МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Исследование блочных шифров»**

Студент:

Храмых Владислав Олегович

Вариант 2

Преподаватель:

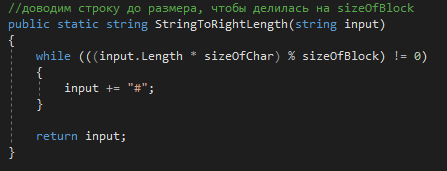
Блинова Евгения Александровна

Минск 2020

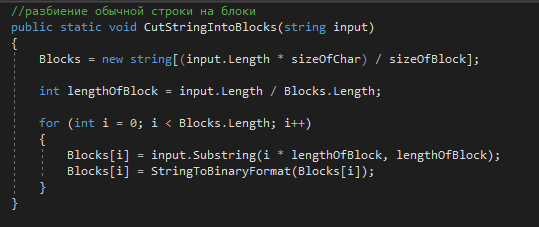
**ЗАДАНИЕ 1.** Алгоритм DES.

Итак, чтобы зашифровать сообщение алгоритмом DES, необходимо выполнить следующую последовательность шагов:

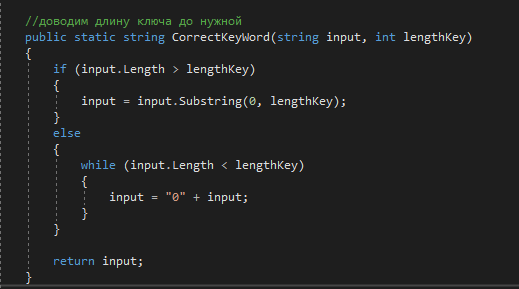
1. довести исходное сообщение до такого размера (в битах), чтобы оно нацело делилось на размер блока (sizeOfBlock = 128 бит);

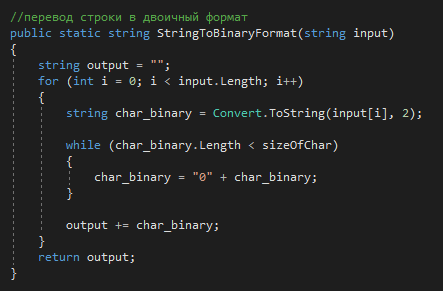


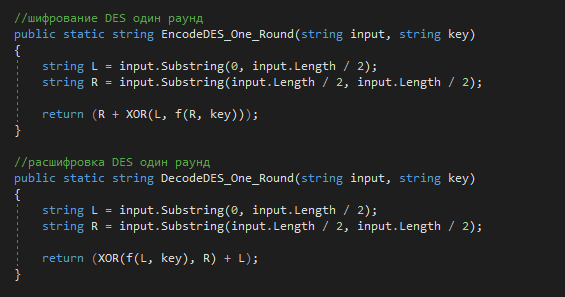
1. разделить исходное сообщение на блоки;

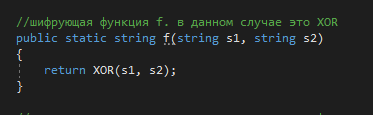


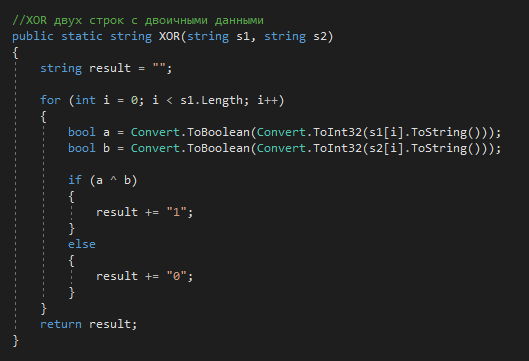
1. довести длину ключа до длины половины блока;

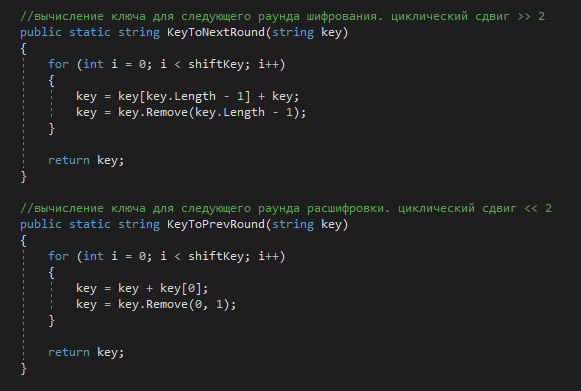


1. перевести ключ в бинарный формат (в нули и единицы); 
2. провести над каждым блоком прямое преобразование сетью Фейстеля в течении 16-ти раундов. После каждого раунда необходимо выполнять циклический сдвиг ключа на заданное количество символов





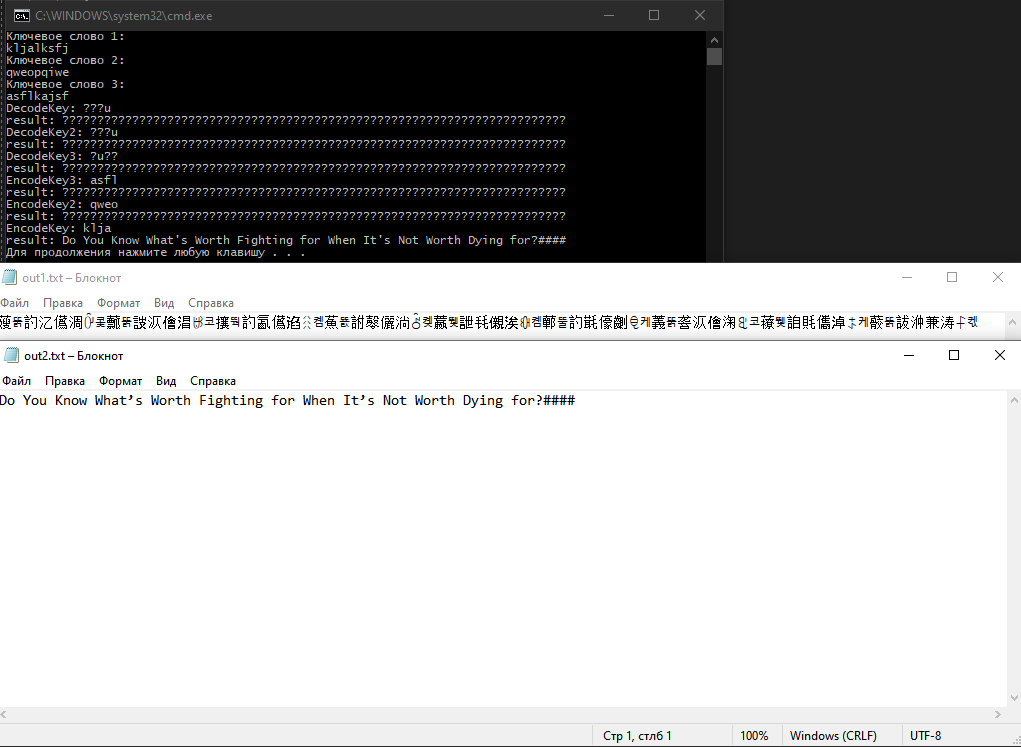


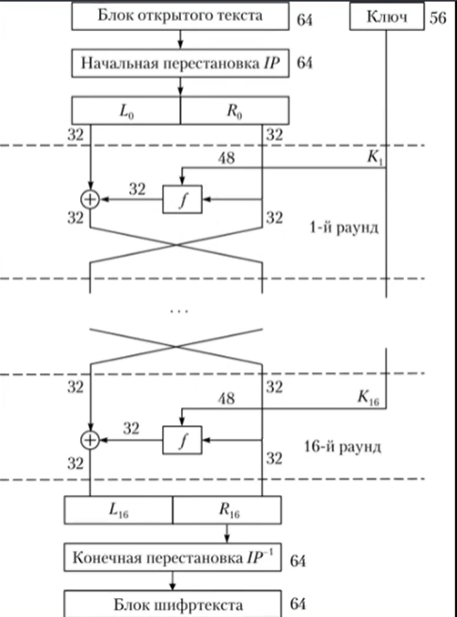


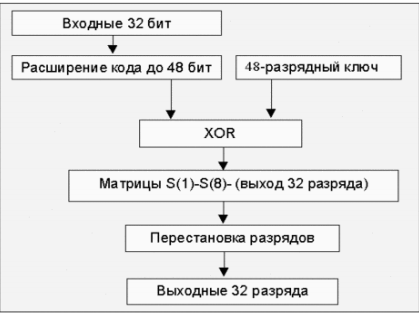
1. соединить все блоки вместе; таким образом получим сообщение, зашифрованное алгоритмом DES.

Расшифровка DES производится по аналогии. Используется обратное преобразование сетью Фейстеля.

Результат работы программы представлен ниже



Общая реализация на схемах ниже:



F - функция

