Homework #5

I. Lý thuyết

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

Trong phương pháp mã hóa DES (Data Encryption Standard), các thông số kỹ thuật chính gồm:

Kích thước khối mã hóa (Block size): 64 bit

Kích thước khóa (Key size): 56 bit (với 8 bit kiểm tra chẵn lẻ, tổng cộng 64 bit nhưng thực tế chỉ có 56 bit được sử dụng cho mã hóa)

Số vòng (Number of rounds): 16 vòng

II. Bài tập

2.

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

Dịch trái 3-bit có nghĩa là dịch tất cả các bit sang trái 3 vị trí, và các bit dịch ra ngoài sẽ được quay lại từ phía bên phải.

$$(10011011)_2 \xrightarrow{\text{dịch trái 3-bit}} (11011100)_2$$

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

Dịch phải 3-bit có nghĩa là dịch tất cả các bit sang phải 3 vị trí, và các bit dịch ra ngoài sẽ được quay lại từ phía bên trái.

$$(11011100)_2 \xrightarrow{\text{dịch phải 3-bit}} (00011011)_2$$

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

- Từ gốc của câu (a): (10011011)2
- Kết quả của câu (b): (00011011)2

Kết quả từ câu (b) không giống hoàn toàn từ gốc của câu (a). Cụ thể, ba bit đầu tiên đã thay đổi từ 100 thành 000, trong khi năm bit cuối cùng vẫn giữ nguyên (11011).

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

a. (01001101) ⊕ (01001101)

Phép toán XOR giữa mỗi cặp bit:

$$0 \oplus 0 = 0$$
$$1 \oplus 1 = 0$$
$$0 \oplus 0 = 0$$
$$0 \oplus 0 = 0$$
$$1 \oplus 1 = 0$$
$$1 \oplus 1 = 0$$
$$0 \oplus 0 = 0$$
$$1 \oplus 1 = 0$$

Kết quả:

$$(01001101)_2 \oplus (01001101)_2 = (00000000)_2$$

b. (01001101) ⊕ (10110010)

Phép toán XOR giữa mỗi cặp bit:

$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$0 \oplus 1 = 1$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 0 = 1$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$

Kết quả:

$$(01001101)_2 \oplus (10110010)_2 = (11111111)_2$$

c. (01001101) ⊕ (00000000)

Phép toán XOR giữa mỗi cặp bit:

$$
\begin{aligned}
0 \oplus 0 &= 0 \\
1 \oplus 0 &= 1 \\
0 \oplus 0 &= 0 \\
0 \oplus 0 &= 0 \\
1 \oplus 0 &= 1 \\
1 \oplus 0 &= 1 \\
0 \oplus 0 &= 0 \\
1 \oplus 0 &= 1
\end{aligned}
$$

Kết quả:

$$(01001101)_2 \oplus (00000000)_2 = (01001101)_2$$

d. (01001101) ⊕ (11111111)

Phép toán XOR giữa mỗi cặp bit:

$$
\begin{aligned}
0 \oplus 1 &= 1 \\
1 \oplus 1 &= 0 \\
0 \oplus 1 &= 1 \\
0 \oplus 1 &= 1 \\
1 \oplus 1 &= 0 \\
1 \oplus 1 &= 0 \\
0 \oplus 1 &= 1 \\
1 \oplus 1 &= 0
\end{aligned}
$$

Kết quả:

$$(01001101)_2 \oplus (11111111)_2 = (10110010)_2$$

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?

- Mỗi ký tự thường được mã hóa thành 8 bit (1 byte).
- Một thông điệp có 2000 ký tự sẽ có độ dài:

$$2000 \text{ ký tự} \times 8 \text{ bit/ký tự} = 16000 \text{ bit}$$

$$\frac{16000 \text{ bit}}{64 \text{ bit/khối}} = 250 \text{ khối}$$

Kết luận

Số bit cần thêm vào để thông điệp có độ dài là bội của 64 bit:

$$\text{Số bit cần thêm vào} = 0 \text{ bit}$$

Note:

- Nếu tổng số bit là bội của 64, thì không cần thêm bit nào.
- Nếu không, cần thêm bit để làm cho tổng số bit là bội của 64.

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

Bảng PC-1:

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Ta có :
K = 0123456789ABCDEF
= 0000000100100011010001010110011110001001101010111100110111101111

Sau khi hoán vị PC-1, ta được:

PC-1 = 11110000110011001010101000001010101011001100111100000000

C0 = 1111000011001100101010100000

C1 = 11110000110011001010101000001

P0 = 10101010110011001111000000000

P1= 01010101100110011111000000001

Bảng PC-2

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

PC-2 = 11110000110011001010101000001010101011001100111100000000001

Sau khi hoán vị PC-2, ta được:

00001011 00000010 01100111 10011011 01001001 10100101

K1 = 0B02679B49A5

b. Cho biết chuỗi bit L_0 và R_0

Ta có P = 0123456789ABCDEF
= 0000000100100011010001010110011110001001101010111100110111101111

Initial Permutation							
58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Sau khi hoán vị, ta được:
IP=1100110000000000110011001111111111110000101010101111000010101010
L0 (32 ký tự từ bên trái) = 11001100000000001100110011111111

R0 (32 ký tự từ bên phải) =11110000101010101111000010101010

c. Hãy mở rộng chuỗi con R_0 từ 32 bits thành 48 bits kết quả lưu vào E(R_0).
Bảng mở rộng (E):

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Từ câu b ta có:

R0 =11110000101010101111000010101010

E(R0) = 011110100001010101010101011110100001010101011101 (BIN)

=> **E(R0)** = **7A15557A155D (HEX)**

d. Hãy tính $A = E(R_0) \oplus k_1$

Từ câu a và câu b, ta có:

K1 = 0B02679B49A5

byte	byte	hexan	dec
1	00001011	0B	11
2	00000010	02	2
3	01100111	67	103
4	10011011	9B	155
5	01001001	49	73
6	10100101	A5	165

E(R0) = 7A15557A155D

byte	byte	hexan	dec
1	01111010	7A	122
2	00010101	15	21
3	01010101	55	85
4	01111010	7A	122
5	00010101	15	21
6	01011101	5D	93

byte	$E(R_0) \oplus k_1$	bin	HEX
1	113	01110001	71
2	23	00010111	17
3	50	00110010	32
4	225	11100001	E1
5	92	01011100	5C
6	248	11111000	F8

A = E(R0)XORK1 = 711732E15CF8

e. Hãy tính *B* là kết quả của *A* khi qua các hộp S-boxes (Table 3.3 Definition of DES S-Boxes)

Từ câu d, ta có:

A = E(R0)XORK1 = 711732E15CF8

= 01110001000101110011001011100001010111001111000

stt	bin	hàng	cột	hàng	cột
1	011100	00	1110	0	E
2	010001	01	1000	1	8
3	011100	00	1110	0	E
4	110010	10	1001	2	9
5	111000	10	1100	2	C
6	010101	01	1010	1	A
7	110011	11	1001	3	9
8	111000	10	1100	2	C

S-box1	S-box2	S-box3	S-box4	S-box5	S-box6	S-box7	S-box8
0	12 (C)	2	1	6	13(D)	5	15(E)

=> **B** = 0C 21 6D 5E

f. Hãy tính P(*B*) là hoán vị của *B*, trong đó P(.) hàm hoán vị 32 bits

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Từ câu e ta có:
B = 0C216D5E
B(BIN) = 00001100001000010110110101011110

P(B) = 10011010000111100010000010111100

g. $R_1 = P(B) \oplus L_0$ Từ câu b và câu f ta có:

P(B) = 10011010000111100010000010111100

byte	byte	hexan	dec
1	10011010	9A	154
2	00011110	1E	30
3	00100000	20	32
4	10111100	BC	188

P(B)= 9A1E20BC

L0 = 11001100000000001100110011111111

byte	byte	hexan	dec
1	11001100	CC	204
2	00000000	00	0
3	11001100	CC	204
4	11111111	FF	255

L0= CC00CCFF

byte	XOR	bin	HEX
1	86	01010110	56
2	30	00011110	1E
3	236	11101100	EC
4	67	01000011	43

P(B)XORL0 = 561EEC43

01010110000111101110110001000011

=> $R1 = P(B) \oplus L0 =$ 01010110000111101110110001000011

h. Viết ra bản mật mã C_1 của vòng 1 theo phương pháp DES.

Từ câu b và g ta có:

R1 = 01010110000111101110110001000011

L1 = R0 = 11110000101010101111000010101010

C1 = R1&L1 =
01010110000111101110110001000011111100001010101011110000101010101