EECE 632 – Cryptography and Computer Security

Homework #2 – Solution

CHAPTER 3

Exercise #1

Compute the bits numbered 9, 39, 49, and 59 at the output of the first round of DES decryption, assuming that the ciphertext block is composed only of ones and the external key is composed only of zeros.

Decryption is the inverse of encryption. It follows the same steps. The only difference is that the order in which the subkeys are applied is reversed.

Ciphertext: 1111 1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111 1111

Key: 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000

Steps to apply on key:
1. Permuted Choice 1 – PC1
2. Left Circular Shift
3. Permuted Choice 2 – PC2

Steps to apply on ciphertext:
4. Initial Permutation – IP
5. Expansion – E-Table
6. XORing with Key
7. Passing through S-Boxes
8. Permutation – P
9. XORing with L_0
10. Swapping

1. Key – PC1
   Applying PC1 on a key of all zeros will not change the bits. It will only decrease its size from 64 bits to 56 bits.
   Key: 0000 0000 0000 0000 0000 0000 0000
   0000 0000 0000 0000 0000 0000 0000

2. Key – LCS
   Applying a left circular shift on the key will not change anything.
   Key: 0000 0000 0000 0000 0000 0000 0000
   0000 0000 0000 0000 0000 0000 0000

3. Key – PC2
   Applying PC2 on a key of all zeros will not change the bits. It will only decrease its size from 56 bits to 48 bits.
   Key: 0000 0000 0000 0000 0000 0000
   0000 0000 0000 0000 0000 0000

4. Ciphertext – IP
   Applying IP on a ciphertext of all ones will not change anything. After this stage, the ciphertext is divided into two halves, each of which is 32 bits long.
   L_0: 1111 1111 1111 1111 1111 1111 1111 1111
   R_0: 1111 1111 1111 1111 1111 1111 1111 1111

5. Ciphertext – E-Table
   Passing R_0 which is all ones through the expansion table will increase its size from 32 bits to 48 bits. All bits remain ones.
   R_0: 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

6. Ciphertext – XOR Key
   In this stage, R_0 is XORed with the 48-bit key. The output is still all ones.

1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111
0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111

7. Ciphertext – S-Boxes
   In this stage, we divide the output from the previous stage into 8 groups of 6 bits.
   111111 111111 111111 111111 111111 111111 111111 111111
   We have 8 S-Boxes which map 6 to 4 bits. Each of the above 8 groups will be inputted to one of the S-Boxes. The outer bits of a group – bits 1 and 6 – are the row bits. In our case they are always 11. This means that we should always look at the 3rd (lowest) row in the S-Boxes. The inner bits of a group – bits 2, 3, 4 and 5 – are the column bits. In our case they are always 1111. This means that we should always look at the 15th (right-most) column in the S-Boxes. Taking the values in the 3rd row and 15th column of each of the 8 S-Boxes will give us the following numbers:
   13 9 12 14 3 13 12 11
   After changing the above numbers to binary, we get the 32 bit output of this stage.
   1101 1001 1100 1110 0011 1101 1100 1011

8. Ciphertext – P
   Apply the permutation function P to the output from the previous stage.
   1101 1001 1100 1110 0011 1101 1100 1011

   0011 1000 1101 1011 1111 1001 1100 1011

9. Ciphertext – XOR L_0
   Get the value of R_1 by XORing the output from the previous stage with L_0.

0011	1000	1101	1011	1111	1001	1100	1011
1111	1111	1111	1111	1111	1111	1111	1111
1100	0111	0010	0100	0000	0110	0011	0100

10. Ciphertext – Swap

L_1:	1111	1111	1111	1111	1111	1111	1111	1111
R_1:	1100	0111	0010	0100	0000	0110	0011	0100

The bits numbered 9, 39, 49, and 59 are 1, 1, 0, and 1 respectively.

Exercise #2

Assume that you have the following input:

The key, K, in hexadecimal is:

F F D D B B 9 9 7 7 5 5 3 3 1 1

K in binary is:

1111	1111	1101	1101	1011	1011	1001	1001
0111	0111	0101	0101	0011	0011	0001	0001

The plaintext, T, in hexadecimal is the reverse of the key, K:

1 1 3 3 5 5 7 7 9 9 B B D D F F

Now, perform one round of DES, writing out the following steps:

a. Derive the first-round sub-key, K_1

Key:	1111	1111	1101	1101	1011	1011	1001	1001
	0111	0111	0101	0101	0011	0011	0001	0001

⇨ PC1

Key:	0000	1111	0011	0011	0101	0101	1111	
	0101	0101	0011	0011	0000	1111	1111	

⇨ LCS

Key:	0001	1110	0110	0110	1010	1011	1110	
	1010	1010	0110	0110	0001	1111	1110	

⇨ PC2

K_1:	**1111**	**0100**	**1111**	**1101**	**1001**	**1000**
	0110	**0100**	**1011**	**0110**	**0101**	**1010**

b. Derive L_0 and R_0

T: 0001 0001 0011 0011 0101 0101 0111 0111
1001 1001 1011 1011 1101 1101 1111 1111

⇨ IP

L_0: 1100 1100 1111 1111 1100 1100 1111 1111
R_0: 1111 0000 1010 1010 1111 0000 1010 1010

c. Use the expansion function, E, to get $E[R_0]$

$E(R_0)$: 0111 1010 0001 0101 0101 0101 0111 1010 0001 0101 0101 0101

d. Calculate $A = E[R_0] \oplus K_1$

$E(R_0)$: 0111 1010 0001 0101 0101 0101 0111 1010 0001 0101 0101 0101
K_1: 1111 0100 1111 1101 1001 1000 0110 0100 1011 0110 0101 1010
A: 1000 1110 1110 1000 1100 1101 0001 1110 1010 0011 0000 1111

A: 100011 101110 100011 001101 000111 101010 001100 001111

e. Perform S-box substitutions to obtain a 32-bit result, B

$S_1(100011) = 15$ 1111
$S_2(101110) = 1$ 0001
$S_3(100011) = 10$ 1010
$S_4(001101) = 0$ 0000
$S_5(000111) = 12$ 1100
$S_6(101010) = 8$ 1000
$S_7(001100) = 8$ 1000
$S_8(001111) = 4$ 0100

B: 1111 0001 1010 0000 1100 1000 1000 0100

f. Perform the permutation P(B)

P(B): 0001 0001 1000 0100 1100 0011 0010 0111

g. Compute $R_1 = P(B) \oplus L_0$

P(B): 0001 0001 1000 0100 1100 0011 0010 0111
L_0: 1100 1100 1111 1111 1100 1100 1111 1111
R_1: 1101 1101 0111 1011 0000 1111 1101 1000

h. Write down the resulting ciphertext

L_1: 1111 0000 1010 1010 1111 0000 1010 1010
R_1: 1101 1101 0111 1011 0000 1111 1101 1000

C: 1111 0000 1010 1010 1111 0000 1010 1010 1101
C: F 0 A A F 0 A A D
1101 0111 1011 0000 1111 1101 1000
D 7 B 0 F D 8