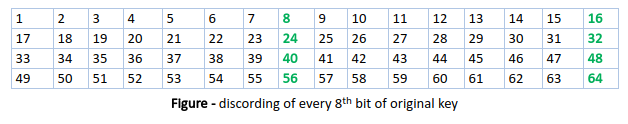
SINGLE ROUND ALGORITHM

**Key-generation:**

1. Key input size is 64-bit,
2. Now convert 64-bit to 56-bit. (every 8-bit of the key is discarded to produce a 56-bit.)



1. Now 56-bit key is divided into two 28-bit parts name as key1 and key2.
2. Apply shift key into both 28-bit key.
3. Apply permutation on key1 & key2 and generate 48-bit key.

**Operation on Input 64-bit:**

1. Find initial permutation of 64-bit key.
2. Now divide 64-bit into two part 32-bit left box and 32-bit right box.
3. Now apply operation on right-box.
   1. Apply expansion and permutation on right box output is 48-bit.
   2. Generated output of expansion box and 48-bit key is XOR.
   3. After XOR output is go to S-box; S-box convert 48-bit input into 32-bit.
   4. 32-bit of s-box output is again permuted.
4. Now generated right-box is XOR with Left-box.

<https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>

<https://www.educative.io/edpresso/what-is-the-des-algorithm>