Activity # 3

Key: 00111010 01010101 11100001
00111100 10100000 00011110
10111111 00000101

Plain Text: 11010000 11110000 10101010
11001010 11100001 10111101
10101111 11110010

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

We use above table PC-1 to convert 64 bit key into 56 bit.

Permutedte key is following :

k^+ = 0101010 0000001 1001011
1010110 1110000 1011010
1011101 0011011

For C_0 & D_0 divide k^+ into half.

C_0 = 0101010 0000001 1001011
1010110

D_0 = 1110000 1011010 1011101
0011011

Iteration No	No. of left shift
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

We will generate keys

C_0 = 0101010000011001011101011
D_0 = 1110000101101010111001011

C_1 = 1010100000001100101110100
D_1 = 1100001011010101110011011

C_2 =
D_2 =
⋮
C_{15} =
D_{15} =

Now will convert 56 bit into 48 bit by using following PC-2 table.

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

For $C_1 D_1$

$K_1 =$ 110011 100010 110010
000110 010101 111101
100100 110010

Similarly generate keys for

$C_2 D_2 = K_2$ till $C_{16} D_{16} = K_{16}$

Initial Round:

Now we will take plain text convert it into another by using following table IP

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

plain text = 11010000 11110000
10101010 11001010 11100001
10111101 10101111 11110010

IP = 10011011 10100011 01100000
01110000 11111111 11110110
01101100 11001100

Divide IP into two half L_0 and R_0

L_0 = 10011011 10100011 01100000 01110000

R_0 = 11111111 11110110 01101100 11001100

Round 1

$L_n = R_{n-1}$

$R_n = L_{n-1} + f(R_{n-1}, K_n)$

put $n = 1$

$L_1 = R_0$

$R_1 = L_0 + f(R_0, K_1)$

(R_0, K_1)

K_1 is 48 bit & R_0 is 32 bit first we convert R_0 into 48 bit, using following E-bit selection Table.

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

R_0 = 1111 1111 1111 0110 0110 1100 1100 1100

E(R_0) = 011111 111111 111110 101100 001101 011001 011001 011001

$K_1 \oplus E(R_0) =$ 101100 011101
001100 101010
011000 100100
111101 101011

Now we will convert this into 32 bit again
We divide 48 bit into 6 bit chunk of 8 and named them $B_1, B_2 \ldots B_8$

$S_1(B_1), S_2(B_2) \ldots S_8(B_8)$

$S_1 = 101100$
$= 0010$

10 ⇒ 2 col
0110 = 6 Row

$S_2 = 011101$
$= 1011$

01 ⇒ 1 col
1110 ⇒ 14 Row

$S_3 = 001100$
$= 1111$

00 ⇒ 0 col
0110 ⇒ 6 Row

S_4 = 101010 → 10 ⇒ 2 Col, 0101 ⇒ 5 Row
= 1011

S_5 = 011000 → 00 ⇒ 0 Col, 1100 ⇒ 12 Row
= 1101

S_6 = 100100 → 10 ⇒ 2 Col, 0010 ⇒ 2 Row
= 1111

S_7 = 111010 → 11 ⇒ 3 col, 1110 ⇒ 14 Row
0011

S_8 = 101011 → 11 ⇒ 3 col, 0101 ⇒ 5 Row
= 1010

= 0010 1011 1111 1011 1101
1111 0011 1010

Now we will perform the permutation again

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

f = 1111 1111 0110 1111 0110
0111 0100 1100

~~R L P~~

$R_1 = L_0 \oplus f(R_0, K_1)$

= 10011011101000110110000
0011110000 ⊕ 1111 1111 0110
1111 0110 0111 0100 1100

R_1 = 01100100110011000000000
111001111100

L_1 = 1111 1111 1111 0111 0011 011100
1100 1100

Round ⇒ 2

L_2 = R_1

R_2 = $L_1 + f(R_1, K_2)$

K_2 = 000100 010000 011100
100111 100111 001100
101111 001110

R_1 = 011001 001100 110000 000
111 00 111100

$E(R_1)$ = 001100 001001 011001
011000 000000 001100
100111 111000

$K_2 \oplus E(R_1)$ = 001000 011001 000101
111111 100111 000010
001000 110110

By applying $S_1(B_1) \cdots S_8(B_8)$

We have
= 0010 0110 0000 1110 0111
0001 1111 1101

Now we perform permutation,

F_2 0110 1010 0101 0100
0011 1110 1111 0001

$R_2 = L_1 \oplus f(R_1, K_2)$

L_2 = 011001 001100 111000 000
111001 111100

R_2 = 100101 011010 001001 001
000 111101

Now Reverse order.

R_2L_2 = 10010101101000100101
00100001111010111001 0011
000 0000 11100 111100

Inverse permutation.

Use the following table

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

IP^{-1} = 01000001 00011100 11101011
00100011 01000111 10010011
10100100 01110000

Result = 73 28 235 35 71
147 112