Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №7**

**Тема «****Исследование блочных шифров»**

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации блочных шифров.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости блочных шифров.
2. Разработать приложение для реализации указанных преподавателем методов блочного зашифрования/расшифрования.
3. Выполнить анализ криптостойкости блочных шифров
4. Оценить скорость зашифрования/расшифрования реализованных шифров.
5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Блочный шифр**

**Блочный шифр** – это криптографическая система, которая делит открытый текст на отдельные блоки, как правило, одинакового размера и независимо оперирует с каждым из них с целью получения последовательности блоков шифрованного текста.

**Алгоритм DES**

**DES (Data Encryption Standard) –** алгоритм, который берет строку битов открытого текста фиксированной длины и преобразует ее с помощью серии сложных операций в другую строку битов зашифрованного текста той же длины.

Алгоритм строится на основе сети Фейстеля, при шифровании используется ключ размером в 56 бита (7 байт, 7 символов), если ключ не соответствует размеру, то он дополняется. Исходное сообщение делится на блоки по 64 бита и дополняется пустыми символами, если размера блока не хватает. Блок делится на левый *L* и правый *R* подблоки*. R* подблок изменяется функцией с использование раундового ключа. Результат складывается по модулю 2(*XOR*) с подблоком *L*. *R* подблок текущего раунда будет использован в следующем раунде как *L* подблок. В нашем случае данный алгоритм повторяется 16 раз для каждого блока. Ключ вычисляется по какому-либо мат. правилу и в каждом раунде разный.

**Лавинный эффект** – это эффект, когда изменение одного бита входного сообщения приводит к значительным изменениям в зашифрованном сообщении.

Общая схема алгоритма предоставлена на рисунке 1.1.



Рисунок 1.1 – Общая схема алгоритма DES

Код программы для шифрования и дешифрования предоставлены на рисунках 1.2 и 1.3, а результат работы программы на рисунке 1.4

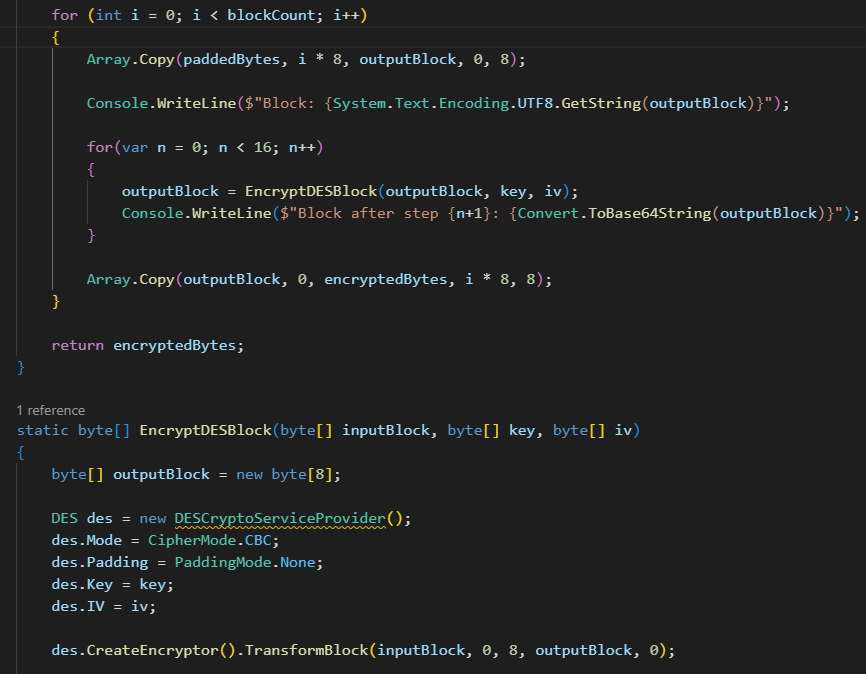


Рисунок 1.2 – Код программы для шифрования

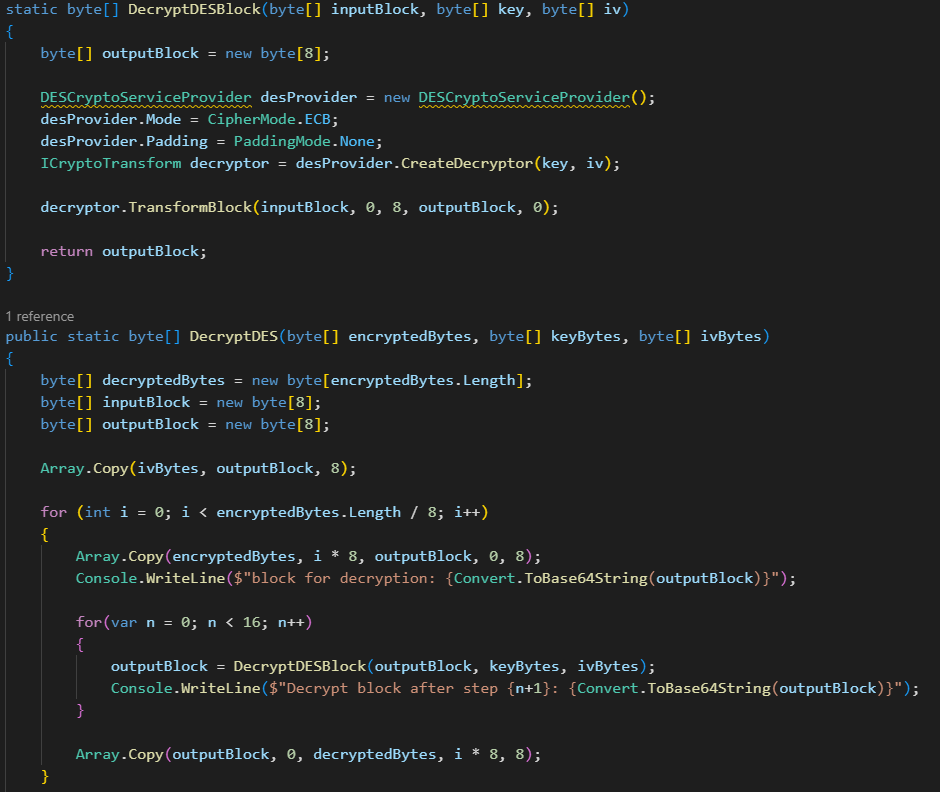


Рисунок 1.3 – Код программы для дешифрования



Рисунок 1.4 – Результат выполнения программы

Пример лавинного эффекта изображён на рисунке 1.5

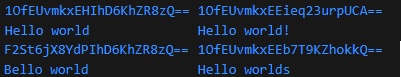


Рисунок 1.5 – Пример лавинного эффекта

На рисунке 1.5 мы видим, что при незначительном изменении исходного сообщения, зашифрованное сообщение значительного изменяется.

Так же существуют слабые и полуслабые ключи. Слабые ключи называются ключи, при которых *DES*(*DES*(*x*)) = *x.* Где *x* – 64-битный блок.

Полуслабыми ключами называется пара ключей (*k*1, *k*2), при которых *DESk*1(*DESk*2(*x*)) = *x*. Где *x* – 64-битный блок

Известные пары ключей слабых и полуслабых ключей предоставленына рисунках 1.7 и 1.8 соответственно.

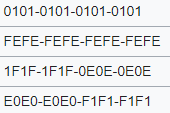


Рисунок 1.7 – известные примеры слабых ключей

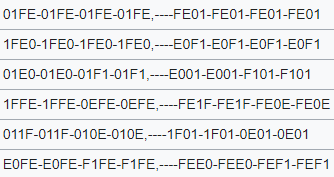


Рисунок 1.8 – известные примеры полуслабых ключей

Скорость шифрования и дешифрования предоставлена на рисунке 1.8

Рисунок 1.8 – Скорость шифрования и дешифрования

**Сжатие**

При сжатии файла, содержащий исходный текст, из 6772 байт на выходе получаем 3253 байт. При сжатии файла, содержащий зашифрованный текст, из 9036 байт на выходе получаем 6859 байт.

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки практические навыки разработки приложения для реализации блочных шифров.