**Block Ciphers and DES**

**P8 = { 6, 3, 7, 4, 8, 5, 10, 9}**

**Simplified DES Example**

**P10 = { 3, 5, 2, 7, 4, 10, 1, 9, 8, 6}**

****

**Assume input 10-bit key, K, is: 1010000010**

Then the steps for generating the two 8-bit round keys, K1 and K2, are:

1. Rearrange K using P10: 1000001100
2. Left shift by 1 position both the left and right halves: 00001 11000
3. Rearrange the halves with P8 to produce K1: 10100100
4. Left shift by 2 positions the left and right halves: 00100 00011
5. Rearrange the halves with P8 to produce K2: 01000011

K1 and K2 are used as inputs in the encryption and decryption stages

.

**Assume a 8-bit plaintext, P: 01110010**

**IP -1= { 4,1 ,3 ,5 ,7 ,2 ,8 , 6}**

**P4 = { 2, 4, 3, 1}**

**IP = { 2, 6, 3, 1, 4, 8, 5 , 7 }**

**EP = { 4, 1, 2, 3, 2, 3, 4, 1}**

Then the steps for encryption are:

1. Apply the initial permutation, IP, on P: 10101001
2. Assume the input from step 1 is in two halves, L and R: L=1010, R=1001
3. Expand and permutate R using E/P: 11000011
4. XOR input from step 3 with K1: 10100100 XOR 11000011 = 01100111
5. Input left halve of step 4 into S-Box S0 and right halve into S-Box S1:
	1. For S0: 0110 as input: b1,b4 for row, b2,b3 for column
	2. Row 00, column 11 -> output is 10
	3. For S1: 0111 as input:
	4. Row 01, column 11 -> output is 11
6. Rearrange outputs from step 5 (1011) using P4: 0111
7. XOR output from step 6 with L from step 2: 0111 XOR 1010 = 1101
8. Now we have the output of step 7 as the left half and the original R as the right half. Switch the halves and move to round 2: 1001 1101
9. E/P with right half: E/P(1101) = 11101011
10. XOR output of step 9 with K2: 11101011 XOR 01000011 = 10101000
11. Input to s-boxes:
12. For S0, 1010
13. Row 10, column 01 -> output is 10
14. For S1, 1000
15. d. Row 10, column 00 -> output is 11
16. Rearrange output from step 11 (1011) using P4: 0111
17. XOR output of step 12 with left halve from step 8: 0111 XOR 1001 = 1110
18. Input output from step 13 and right halve from step 8 into inverse IP
19. a. Input us 1110 1101
20. b. Output is: 01110111

**So our encrypted result of plaintext 01110010 with key 1010000010 is: 01110111**