**DES Summary**

**1) IP (Initial Permutation): inverse of the 64 bits.**

**2) Computation of key: 8 bits are used for parity check, the other 56 used to compute the key. These 56 bits are divided into two 28-bits long that are used when applying the shifts.**

**- Left shift, one position (i = 1, 2, 9, 16)**

**- two positions (the rest)**

**After that we get Ki of 48 bits. K16 ... K1 are used to encrypt data.**

**3) Expanding IP (using the right 28 bits).**

**4) Applying XOR function on the result with the key,**

**5) 6 bits are applied on each S-box to give a result of 4-bits of each S-box, and a total of 32 bits out of the 8 S-boxes**

**example :**

**110111**

**red bits are used to compute the row**

**blue bits are used to compute the column**

**3rd row, 11th column -- result = 14 = (1110)2**

**6) Merge the output of the X-boxes with each other**

**7) Permutation P4**

**8) Applying XOR function on the result of P4 with the left 28 bits**

**9) Swapping.**