Assignment 4
22F-3712

Question:

Key: F22371299BBCDFF1

Plaintext: F223712789ABCDEF

Binary form:-

Key: 1111 0010 0010 0011 0111 0001 0010 1001 1001 1011 1011 1100 1101 1111
1111 0001

Plaintext: 1111 0010 0010 0011 0111 0001 0010 0111 1000 1001 1010 1011 1100 1101
1110 1111

· The initial Permutation table, which is predefined is:

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

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

After Initial Permutation:

1100 0101 0000 0101 1110 1000 1111 1110 1111 0001 1010
1111 1110 0000 1010 1011

Now, split the permuted plaintext into two halves. Each half is 32 bit.

- Left half (L0): 1100 0101 0000 0101 1110 1000 1111 1110
- Right half (R0): 1111 0001 1010 1111 1110 0000 1010 1011

Key Generation:-

(iii) Convert 64 bit binary key into 56 by discarding every 8th bit, which is then divided into two 28-bit halves

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

→ PC-1

= 1111 0001 1100 0101 1010 1111 1111 0101 0011 0110 0000 0111 1000 0101

48 bit Key generation process for each round.

Splitting into halves:-

The 56-bit key is divided into two 28-bit halves:

- C_0 (28 bit): 1111 0001 1100 0101 0101 1111 1111
- D_0 (28 bit): 0101 0011 0110 0000 0111 1000 0101

C_4: 0111 0001 0101 0111 1111 1111 1100

D_4: 1101 1000 0001 1110 0001 0101 0100 → 2 shifts

C_5: 1100 0101 0101 1111 1111 1111 0001 → 2 shifts

D_5: 0110 0000 0111 1000 0101 0101 0011

C_6: 0001 0101 0111 1111 1111 1100 0111 → 2 shifts

D_6: 1000 0001 1110 0001 0101 0100 1101

Rounds:-

Using formula:-

$L_n = R_{n-1}$

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

'+' denote XOR addition, (bit-by-bit addition modulo 2)

⇒ for $n=1$, we have

K_1 = 0101 1011 1010 1100 1101 1111 0011 1100 0101 0000 1110 0010

$L_1 = R_0$ = 1111 0001 1010 1111 1110 0000 1010 1011

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

to calculate f, we first expand each block R_0 from 32 bits to 48 would be done by using 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

→ E-BIT SELECTION TABLE

We calculate $E(R_0)$ from R_0 as follows:-

R_0 = 1111 0001 1010 1111 1110 0000 1010 1011

$E(R_0)$ = 1111 1010 0011 1101 0101 1111 1111 0000
0001 0101 0101 0111

Now calculate $K_n + E(R_{n-1})$

K_1 = 0101 1011 1010 1100 1101 1111 0011 1100 0101 0000 1110 0010

$E(R_0)$ = 1111 1010 0011 1101 0101 1111 1111 0000 0001 0101 0101 0111

$K_1 + E(R_0)$ = 1010 0001 1001 0001 1000 0000 1100 1100 0000 0101 1011 0101

Substitution (S-Box)

$K_n + E(R_{n-1}) = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$

$S_1(B_1) S_2(B_2) S_3(B_3) S_4(B_4) S_5(B_5) S_6(B_6) S_7(B_7) S_8(B_8)$

$S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8$ tables:-

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_1

15	1	8	14	6	11	3	4	9	7	2	3	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	S_2
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
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	

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
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	

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
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	

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
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	

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	S_7
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	

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	1	0	14	9	2	S_8
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	

Make 6 bit pair of $K_n + E(R_{n-1})$

= 101000 011001 000110 000000 110011 000100 010110 110101

$S_1(B_1) = 1110$ | $S_3(B_3) = 1110$ | $S_5(B_5) = 1111$

$S_2(B_2) = 0110$ | $S_4(B_4) = 0\cancel{0}1\cancel{0}$ | $S_6(B_6) = 1010$

$S_7(B_7) = 0111$ $S_8(B_8) = 1001$

as $f = P(S_1(B_1) S_2(B_2) \dots S_8(B_8))$

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

$\rightarrow P$

$f = 1111\ 1011\ 1111\ 0101\ 1001\ 1111\ 1001\ 0100$

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

$R_1 = 1100\ 0101\ 0000\ 0101\ 1110\ 1000\ 1111\ 1110 +$
$1111\ 1011\ 1111\ 0101\ 1001\ 1111\ 1001\ 0100$

$R_1 = 0011\ 1110\ 1111\ 0000\ 0111\ 0111\ 0110\ 1010$

$\Rightarrow$ Using $n=2$,

$L_2 = R_1 = 0011\ 1110\ 1111\ 0000\ 0111\ 0111\ 0110\ 1010$

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

$K_2 = 1001\ 1001\ 0110\ 1110\ 1111\ 1110\ 1010\ 1010\ 0110$

using E_BIT SELECTION table, find $E(R_1)$

$E(R_1) = 0001\ 1111\ 1101\ 0111\ 1010\ 0000\ 0011\ 1010\ 1110\ 1011\ 0101\ 0100$

Now calculate $K_n + E(R_{n-1})$

$K_2 + E(R_1) = 1000\ 0110\ 1011\ 1001\ 0101\ 1110\ 1001\ 0000\ 1000\ 0010\ 1111$
0000

Now Substitution ⇒

Make 6 bit pair

100001 101011 100101 011110 100100 001000 001011 110000

$S_1(B_1) = 1111$

$S_2(B_2) = 0011$

$S_3(B_3) = 1101$

$S_4(B_4) = 1111$

$S_5(B_5) = 0001$

$S_6(B_6) = 1001$

$S_7(B_7) = 1001$

$S_8(B_8) = 0000$

as $f = P(S_1(B_1) \ldots S_8(B_8))$ using P table

$f = 1111\ 0110\ 1100\ 0001\ 1111\ 0011\ 0100\ 0011$

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

$= 1111\ 0001\ 1010\ 1111\ 1110\ 0000\ 1010\ 1011 +$
$1111\ 0001\ 1010\ 1111\ 0011\ 0100\ 0011$
$1111\ 0110\ 1100\ 0001\ 1111$

$R_2 = 0000\ 0111\ 0110\ 1110\ 0001\ 0011\ 1110\ 1000$

Using n=3

$L_3 = R_2 = 0000\ 0111\ 0110\ 1110\ 0001\ 0011\ 1110\ 1000$

$R_3 = L_2 + f(R_2, K_3)$

$K_3 = 1101\ 0101\ 0111\ 1111\ 1010\ 1100\ 0110\ 0000$
$0100\ 1001\ 1001\ 1001$

Using E-BIT SELECTION TABLE, find $E(R_2)$

$E(R_2) = 0000\ 0000\ 1110\ 0011\ 0101\ 1100\ 0000\ 1010$
$0111\ 1111\ 0101\ 0000$

Now calculate $K_n + E(R_{n-1})$

$K_3 + E(R_2)$ = 1101 0101 1001 1100 1111 0000 0110 1010 0011 0110 1100 1001

Substitution:-

Make 6 bit pair

110101 011001 110011 110000 011010 100011 011011 001001

$S_1(B_1)$ = 0011

$S_2(B_2)$ = 0110

$S_3(B_3)$ = 1111

$S_4(B_4)$ = 1111

$S_5(B_5)$ = 0000

$S_6(B_6)$ = 0011

$S_7(B_7)$ = 1111

$S_8(B_8)$ = 1010

as $f = P(S_1(B_1) \ldots S_8(B_8))$ using P table

f = 1100 1110 0111 0011 0011 0111 0101 0111

$R_3 = L_2 + f(R_2, K_3)$

R_3 = 0011 1110 1111 0000 0111 0111 0110 1010 +
1100 1110 0111 0011 0011 0111 0101 0111

R_3 = 1111 0000 1000 0011 0100 0000 0011 1101

final Cipher = 0000 0111 0110 1110 0001 0011 1110 1000 1111
0000 1000 0011 0100 0000 0011 1101