Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование блочных шифров.**

Студент: Плотников Д.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

1. **Постановка задачи**

В ходе лабораторной работы необходимо было закрепить теоретические знание по алгебраическому описанию, алгоритмам реализации операций зашифрования\расшифрования, выполнить анализ криптостойкости блочных шифров.

По условию лабораторной работы необходимо было разработать приложение, позволяющее зашифровывать и расшифровывать исходное сообщение с помощью алгоритма DES. Общий алгоритм DES изображен на рисунке 1.

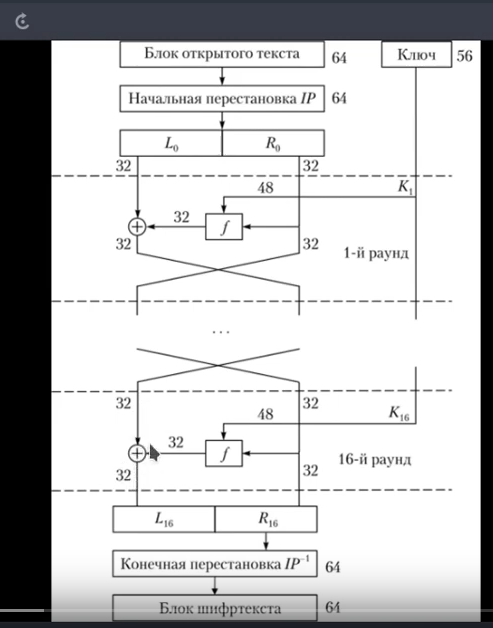


Рисунок 1 – Общий алгоритм DES.

Стоит рассмотреть повнимательнее, что из себя представляет функция f. Ее содержимое предоставлено на рисунке 2.

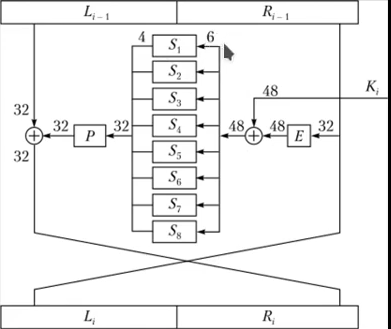


Рисунок 2 – Функция f.

Как видно, правый блок попадает в функцию расширения E, который по определенной таблице дублирует некоторые исходные биты и затем ему применяется операция XOR, с ключом. Как правило ключ изначально имеет длину 64 бит, но на вход удаляется каждый восьмой, либо по какому-нибудь другому принципу. Затем в зависимости от раунда ключ сдвигается и таким образом для зашифрования используется только его 48 бит. Более подробно просмотреть то, что происходит с ключом можно на рисунке 3.

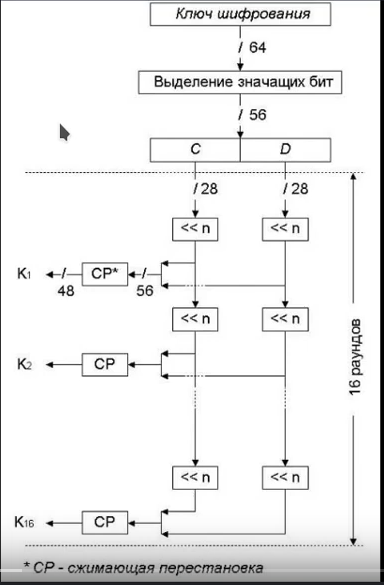


Рисунок 3 – Преобразование ключа.

# 2. Описание приложения

Приложение, представляет собой программу, шифрующую и расшифрующую выбранный текст алгоритмом DES. Программа написана на языке программирования C#, для работы с алгоритмами шифрования использовалась стандартная библиотека. Как видно на рисунке 4, текст, передаваемы для шифрования устанавливается в переменную str. Далее он будет зашифрован и расшифрован а обе версии будут отображены на экране.

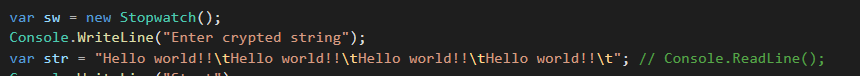


Рисунок 4 – Исходный текст для шифрования.

Для шифрования и обратного процесса было написано две соответствующие функции. Функция для шифрования предоставлена на рисунке 5, функция для дешифрования предоставлена на рисунке 6. Таким образом в приложении есть весь необходимый функционал для работы с шифром DES.

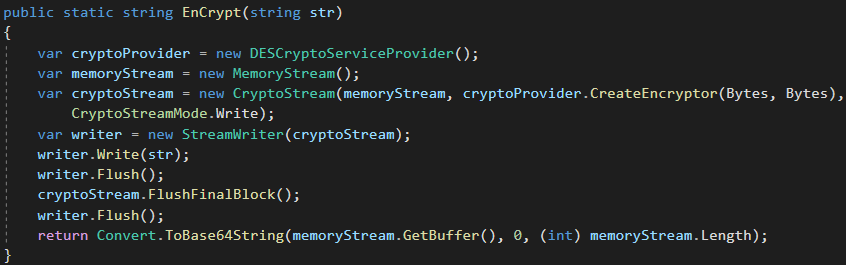


Рисунок 5 – Функция, используемая для шифрования.

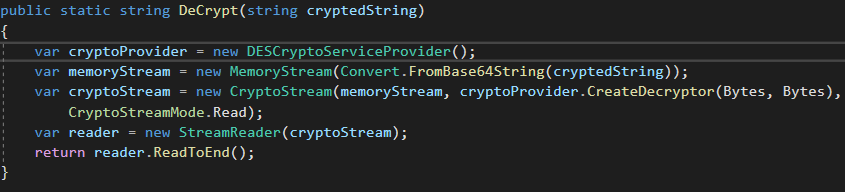


Рисунок 6 – Функция, используемая для дешифрования.

В результате работы с приложением достаточно использовать две эти функцию, чтобы полностью насытиться функционалом.

На этапе пользования приложением было выявлено, что алгоритм является достаточно медленным, что недопустимо для часто шифруемых данных. Например, приведенная выше строка шифровалась около 3мс, но с ростом длины строки линейно будет и расти время, необходимое для осуществления шифрования и соответственно дешифрования.

**Вывод**

В ходе этой работы были изучены и приобретены практические навыки разработки и использования блочных шифров. Разработано приложения на языке программирования С#, позволяющее выполнять шифрование и дешифрование текста с помощью блочного алгоритма DES. Изучены тонкости и детали его работы, а так же оценено время, необходимое для осуществления шифрования и дешифрования этим алгоритмом.