Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

CRYPTOGRAPHY AND NETWORK SECURITY

Lab 2

Nguyen Phuong Vuong - 1614186

Exercise 1.

A transformation is singular if it is not invertible or undoable. This means if you apply that, you will lose information. A nonsingular transform means you can undo the transform.

Exercise 2.

A block cipher is one in which a block of plain-text is treated as a whole and used to produce cipher-text block of equal length.
A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

Exercise 4.

Part a. Derive K1, the first round key.
K = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Follow the table PC-1, we have:
K+ = 1111 0000 1100 1100 1010 1010 0000 1010 1010 1100 1100 1111 0000 0000
Next, split this key into left and right halves, C0 and D0, where each half has 28 bits.
C0 = 1111 0000 1100 1100 1010 1010 0000
D0 = 1010 1010 1100 1100 1111 0000 0000
To derive K1, we will calculate C1, D1 by moving each bit one place to the left of C0 and D0.
C1 = 1110 0001 1001 1001 0101 0100 0001
D1 = 0101 0101 1001 1001 1110 0000 0001
We have **C1D1 = 1110 0001 1001 1001 0101 0100 0001 0101 0101 1001 1001 1110 0000 0001**
Follow the table PC-2, we have:

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

After we apply the permutation PC-2, becomes

K1 = 0000 1011 0000 0010 0110 0111 1001 1011 0100 1001 1010 0101

b,

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Follow the table IP, we have:

IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010

Next divide the permuted block IP into left half L0 of 32 bits and a right half R0 of 32 bits.

L0 = 1100 1100 0000 0000 1100 1100 1111 1111

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

c,

E BIT-SELECTION TABLE

32	1	2	3	4	5
4	5	6	7	8	9
8	9	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	30	31	32	1

The E table expands R0 to 48 bits:
E(R0) = 01110 100001 010101 010101 011110 100001 010101 010101
d,
A = 011100 010001 011100 110010 111000 010101 110011 110000
e,
Follow tables S1, S2, S3, S4, S5, S6, S7, S8, we have:
B1 = 111100, S1[0,14]= 0 or 0000
B2 = 010001, S2[1,8]= 12 or 1100
B3 = 011100, S3[0,14]= 2 or 0010
B4 = 110010, S4[2,9]= 1 or 0001
B5 = 111000, S5[2,12]= 6 or 0110
B6 = 010101, S6[1,10]= 13 or 1101
B7 = 110011, S7[3,9]= 5 or 0101
B8 = 110000, S8[2,8]= 0 or 0000
f, Follow the results of exercise e, we get B with 32 bits:
B = 0000 1100 0010 0001 0110 1101 0101 0000
g,

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Follow table P, we have:

P(B) = 1001 0010 0001 1100 0010 0000 1001 1100

h,

R1 = P (B) ⊕ L0

R1 = 0101 1110 0001 1100 1110 1100 0110 0011

i,

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

R1 = 0101 1110 0001 1100 1110 1100 0110 0011

L1 = R0. The cipher-text which is the concatenation of L1 and R1, is

F 0 A A F 0 A A 5 E 1 C E C 6 3

Exercise 5.

Decrypt the string (10100010) using the key (0111111101)

- First, we generate 2 keys:

We use table P10 to permutation key:

Table P10

Input	1	2	3	4	5	6	7	8	9	10
Output	3	5	2	7	4	10	1	9	8	6

We derive K = 11111 10011

We will calculate K1 by moving each bit one place to the left of 2 section of 11111-10011 and using table P8:

LS-1 = 11111 00111

Table P8

Input	1	2	3	4	5	6	7	8	9	10
Output	6	3	7	4	8	5	10	9		

We use table P8 to deriving permutation key:

K1 = 0101 1111

We will calculate K2 by moving each bit two place to the left of 2 section of 11111-00111 and using table P8:

LS-2 = 11111 11100

We use table P8 to deriving permutation key:

K2 = 1111 1100

- Secondly, we decrypt the string S = 10100010

Table IP

Input	1	2	3	4	5	6	7	8
Output	2	6	3	1	4	8	5	7

IP(S) = 0011 0001

Split IP(S) into 2 section such as the left section (0011) and the right section (0001)

Table E/P

Input	1	2	3	4				
Output	4	1	2	3	2	3	4	1

We use table E/P to deriving the permutated right section(0001)
E/P(0001) = 1000 0010
Xor(K2 and E/P(0001)) = 0111 1110
Split Xor(K2 and E/P(0001)) into 2 section such as the left section(0111) and the right section(1110)
We derive the left section(0111) to use for table S0:

- S_0

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

We have row= 01 and column = 11 ➔ S0(left) = 00
We derive the right section(1110) to use for table S1:

- S_1

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

We have row = 10 and column = 11 → S1(right) = 00
We use S1S2(0000) to use for table P4(2341) we derive P4(S1S2) = 0000
Xor(the left section of IP and P4(S1S2)) = 0011
We put together the right section of IP and the result of XOR above: 0001 0011 (1)
Split 0001 0011 into 2 section left (0001) and section right (0011)
We derive the left section(0011) to use for table S0:

- S_0

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

We have row= 01 and column = 01 ➔ S0(left) = 10
We derive the right section(0001) to use for table S1:

- S_1

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

We have row = 01 and column = 00 ➔ S1(right) = 10
We use S1S2(0100) to use for table P4(2341) we derive P4(S1S2) = 1010
Xor(the left section of (1) and P4(S1S2)) = 1011
We put together the right section of (1) and the result above: 1011 0011
We use it for table IP-1:

Input	1	2	3	4	5	6	7	8
Output	4	1	3	5	7	2	8	6

We derive the plain-text: 1110 1010