**Министерство науки и высшего образования РФ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»**

**(ВлГУ)**

**Кафедра ИЗИ**

отчет

**по лабораторной работе №2**

**по дисциплине «МСКЗИ»**

Тема: «**Шифрование файлов. Четыре криптопримитива.»**

|  |  |  |  |
| --- | --- | --- | --- |
| Студент гр. ИСБ-121 |  |  | Розанов Л.А. |
| Преподаватель |  |  | Александров А.В. |

Владимир

2023

Цель работы: реализовать четыре основных криптографических примитива.

Постановка задачи: написать программу, осуществляющую шифрование и дешифрование

произвольных файлов при помощи четырех примитивных криптоалгоритмов. Допускается как

реализация всех криптоалгоритмов в разных программах, так и в одной программе,

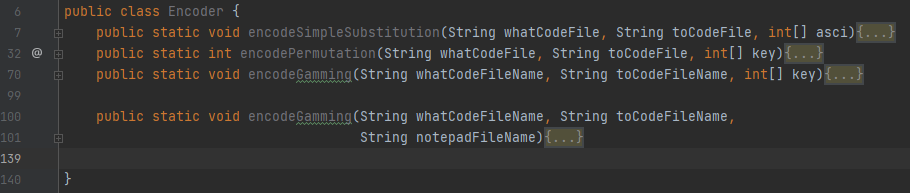
запускаемой в разных режимах. Программа должна генерировать ключ, сохранять его в

ключевом файле, считывать ключ из ключевого файла, шифровать данный файл по ключу и

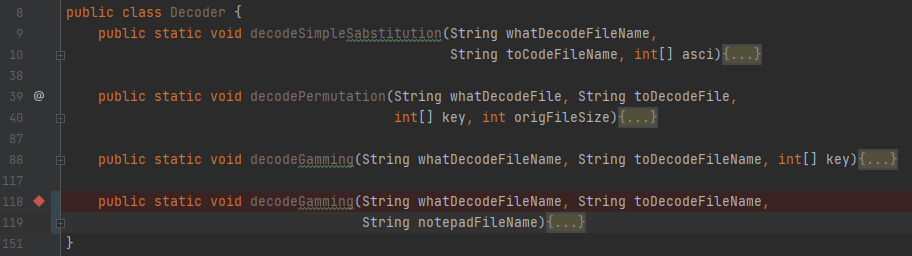
расшифровывать закрытый файл.

Все примитивы реализованы с помощью методов двух классов:

Encoder, который кодирует

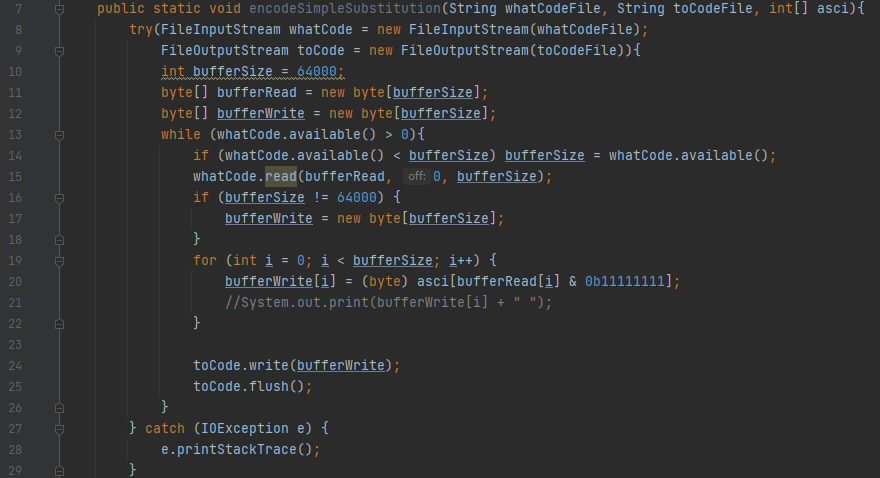


Decoder, который декодирует

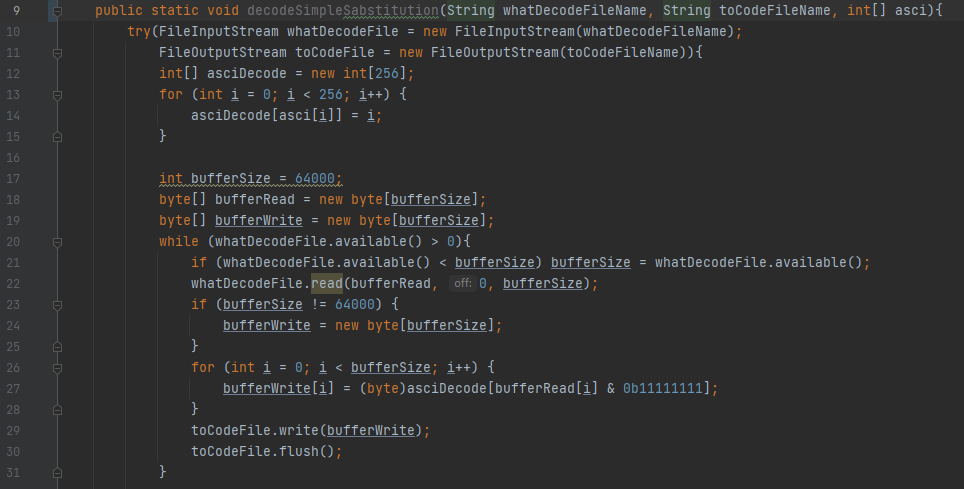


1. Простая подстановка.

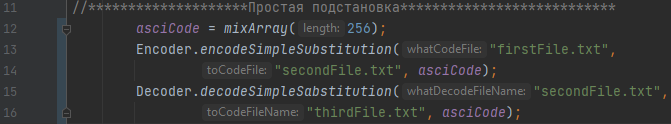
Метод, который кодирует, принимает на вход название файла, который нужно закодировать, и название файла, в который будет заноситься закодированная информация, также необходим перемешанный массив ASCI кодов.



Метод, который декодирует, принимает на вход название файла, который нужно декодировать, и название файла в который будет заноситься декодированная информация, также необходим перемешанный массив ASCI кодов.

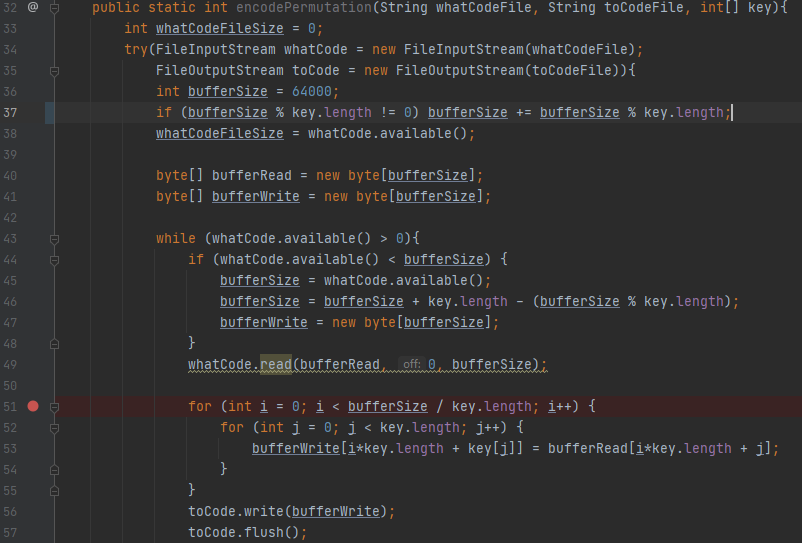


Пример вызова этих методов



1. Перестановка (транспозиция).

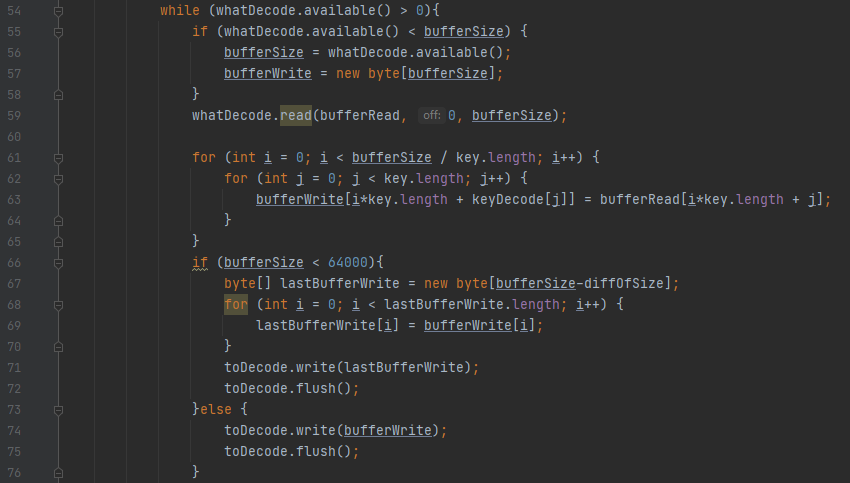
Метод, который кодирует, принимает на вход название файла, который нужно закодировать, и название файла, в который будет заноситься закодированная информация, также необходим перемешанный массив чисел от 1 до N(ключ).



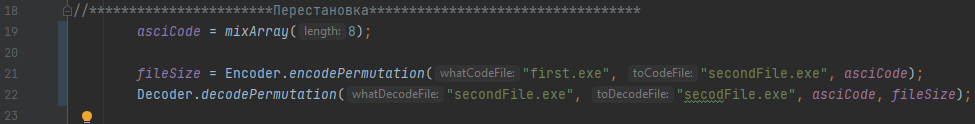
Метод, который декодирует, принимает на вход название файла, который нужно декодировать, и название файла, в который будет заноситься декодированная информация, также необходим перемешанный массив чисел от 1 до N(ключ) и размер оригинального файла.



Функциональная часть метода:



Пример вызова этих методов



1. Гаммирование (шифр Виженера).

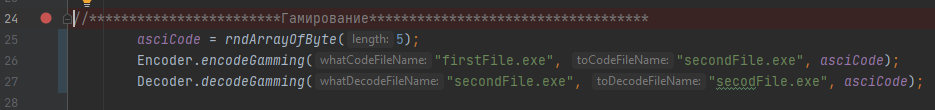
Метод, который кодирует, принимает на вход название файла, который нужно закодировать, и название файла, в который будет заноситься закодированная информация, также необходим массив чисел где каждое число случайным образом варьируется в диапазоне [0;255], длина произвольная.



Метод, который декодирует, принимает на вход название файла, который нужно декодировать, и название файла, в который будет заноситься декодированная информация, также необходим массив чисел где каждое число случайным образом варьируется в диапазоне [0;255], длина произвольная.

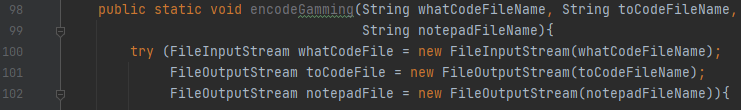


Пример вызова этих методов

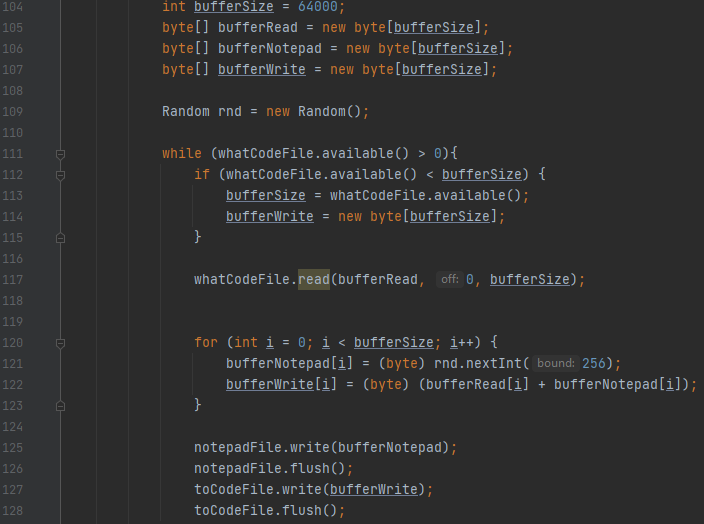


1. Одноразовый блокнот (шифр Вернама)

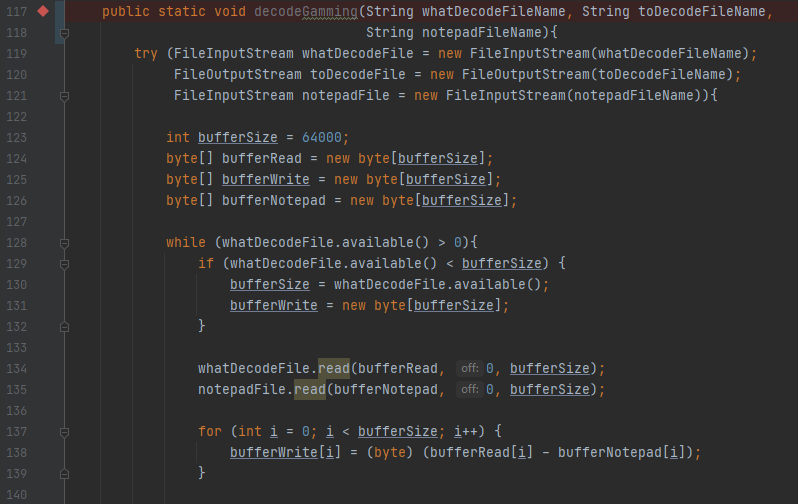
Метод, который кодирует, принимает на вход название файла, который нужно закодировать, и название файла, в который будет заноситься закодированная информация, также необходимо название файла-блокнота.



Функциональный код метода



Метод, который декодирует, принимает на вход название файла, который нужно декодировать, и название файла, в который будет заноситься декодированная информация, также необходимо название файла-блокнота.



Пример использования этих методов

