Homework #5

I. Lý thuyết

1. Hãy cho biết kích thước khối mã hóa, khóa và số vòng trong phương pháp DES?

II. Bài tập

2.

   a. Cho biết kết quả của phép dịch trái 3-bit của từ $(10011011)_2$

   b. Cho biết kết quả của phép dịch phải 3-bit của từ kết quả từ câu (a).

   c. So sánh kết quả câu (b) với từ gốc của (a) .

3. Cho biết kết quả của những biểu thức sau:

   a. $(01001101) \oplus (01001101)$

   b. $(01001101) \oplus (10110010)$

   c. $(01001101) \oplus (00000000)$

   d. $(01001101) \oplus (11111111)$

4. Một thông điệp có 2000 ký tự, giả sử rằng nếu nó được mã hóa dựa trên khối 64bits, hãy cho biết số bit(s) cần phải thêm vào?

5. Giả sử có bản rõ P (plaintext) và khóa K (key) được biểu dưới dạng số thập lục phân như sau: 0 1 2 3 4 5 6 7 8 9 A B C D E F. Hãy tính toán kết quả từng bước vòng mã hóa thứ nhất theo phương DES:

   a. Tính khóa con k_1
   b. Cho biết chuỗi bit L_0 và R_0
   c. Hãy mở rộng chuỗi con R_0 từ 32 bits thành 48 bits kết quả lưu vào $E(R_0)$.
   d. Hãy tính $A = E(R_0) \oplus k_1$
   e. Hãy tính B là kết quả của A khi qua các hộp S-boxes (Table 3.3 Definition of DES S-Boxes)

f. Hãy tính P(B) là hoán vị của B, trong đó P(.) hàm hoán vị[1] 32 bits
g. $R_1 = \text{P(B)} \oplus L_0$
h. Viết ra bản mật mã C_1 của vòng 1 theo phương pháp DES.

[1] Table 6.11, slide 6.27, bài giảng

Table 3.3 Definition of DES S-Boxes

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

--------//---------