тело в переменную «shBytes». Далее мы записываем в файл который мы получим на выходе сначала нетронутый заголовок, потом зашифрованное тело рисунок 3.

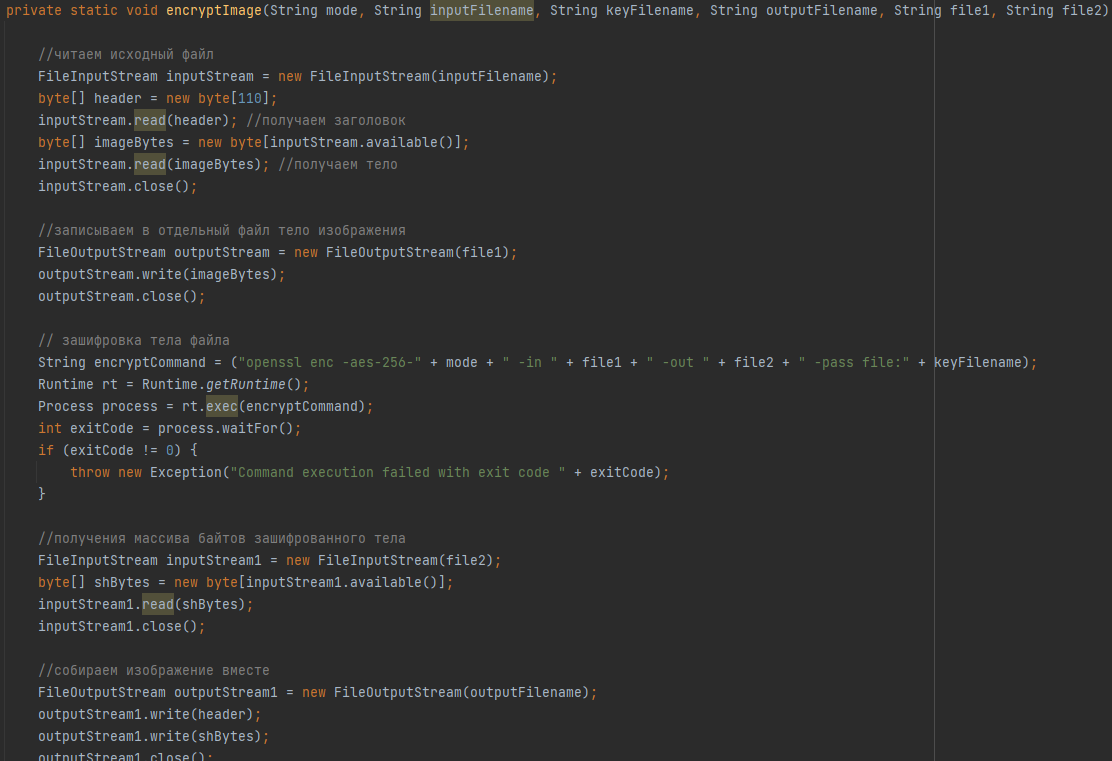


Рисунок 3 – encryptImage.

1. Метод для расшифровки аналогичен методу шифрования, только в OpenSSL передается дополнительная опция «-d» для расшифровки файла. И в этом методе в первом файле будет хранится зашифрованное тело, а во втором расшифрованное тело изображения. Метод представлен на рисунке 5.

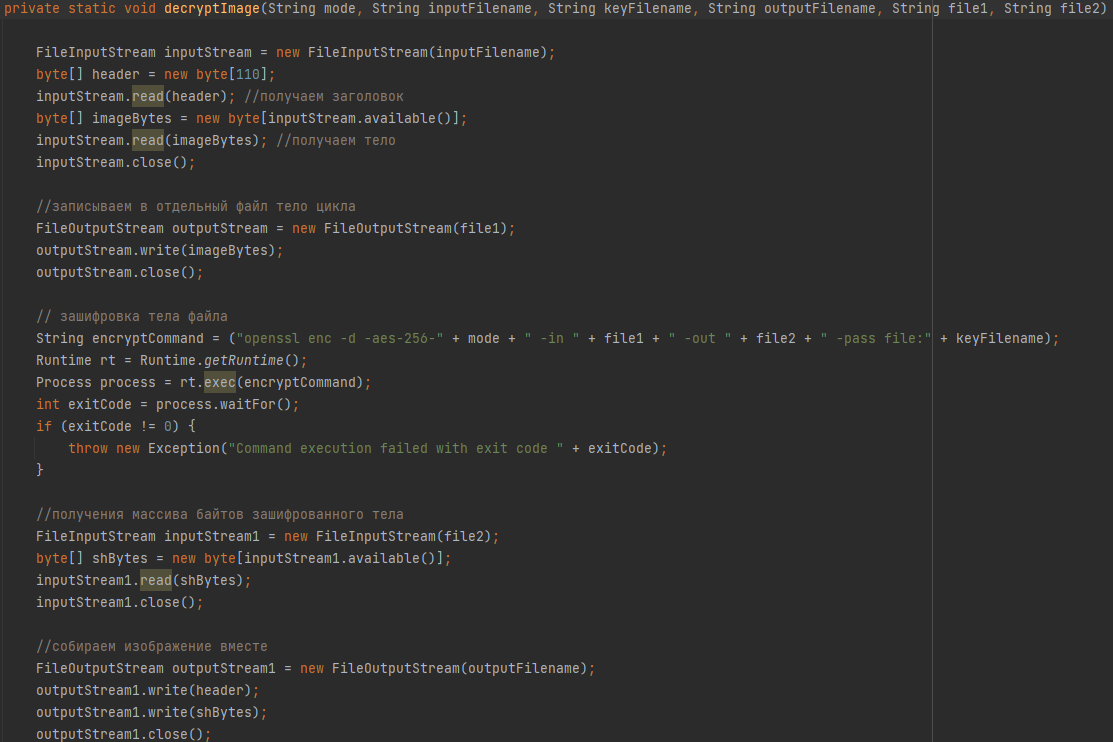


Рисунок 4 – decryptImage.

1. В результате мы получаем 4 зашифрованных изображения (представлены ниже) и 4 расшифрованных изображений и дополнительно для сравнения изображений я вывожу их размер в байтах рисунок 5.

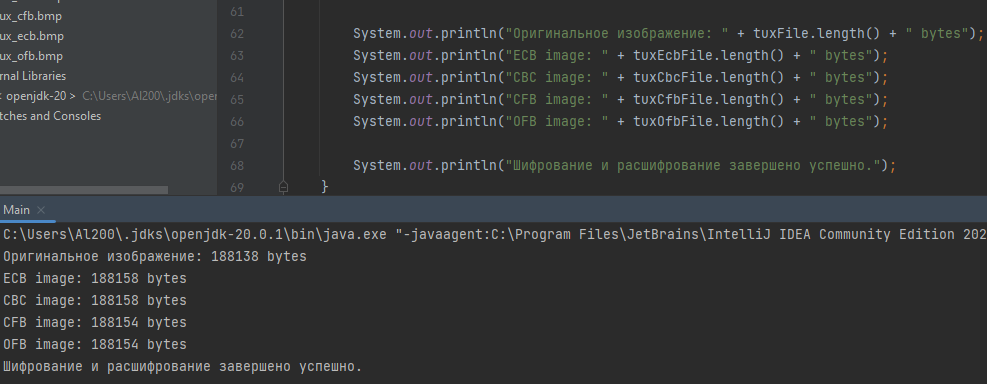
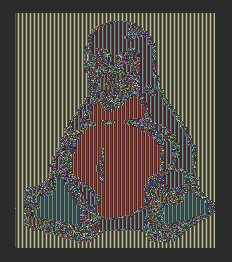
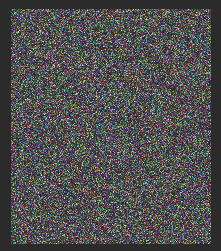


Рисунок 5 – Размер полученных файлов

Зашифрованное изображение в режиме ECB



Зашифрованное изображение в режиме CBC



Зашифрованное изображение в режиме CFB



Зашифрованное изображение в режиме OFB

