Expand R(X) to 8 bits



Ki

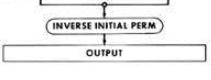
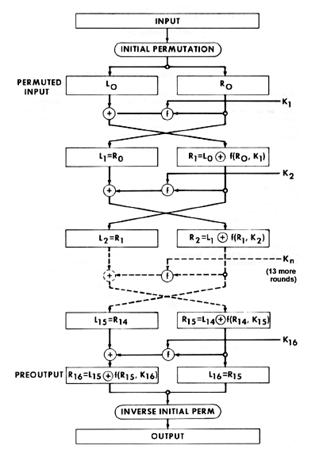
K: 10 bit key

K used to generate two 8-bit sub-keys K1,K2

S0(x1x2x3x4)||S1(x5x6x7x8)=y1y2y3y4

P4(y1y2y3y4)

F



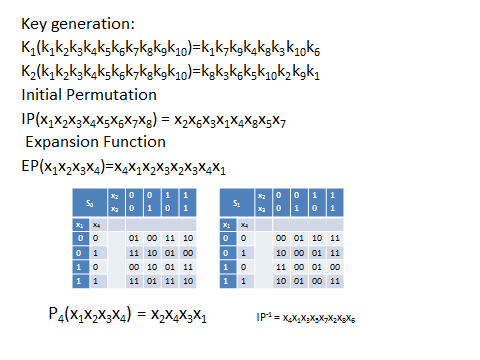
Encipher

Input: X (8 bits) , K (10 bits)

1. Expand K into K1,K2
2. Apply Initial permutation, then IP(x)=L(x) || R(x)
3. Find EP(R(x))  Ki= x1x2x3x4 x5x6x7x8
4. Apply S-boxes S0(x1x2x3x4) || S1(x5x6x7x8) = y1y2y3y4
5. Compute L’(x)= L(X)  P4(y1y2y3y4) (Note R’(X) = R(X))
6. Switch L’(X) and R’(X) to get new input R’(X)||L’(X)
7. Repeat 3-5 with new input for the 2nd round
8. Apply the inverse permutation to the output of round 2 to get the final answer.

Output: 8 bits

Note: To decipher use the same algorithm, but use K2 first, then K­1 (still do the IP at the beginning and IP-1 at the end)



IP-1 = x4x1x3x5x7x2x8x6