Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №7**

Студент: Бобрович Г.С.

ФИТ 3 курс 7 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Разработать приложение для реализации указанных преподавателем методов блочного зашифрования/расшифрования.**

****

Рисунок 1.1 — Условие

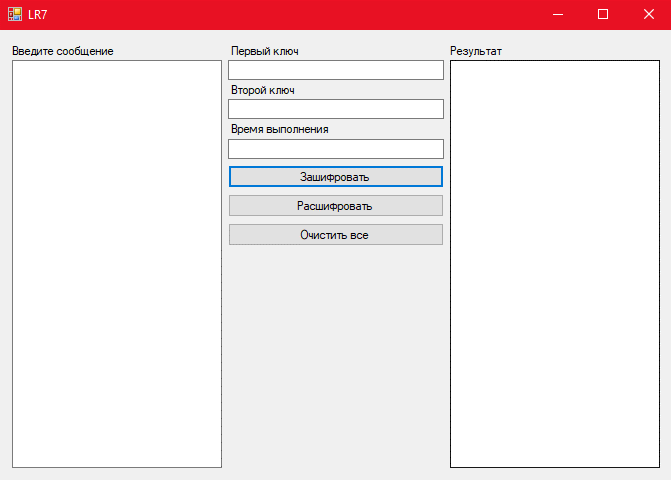
****

Рисунок 1.2 — Приложение

Для проверки работы приложения, введем какой-нибудь текст.

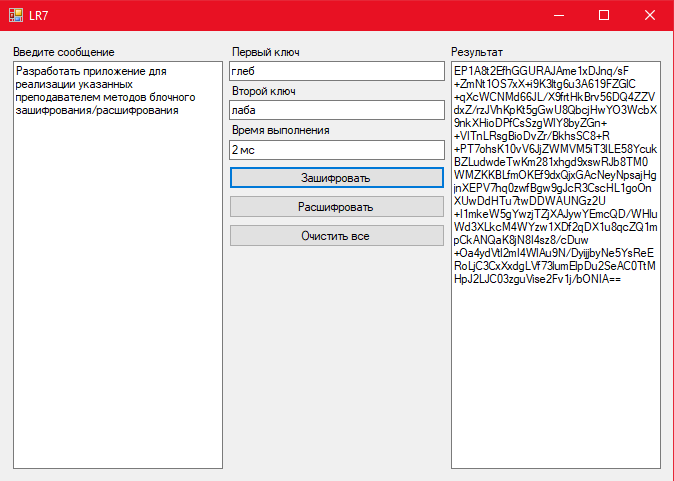


Рисунок 1.3 — Результат зашифрования

Теперь расшифруем полученный текст:

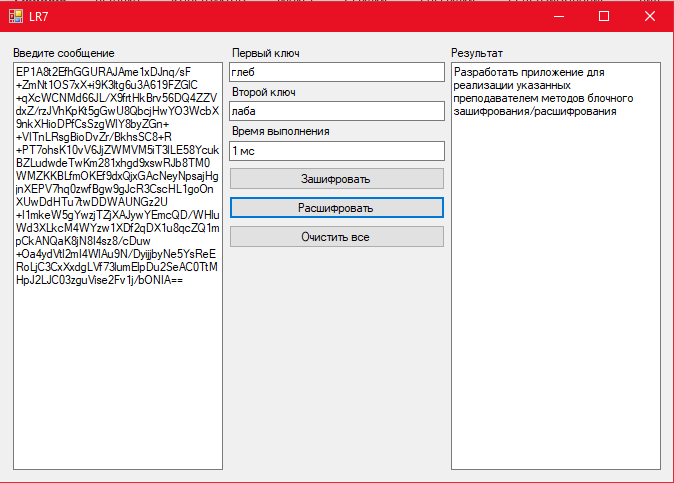


Рисунок 1.4 — Результат расшифрования

Зашифровка происходит с помощью классов, взятых из System.Security.Cryptography. Само зашифрование работает следующим образом: исходная строка (сообщение) разбивается на блоки с фиксированной длиной и дополнительным последним блоком. DES-EEE2 представляет собой операции шифрования, расшифрования, шифрования. Его отличие от других в том, что на первом и третьих шагах используется один и тот же ключ. То есть, сначала исходное сообщение зашифруется с помощью первого ключа, затем результат зашифруется с помощью второго ключа и в конце концов результат второй операции зашифруется первым ключом. Расшифровка выполняется в обратном порядке: зашифрованный текст расшифруется с помощью первого ключа, затем результат расшифруется с помощью второго и этот результат расшифруется первым ключом. В итоге, мы получим исходное сообщение

Из полученных результатов видно, что зашифровка исходного сообщения заняла 2 мс. При расшифровке зашифрованного сообщения время выполнения ­­­– 1 мс. Расшифровка происходит быстрее, так как используются данные кэша, полученные при зашифровке сообщения

Также была оценена степень сжатия файлов исходного и зашифрованного сообщений. Для исходного – 228 байт, для зашифрованного – 1014 байт. Большая разница в размере вызывается из-за лавинного эффекта, возникающего при каждом зашифровании, когда растет зависимость всех битов результата от битов исходных данных и ключа вместе с этим растет и количество символов в зашифрованном сообщении по отношении к количеству символов в исходном сообщении.

**Вывод**

В ходе выполнения лабораторной работы были изучены и приобретены практические навыки разработки и использования приложения для реализации блочных шифров.