МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Отчет к лабораторной работе №7**

**Исследование блочных шифров»**

Студент:

Септилко Анастасия Антоновна

Преподаватель:

Блинова Евгения Александровна

Минск 2020

**ЗАДАНИЯ:**

1. Разработать авторское приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться готовыми библиотеками либо программными кодами, реализующими некоторые блочные алгоритмы, из приложения в [4].

Приложение должно реализовывать следующие операции:

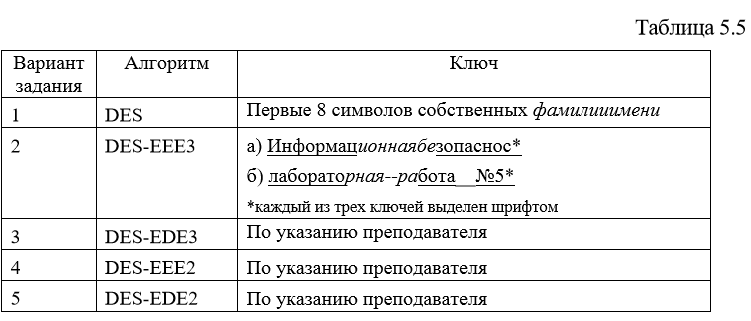
• разделение входного потока данных на блоки требуемой длины с необходимым дополнением последнего блока;

• выполнение требуемых преобразований ключевой информации;

• выполнение операций зашифрования/расшифрования;

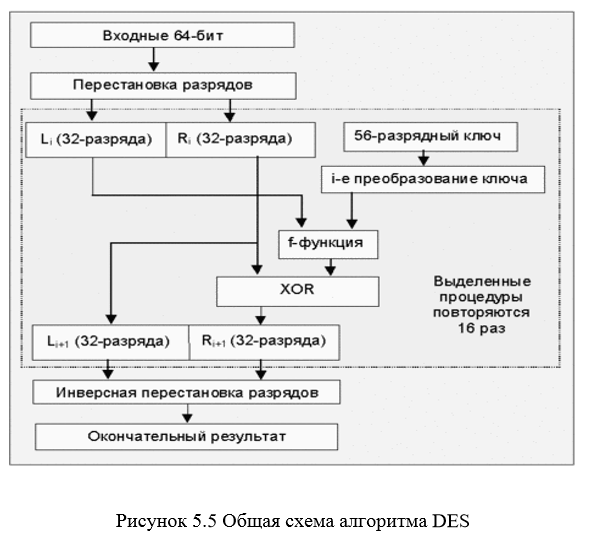
• оценка скорости выполнения операций зашифрования/расшифрования;

• пошаговый анализ лавинного эффекта с подсчетом количества изменяющихся символов по отношению к исходному слову. Исследуемый метод шифрования и ключевая информация – в соответствии с вариантом из нижеследующей табл. 5.5.



Алгоритм строится на основе сети Фейстеля.

Входной блок данных, состоящий из 64 бит, преобразуется в выходной блок идентичной длины. В алгоритме широко используются рассеивания (подстановки) и перестановки битов текста, о которых мы упоминали выше. Комбинация двух указанных методов преобразования образует фундаментальный строительный блок DES, называемый раундом или циклом. Один блок данных подвергается преобразованию (и при зашифровании, и при расшифровании) в течение 16 раундов.

После первоначальной перестановки и разделения 64-битного блока данных на правую (R0) и левую (L0) половины длиной по 32 бита выполняются 16 раундов одинаковых действий (см. рис. 5.5.). 

Функции, которые продемонстрированы на рисунке 1.1 отвечают за шифровании и расшифрованные. Они содержат в себе ключ в двоичной системе счисление и переменную “iv” в шестнадцатеричной системе счисления.

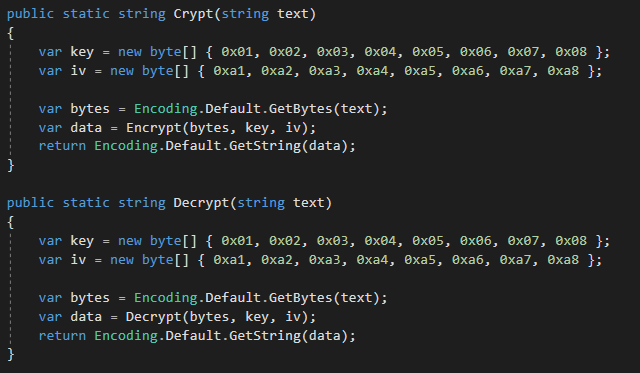


Рисунок 1.1 – Функция Crypt()

Эта функция передается в функцию Crypt для шифрования введенного текста. Ее пример показан на рисунке 1.2.

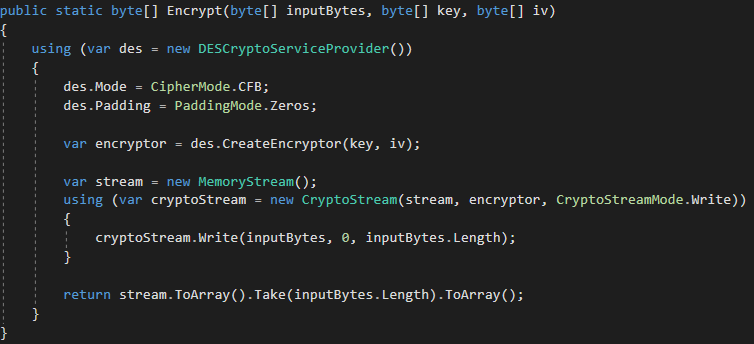


Рисунок 1.2 – Функция Encrypt()

Эта функция использует стандартный метод DESCryptoServiceProvider. Определяет объект-оболочку для доступа к версии алгоритма Data Encryption Standard ( [DES](https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.des?view=netcore-3.1) ), предоставленной поставщиком криптографических услуг (CSP) . Этот класс не может быть унаследован. И так же используем метод CreateEncryptor.

Функция на рисунке 1.3 передается в функцию Decrypt для расшифрования введенного текста.

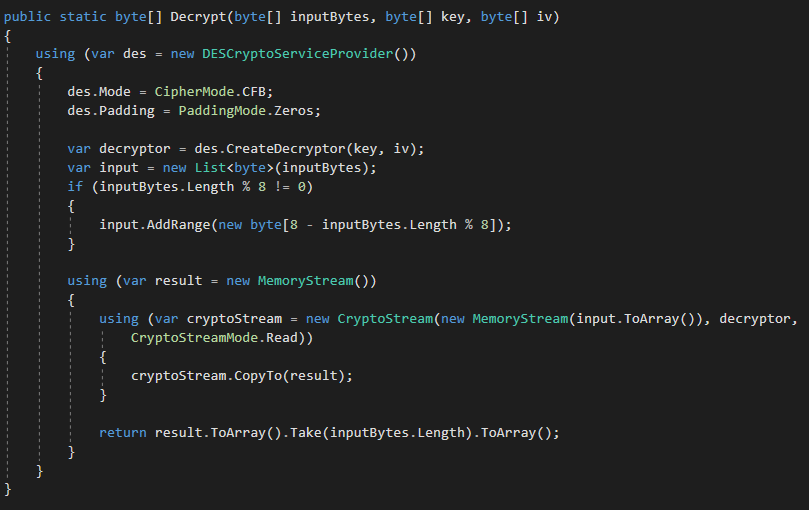


Рисунок 1.3 – Функция Decrypt()

Итог выполнения программы (рисунок 1.4).

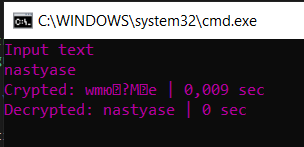


Рисунок 1.4 – Итог выполнения программы