Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование блочных шифров**

Студент: Лагуновский М.Б.

ФИТ 3 курс 6 группа

Преподаватель: Сазонова Д.В.

Минск 2020

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* зашифровать текст с помощью блочного алгоритма шифрования DES;
* расшифровать текст с помощью блочного алгоритма DES.

1. **Методика выполнения поставленных задач**

Для выполнения зашифрования сообщения с помощью блочного алгоритма шифрования необходимо ввести ключ для зашифровки и нажать на кнопку «Зашифровать». И кнопку «Расшифровать» для того, чтобы расшифровать зашифрованный текст. При этом исходный текст размешается в текстовом файле. Также в текстовых файлах размещаются зашифрованный и расшифрованный текст.

Вид главного окна приложения представлен на рисунке 2.1.

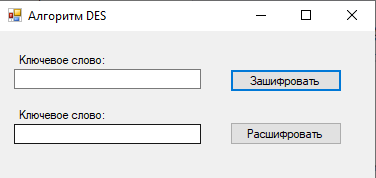


Рисунок 2.1 – Главное окно приложения

В примере, представленном на рисунке 2.2, вводим некоторый ключ, а также посмотрим содержимое входного файла «in.txt».

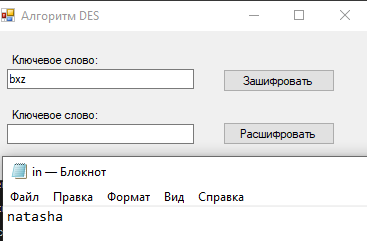


Рисунок 2.2 – Ключ для зашифрования

. Результат зашифрования сообщения представлен на рисунке 2.3.

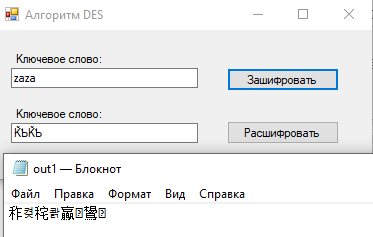


Рисунок 2.3 – Результат зашифрования сообщения

Результат расшифрования представлен на рисунке 2.4.

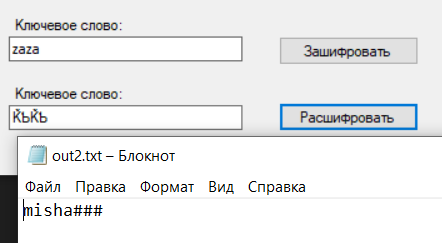


Рисунок 2.4 – Результат расшифрования сообщения

На рисунке 2.5 представлена функция для зашифрования сообщения на основании ключа и входного файла.

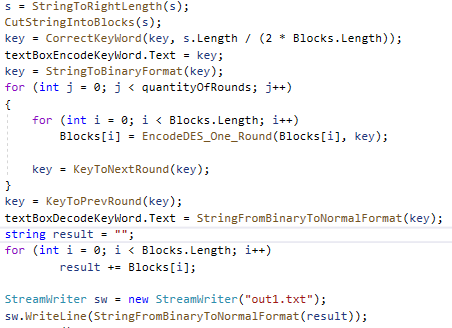


Рисунок 2.5 – Функция для зашифрования

Таким образом, были реализованы все поставленные задачи. Были исследованы блочные шифры, такие как DES. Криптостойкость такого алгоритма слабая и должна зависеть только от ключа.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования блочного шифра DES. Были изучены основные принципы работы блочных шифров и оценена криптостойкость.

Также было разработано приложение, на языке программирования C#, для реализации задач, связанных с шифрованием данных.