БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №7**

**«**Исследование блочных шифров»

Выполнила:

студентка 3 курса 5 группы

Почиковская Юлия Сергеевна

Вариант 10

Проверил:

Берников В. О.

Минск 2022

1. **Разработать приложение реализующие метод шифрования указанный в варианте (DES-EEE2)**

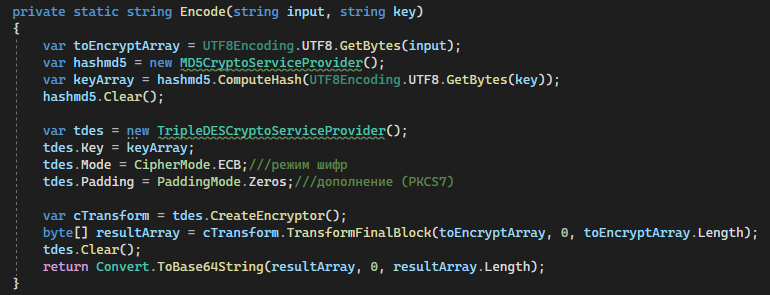
Для зашифрования исходного текста были использованы встроенные экземпляры классов из пространства имен System.Security.Cryptography. Реализация функции зашифрования представлена на рисунке 1.1

Рисунок 1.1 – Реализация функции Encode

Исходная строка разбивается на блоки фиксированной длины с дополнением последнего блока. Поскольку мы указали режим шифрования ECB, входной поток будет разбит на блкои длиной 8 байт (64 бит) по умолчанию. Режим дополнения Zeros указывает, что последний блок будет дополняться нулями. Также выполняется преобразование ключевой информации – переданный в параметрах ключ хешируется с помощью алгоритма MD5.

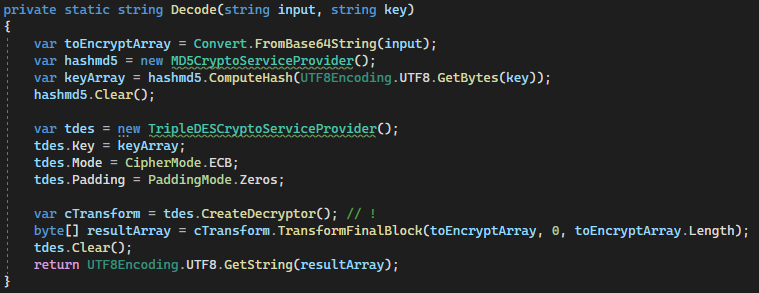
Приложение осуществляет расшифрование используя функцию Decode, реализация функции представлена на рисунке 1.2

Рисунок 1.2 – Реализация функции Decode

В данной функции выполняются те же действия, что и при зашифровании только в обратном порядке.

Данное программное средство должно реализовать алгоритм 3DES-EEE2: операции шифрование-расшифрование-шифрование, на первом и третьем шаге используется одинаковый ключ. Реализация данного алгоритма представлена на рисунке 1.3.

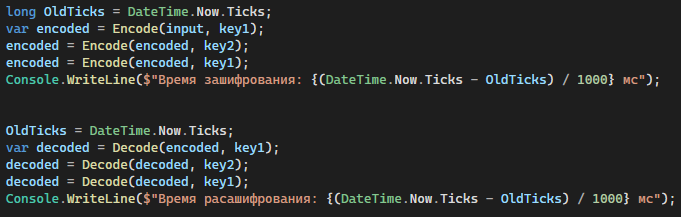


Рисунок 1.3 – Реализация алгоритма DES3-EEE2

Для зашифрования и расшифования используются ключи key1, key2, считанные из файловой системы.

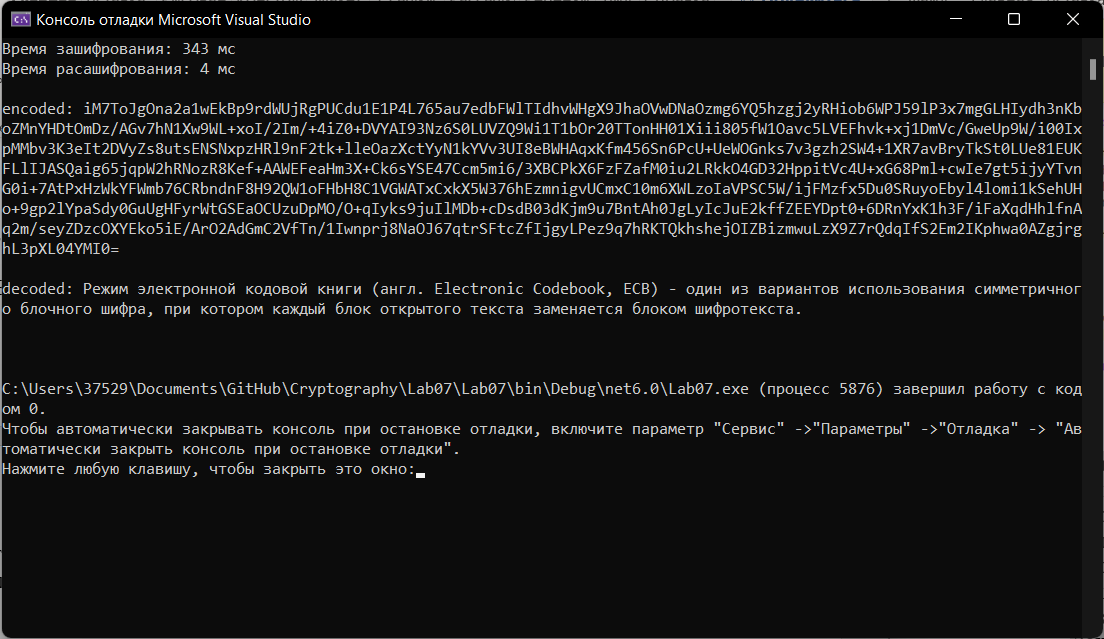
Результат выполнения данного приложения представлен на рисунке 1.4

Рисунок 1.4 – Результат работы приложения