IS

Assignment

<u>*SUBMITTED TO:*</u>

<u>*Dr. Irfan Yousuf*</u>

<u>*SUBMITTED BY:*</u>

<u>*Hammad Ali (2021-CS-705)*</u>

<u>*SECTION:*</u>

<u>*A*</u>

Department of Computer Science, New Campus

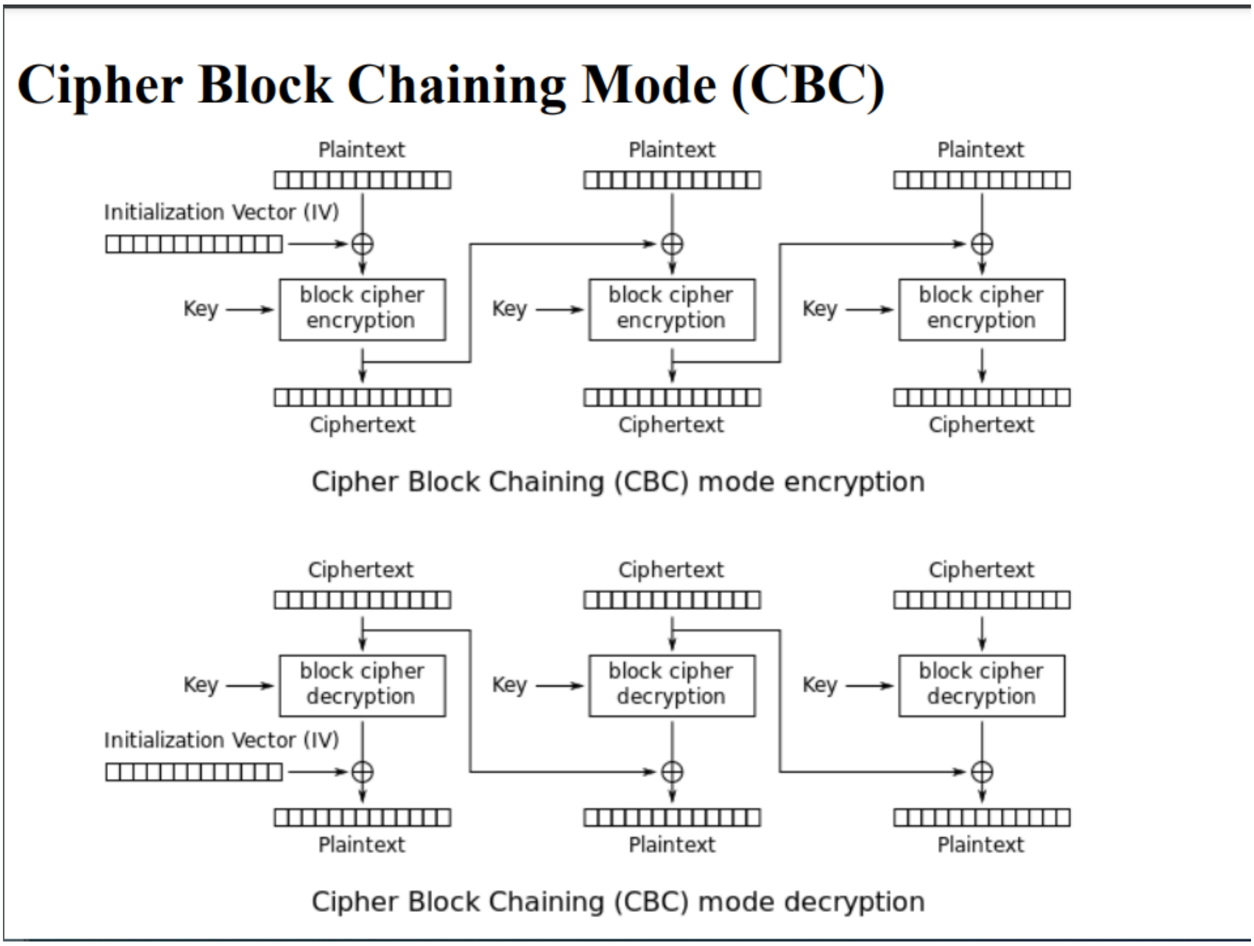
University of Engineering and Technology

Lahore, Pakistan

DES

Mode of Operation: Cipher Block Chaining (CBC)

Figures:



Here,

Block Cipher : DES

DES Key Schedule

(a) Input Key

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

(b) Permuted Choice One (PC-1)

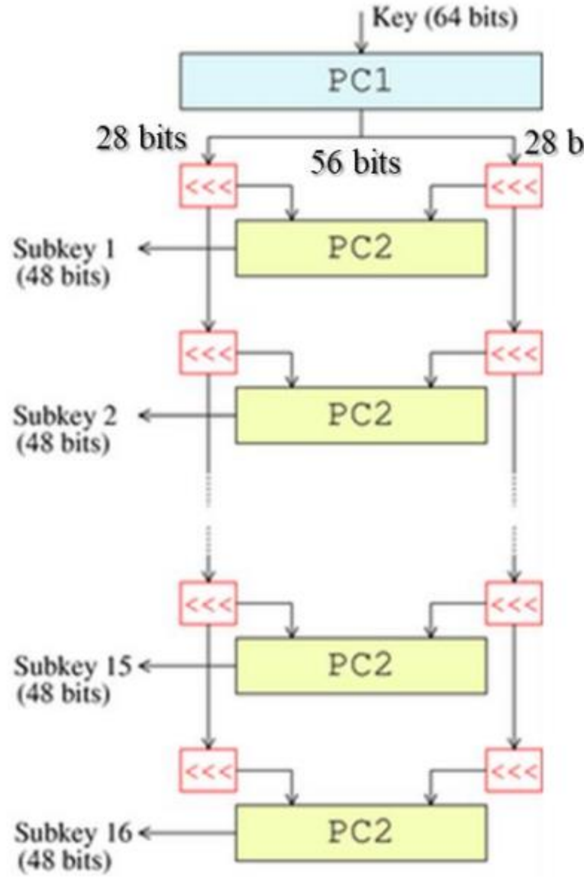
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (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

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1



64-bit ciphertext

Figure 4.5 General Depiction of DES Encryption Algorithm

Note: Only 2 rounds as per requirement.

DES Tables

	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1	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
	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
S_2	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
	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
S_7	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
	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
S_8	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

DES Tables

(a) Initial Permutation (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

(c) Expansion Permutation (E)

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

(b) Inverse Initial Permutation (IP^{-1})

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

(d) Permutation Function (P)

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

Plain Text = LAHORE IS A BIG CITY

P_1 = LAHOREIS

P_1 = 01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

P_2 = ABIGCITY

P_2 = 01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

KEY = HAMMADAL

KEY = 01001000 01000001 01001101 01001101 01000001 01000100 01000001 01001100

IV = MYVECTOR

IV = 01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

Generating Keys

KEY = 01001000 01000001 01001101 01001101 01000001 01000100 01000001 01001100

PC1:

Apply PC1: (64 => 56)

K+ = 0000000 0111111 1100000 0000000 0000000 0101011 0010001 1010000

C_0 = 0000000 0111111 1100000 0000000

D_0 = 0000000 0101011 0010001 1010000

1 circular left shift C_0, D_0

C_1 = 0000000 1111111 1000000 0000000

D_1 = 0000000 1010110 0100011 0100000

C_1D_1 = 0000000 1111111 1000000 0000000 0000000 1010110 0100011 0100000

Again 1 circular left shift C_1, D_1

C_2 = 0000001 1111111 0000000 0000000

D_2 = 0000001 0101100 1000110 1000000

C_2D_2 = 0000001 1111111 0000000 0000000 0000001 0101100 1000110 1000000

PC2:

Apply PC2: (56 => 48)

C_1D_1 = 0000000 1111111 1000000 0000000 0000000 1010110 0100011 0100000

K_1 = 101000 001001 001001 000010 100000 011001 110000 000100

C_2D_2 = 0000001 1111111 0000000 0000000 0000001 0101100 1000110 1000000

K_2 = 101000 000001 001001 010010 000110 010001 001000 001000

Encryption

$Block_1$

P_1 = 01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

$\bigoplus$

IV = 01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

M_1 = 00000001 00011000 00011110 00001010 00010001 00010001 00000110 00000001

IP:

Apply Initial Permutation on M_1:

IP = 00000000 00110110 01000100 10110001 00000000 00000000 00001110 01001100

Split (64 => 32,32) bit:

L_0 = 00000000 00110110 01000100 10110001

R_0= 00000000 00000000 00001110 01001100

$\boldsymbol{L_n = R_{n-1}}$

$\boldsymbol{R_n = L_{n-1} \oplus f(R_{n-1},K_n)}$

$Round_1$

L_1 = 00000000 00000000 00001110 01001100

R_0= 00000000 00000000 00001110 01001100

$E(R_0)$ = 000000 000000 000000 000000 000001 011100 001001 011000

K_1 = 101000 001001 001001 000010 100000 011001 110000 000100

$K_1 \oplus E(R_0)$ = 101000 001001 001001 000010 100001 000101 111001 011100

Apply S-Boxes:

$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$ = 1101 1111 0011 1101 1011 0100 1110 1100

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ ...S_8(B_8))$ = 11101101 10011000 11010100 11111111

$R_1 = L_0 \oplus f$ = 11101101 10101110 10010000 01001110

Round₂

L_2 = 11101101 10101110 10010000 01001110

R_1= 11101101 10101110 10010000 01001110

$E(R_1)$ = 011101 011011 110101 011101 010010 100000 001001 011101

K_2 = 101000 000001 001001 010010 000110 010001 001000 001000

$K_2 \oplus E(R_1)$ = 11010101 10101111 00001111 01010011 00010000 01010101

Apply S-Boxes:

$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$ = 0011 0000 1110 0011 0011 1011 1101 0110

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ ...S_8(B_8))$ = 10110010 01110011 00100011 10100111

$R_2 = L_1 \oplus f$ = 10110010 01110011 00101101 11101011

R_2L_2 = 10110010 01110011 00101101 11101011 11101101 10101110 10010000 01001110

IP^{-1}:

Apply Inverse of Initial Permutation on R_2L_2:

$C_1 = IP^{-1}$ = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

C_1 = s¦§Xõé

$Block_2$

P_2 = 01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

$\bigoplus$

IV = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

M_2 = 11010100 00110001 11101111 11100000 00011011 10111100 11000111 10110000

IP:

Apply Initial Permutation on M_2:

IP = 01001101 10110011 01100101 01010110 11101101 10101110 00110100 01010100

Split (64 => 32,32) bit:

L_0 = 01001101 10110011 01100101 01010110

R_0= 11101101 10101110 00110100 01010100

$L_n = R_{n-1}$

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

$Round_1$

L_1 = 11101101 10101110 00110100 01010100

R_0= 11101101 10101110 00110100 01010100

$E(R_0)$ = 011101 011011 110101 011100 000110 101000 001010 101001

K_1 = 101000 001001 001001 000010 100000 011001 110000 000100

$K_1 \oplus E(R_0)$ = 110101 010010 111100 011110 100110 110001 111010 101101

Apply S-Boxes:

$S_1(B_1)\ S_2(B_2)\ S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)\ S_8(B_8)$ = 0011 0111 1110 1111 1011 1011 0101 1000

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ ...S_8(B_8))$ = 11111011 01110001 01110011 11010110

L_0 = 01001101 10110011 01100101 01010110

$R_1 = L_0 \oplus f$ = 10110110 11000010 00010110 10000000

$Round_2$

$L_2 = R_1$ =10110110 11000010 00010110 10000000

R_1= 10110110 11000010 00010110 10000000

$E(R_1)$ = 010110 101101 011000 000100 000010 101101 010000 000001

K_2 = 101000 000001 001001 010010 000110 010001 001000 001000

$K_2 \oplus E(R_1)$ = 111110 101100 010001 010110 000100 111100 011000 001001

Apply S-Boxes:

$S_1(B_1)\ S_2(B_2)\ S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)\ S_8(B_8)$ = 0000 1101 0010 0101 0100 1011 0101 1010

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ \ldots S_8(B_8))$ = 10011010 00111110 01110000 00010100

L_1 = 11101101 10101110 00110100 01010100

$R_2 = L_1 \oplus f$ = 01110111 10010000 01000100 01000000

R_2L_2 = 01110111 10010000 01000100 01000000 10110110 11000010 00010110 10000000

IP^{-1}:

Apply Inverse of Initial Permutation on R_2L_2:

$C_2 = IP^{-1}$ = 01000000 11101000 11001100 00000000 11011000 11000000 01100101 10110010

C_2 = @èÌØÀe²

Decryption

C_1 = s¦§Xõé

C_1 = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

C_2 = @èÌØÀe²

C_2 = 01000000 11101000 11001100 00000000 11011000 11000000 01100101 10110010

KEY = HAMMADAL

KEY = 01001000 01000001 01001101 01001101 01000001 01000100 01000001 01001100

IV = MYVECTOR

IV = 01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

From Encryption:

K_1 = 101000 001001 001001 000010 100000 011001 110000 000100

K_2 = 101000 000001 001001 010010 000110 010001 001000 001000

Block₁

IP:

C_1 = s¦§Xõé

C_1 = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

Apply Initial Permutation C_1:

IP = 10110010 01110011 00101101 11101011 11101101 10101110 10010000 01001110

Split (64 => 32,32) bit:

L_0 = 10110010 01110011 00101101 11101011

R_0= 11101101 10101110 10010000 01001110

$L_n = R_{n-1}$

$R_n = L_{n-1} \oplus f(R_{n-1}, K_{3-n})$

$Round_1$

$L_1 =$ 11101101 10101110 10010000 01001110

$R_0 =$ 11101101 10101110 10010000 01001110

$E(R_0) =$ 011101 011011 110101 011101 010010 100000 001001 011101

$K_2 =$ 101000 000001 001001 010010 000110 010001 001000 001000

$K_2 \oplus E(R_0) =$ 110101 011010 111100 001111 010100 110001 000001 010101

Apply S-Boxes:

$S_1(B_1)\ S_2(B_2)\ S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)\ S_8(B_8) =$ 0011 0000 1110 0011 0011 1011 1101 0110

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ \ldots S_8(B_8)) =$ 10110010 01110011 00100011 10100111

$L_0 =$ 10110010 01110011 00101101 11101011

$R_1 = L_0 \oplus f =$ 00000000 00000000 00001110 01001100

$Round_2$

$L_2 =$ 00000000 00000000 00001110 01001100

$R_1 =$ 00000000 00000000 00001110 01001100

$E(R_1) =$ 000000 000000 000000 000000 000001 011100 001001 011000

K_1 = 101000 001001 001001 000010 100000 011001 110000 000100

$K_1 \oplus E(R_1)$ = 101000 001001 001001 000010 100001 000101 111001 011100

Apply S-Boxes:

$S_1(B_1)\ S_2(B_2)\ S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)\ S_8(B_8)$ = 1101 1111 0011 1101 1011 0100 1110 1100

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ ...S_8(B_8))$ = 11101101 10011000 11010100 11111111

L_1 = 11101101 10101110 10010000 01001110

$R_2 = L_1 \oplus f$ = 00000000 00110110 01000100 10110001

R_2L_2 = 00000000 00110110 01000100 10110001 00000000 00000000 00001110 01001100

FP:

Apply Final Permutation on R_2L_2:

FP = 00000001 00011000 00011110 00001010 00010001 00010001 00000110 00000001

IV = 01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

$P_1 = FP \oplus IV$ = 01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

P_1 = LAHOREIS

$Block_2$

IP:

C_2 = @èÌØÀe²

C_2 = 01000000 11101000 11001100 00000000 11011000 11000000 01100101 10110010

Apply Initial Permutation C_2:

IP = 01110111 10010000 01000100 01000000 10110110 11000010 00010110 10000000

Split (64 => 32,32) bit:

L_0 = 01110111 10010000 01000100 01000000

R_0= 10110110 11000010 00010110 10000000

$\boldsymbol{L_n = R_{n-1}}$

$\boldsymbol{R_n = L_{n-1} \oplus f(R_{n-1},K_{3-n})}$

$Round_1$

$L_1 = R_0 =$ 10110110 11000010 00010110 10000000

$R_0 =$ 10110110 11000010 00010110 10000000

$E(R_0) =$ 010110 101101 011000 000100 000010 101101 010000 000001

$K_2 =$ 101000 000001 001001 010010 000110 010001 001000 001000

$K_2 \oplus E(R_0) =$ 111110 101100 010001 010110 000100 111100 011000 001001

Apply S-Boxes:

$S_1(B_1)\ S_2(B_2)\ S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)\ S_8(B_8)$ = 0000 1101 0010 0101 0100 1011 0101 1010

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ ...S_8(B_8))$ = 10011010 00111110 01110000 00010100

$L_0 =$ 01110111 10010000 01000100 01000000

$R_1 = L_0 \oplus f =$ 11101101 10101110 00110100 01010100

Round₂

$L_2 = R_1 =$ 11101101 10101110 00110100 01010100

$R_1 =$ 11101101 10101110 00110100 01010100

$E(R_1) =$ 011101 011011 110101 011100 000110 101000 001010 101001

$K_1 =$ 101000 001001 001001 000010 100000 011001 110000 000100

$K_1 \oplus E(R_1) =$ 110101 010010 111100 011110 100110 110001 111010 101101

Apply S-Boxes:

$S_1(B_1)\ S_2(B_2)\ S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)\ S_8(B_8) =$ 0011 0111 1110 1111 1011 1011 0101 1000

Apply P-Box:

$f = P(S_1(B_1)\ S_2(B_2)\ ...S_8(B_8)) =$ 11111011 01110001 01110011 11010110

$L_1 =$ 10110110 11000010 00010110 10000000

$R_2 = L_1 \oplus f =$ 01001101 10110011 01100101 01010110

$R_2L_2 =$ 01001101 10110011 01100101 01010110 11101101 10101110 00110100 01010100

FP:

Apply Final Permutation on R_2L_2:

FP = 11010100 00110001 11101111 11100000 00011011 10111100 11000111 10110000

$C_1 =$ 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

$P_2 = FP \oplus IV =$ 01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

P_2 = ABIGCITY

The End
