Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 7**

«ИССЛЕДОВАНИЕ БЛОЧНЫХ ШИФРОВ»

Выполнил:

Студент: Белицкий В.Д.

ФИТ 2 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

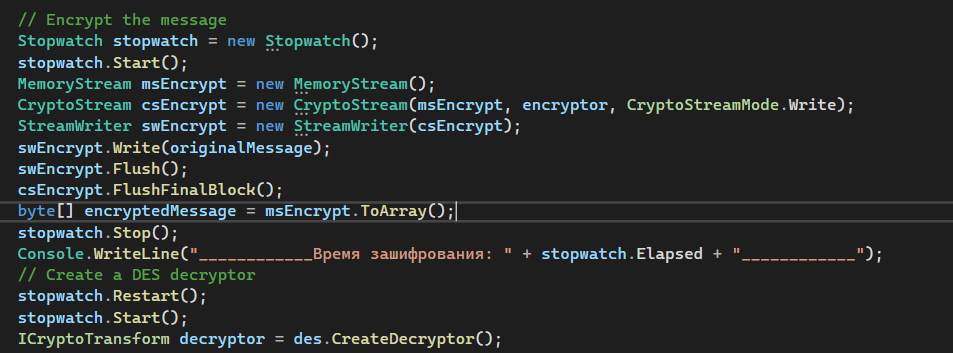
**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации блочных шифров

**Описание приложения**

Приложение написано на языке программирования *C#* и позволяет:

* Зашифровать и расшифровать сообщение использую алгоритм DES.
* Оценить время зашифрования и расшифрования

1. **Методика выполнения расчетов**

Рисунок 1.1 – код зашифрования

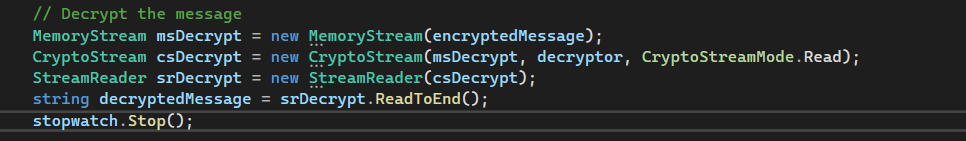


Рисунок 1.2 – код расшифрования

1. **Результаты работы приложения**

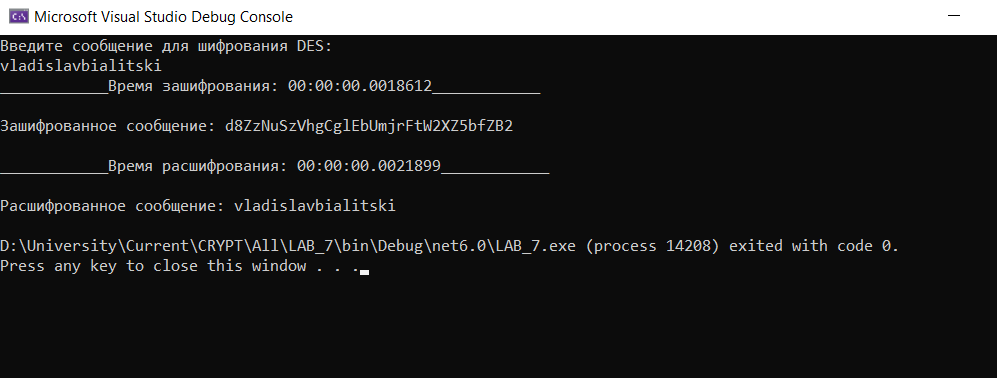


Рисунок 2.1 – результат работы приложения

1. **Проанализировать влияние слабых ключей и полуслабых ключей на конечный результат зашифрования и на лавинный эффект**

Воспользовавшись слабым ключом для шифрования и дешифрования видно, что дешифрование выполняется намного быстрее, если бы мы использовали полуслабый или сильный ключ. Результат работы приложения c слабым ключом представлен на рисунка 3.4.

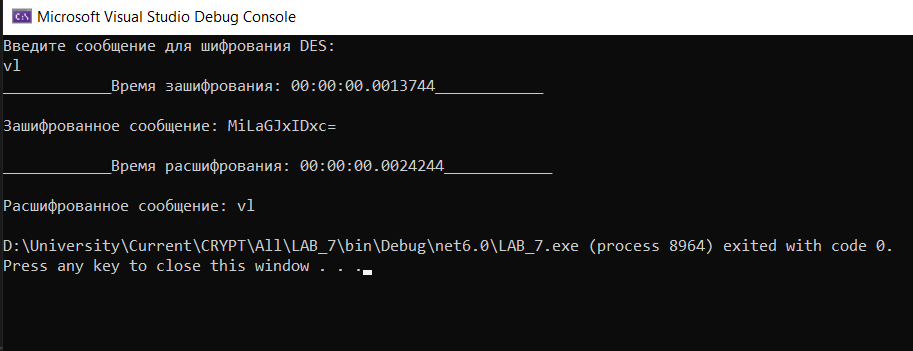


Рисунок 3.4 – Результат работы приложения со слабым ключом

Так же при работе со слабым ключом возможно расшифрование закодированного текста с помощью вообще другого слабого ключа или же вообще исходный текст и зашифрованы могут быть полностью идентичные.

Результат работы приложения c полуслабым ключом представлен на рисунка 3.5.

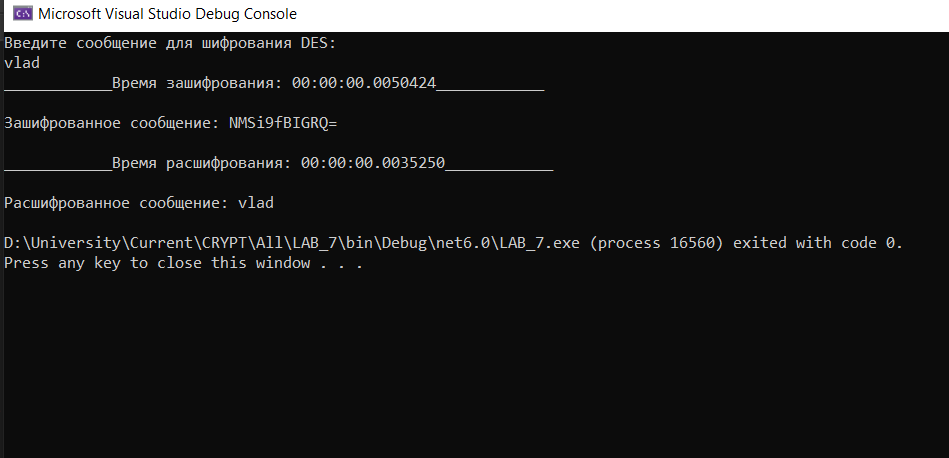


Рисунок 3.5 – Результат работы приложения со полуслабым ключом

Лавинный эффект - это явление, связанное с алгоритмами шифрования и хэширования, при котором небольшие изменения входных данных или ключа приводят к значительным изменениям в выходных данных или хэш-значении. Термин «лавина» описывает аналогию с процессом снежного обвала, где небольшое движение снежных масс приводит к крупной и мощной лавине.

Демонстрация лавинного эффекта представлена на рисунке 3.6

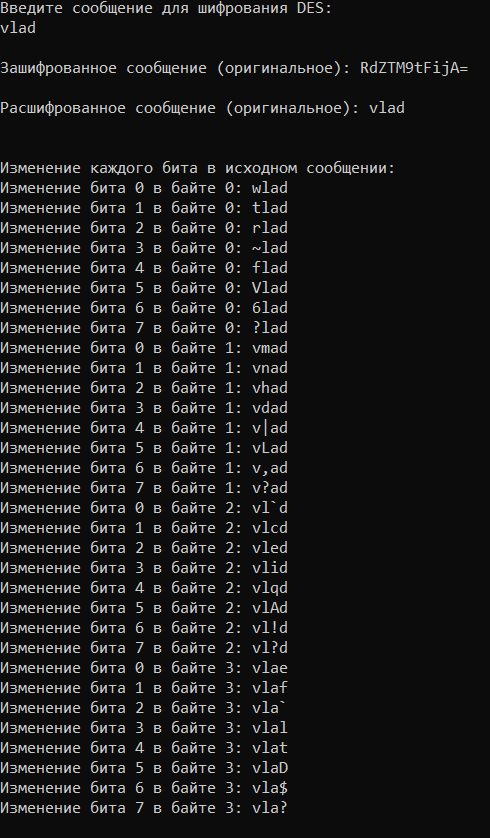


Рисунок 3.5 – Демонстрация лавинного эффекта

В контексте шифрования или хэширования лавинный эффект является желательным свойством, которое гарантирует, что незначительные изменения в исходных данных или ключе приводят к существенным изменениям в выходных данных или хэш-значении. Это важно для обеспечения безопасности и стойкости алгоритмов.

1. **Оценить степень сжатия открытого текста и соответствующего зашифрованного текста**

Если попытаться сжать с помощью программы архивации 7-Zip два файла: с исходным текстом и с зашифрованным - то мы заметим одну закономерность: файл с зашифрованным текстом не сжимается или же практически не сжимается. Результаты сжатия представлены на иллюстрациях 3.6, 3.7. Если рассматривать сжатие в процентном соотношении, то input.txt сжимается на 98%, output1.txt же на 0%.

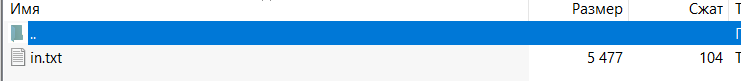
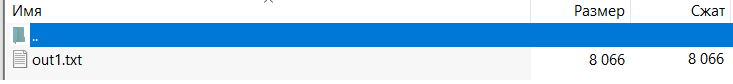
****

Рисунок 3.6 – Результат архивации исходного текста

****Рисунок 3.7 – Результат архивации зашифрованного текста

**Вывод**: в ходе лабораторной работы разработано приложение для реализации алгоритма шифрования «DES». Произведён лавинный эффект, а также произведено исследование влияния слабых и полуслабых ключей.