**Лабораторная работа 10 (генерация ключей для итераций)**

DES создает 16 раундовых ключей *ki* по 48 битов из ключа *k* шифра на 56 битов. Однако, чтобы задать ключ шифра надо среди 56битов ключа дополнительно вписать 8 битов в позиции 8, 16, ..., 64 дляпроверки четности таким образом, чтобы каждый байт содержалнечетное число единиц. С помощью этой операции выявляют ошибкипри обмене и хранении ключей.

Ключевое расписание состоит из этапов:

1). Перестановка сжатия для **удаления битов проверки –** из 64-битового ключа удаляют биты 8,16,24, 32, …,64 и переставляет остальные биты согласно таблице (в ходе перестановки сохраняется нумерация битов расширенного ключа).



2) После перестановки 56 битов ключа делятся на два блока *C*0 и *D*0 по 28 бит каждый. Далее для генерации раундовых ключей из блоков *C*0 и *D*0 с помощью операции циклического сдвига влево на 1-2 бита строятся блоки *Ci* и *Di*, *i* =1,2,...,16 . В раундах 1,2,9 и 16 смещение – на 1 бит, в других раундах — на 2 бита. После определения блоков *Ci* и *Di* биты этих блоков объединяются в один ключ на 56 битов.



**Задание**: Записать 16 чисел по 4 бита каждый (числа от 0 до 15). Перевести их в двоичный код. Удалить лишние биты и произвести итерацию ключа для каждого раунда.