

Block Ciphers and DES

Examples

Steven Gordon

1 Simplified DES Example

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

Then the steps for generating the two 8-bit round keys, K_1 and K_2 , are:

1. Rearrange K using P_{10} : 1000001100
2. Left shift by 1 position both the left and right halves: 00001 11000
3. Rearrange the halves with P_8 to produce K_1 : 10100100
4. Left shift by 2 positions the left and right halves: 00100 00011
5. Rearrange the halves with P_8 to produce K_2 : 01000011

K_1 and K_2 are used as inputs in the encryption and decryption stages.

Assume a 8-bit plaintext, P : 01110010

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 permute R using E/P : 11000011
4. XOR input from step 3 with K_1 : $10100100 \text{ XOR } 11000011 = 01100111$
5. Input left half of step 4 into S-Box S_0 and right half into S-Box S_1 :
 - a. For S_0 : 0110 as input: b_1, b_4 for row, b_2, b_3 for column
 - b. Row 00, column 11 \rightarrow output is 10
 - c. For S_1 : 0111 as input:
 - d. Row 01, column 11 \rightarrow output is 11
6. Rearrange outputs from step 5 (1011) using P_4 : 0111
7. XOR output from step 6 with L from step 2: $0111 \text{ XOR } 1010 = 1101$
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 K_2 : $11101011 \text{ XOR } 01000011 = 10101000$
11. Input to s-boxes:
 - a. For S_0 , 1010
 - b. Row 10, column 01 \rightarrow output is 10

- c. For S1, 1000
 - d. Row 10, column 00 -> output is 11
12. Rearrange output from step 11 (1011) using P4: 0111
 13. XOR output of step 12 with left halve from step 8: 0111 XOR 1001 = 1110
 14. Input output from step 13 and right halve from step 8 into inverse IP
 - a. Input us 1110 1101
 - b. Output is: 01110111

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

Other examples (encrypt or decrypt) could be:

- Plaintext: 11010101; Key: 0111010001; Ciphertext: 01110011
- Plaintext: 01001100; Key: 1111111111; Ciphertext: 00100010
- Plaintext: 00000000; Key: 0000000000; Ciphertext: 11110000
- Plaintext: 11111111; Key: 1111111111; Ciphertext: 00001111