***IS***

***Assignment***



***SUBMITTED TO:***

***Dr. Irfan Yousuf***

***SUBMITTED BY:***

***Hammad Ali (2021-CS-705)***

***SECTION:***

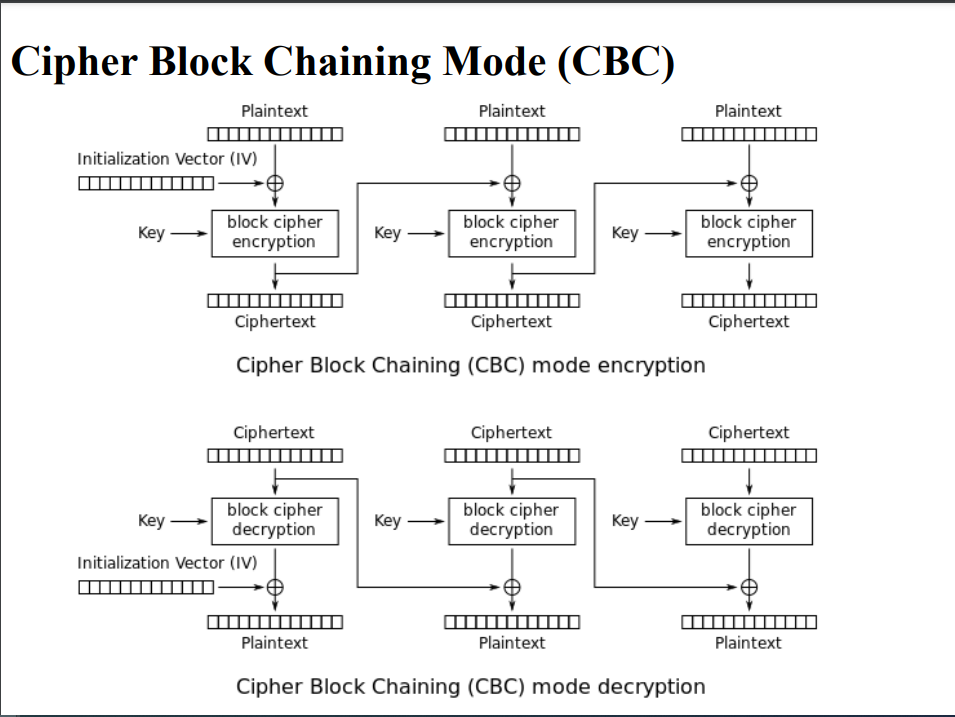
***A***

Department of Computer Science, New Campus

**University of Engineering and Technology Lahore, Pakistan**

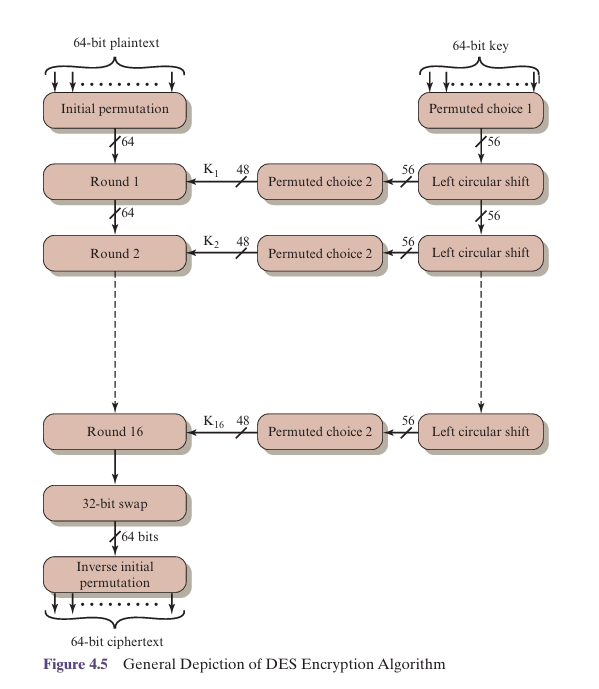
***DES***

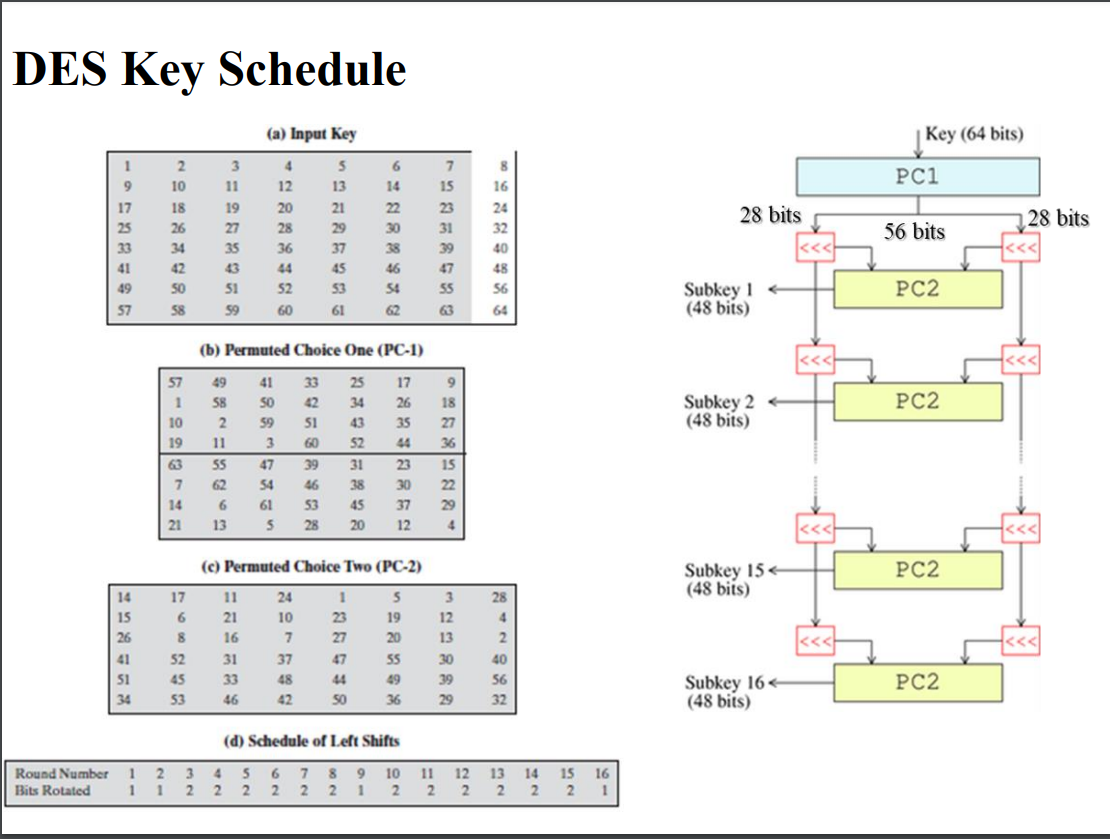
***Mode of Operation: Cipher Block Chaining (CBC)***

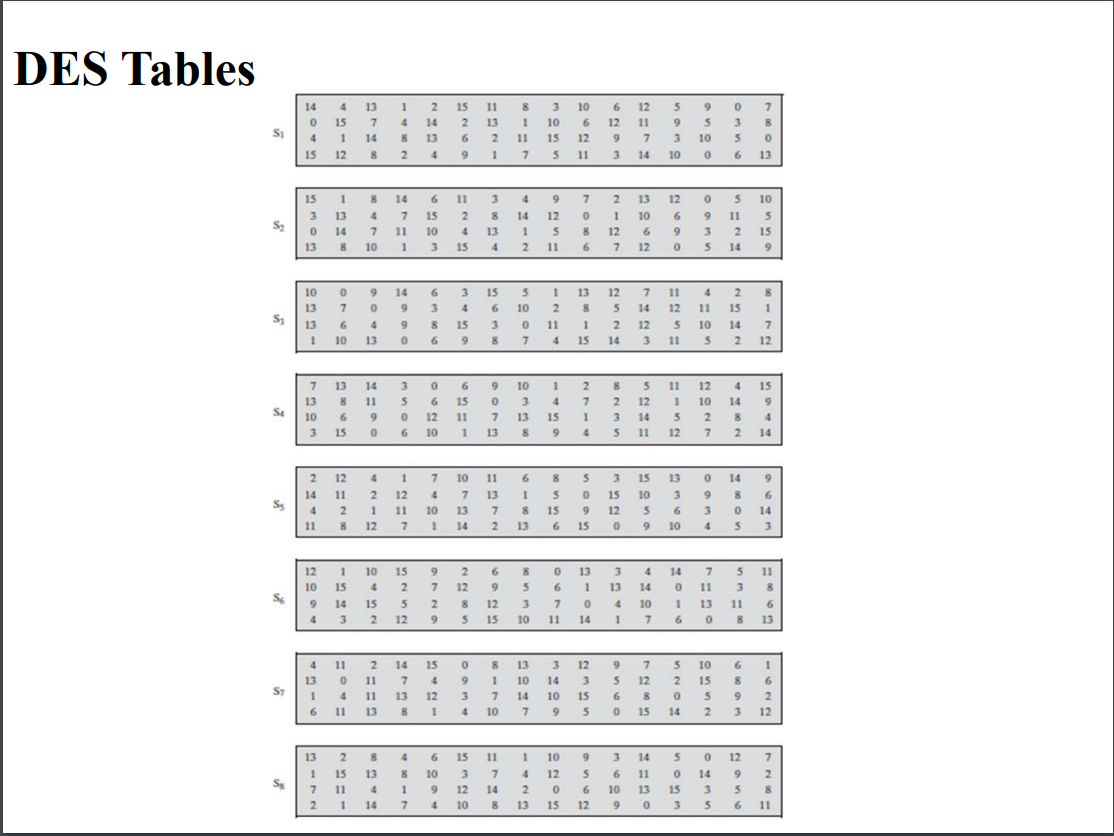
***Figures:***

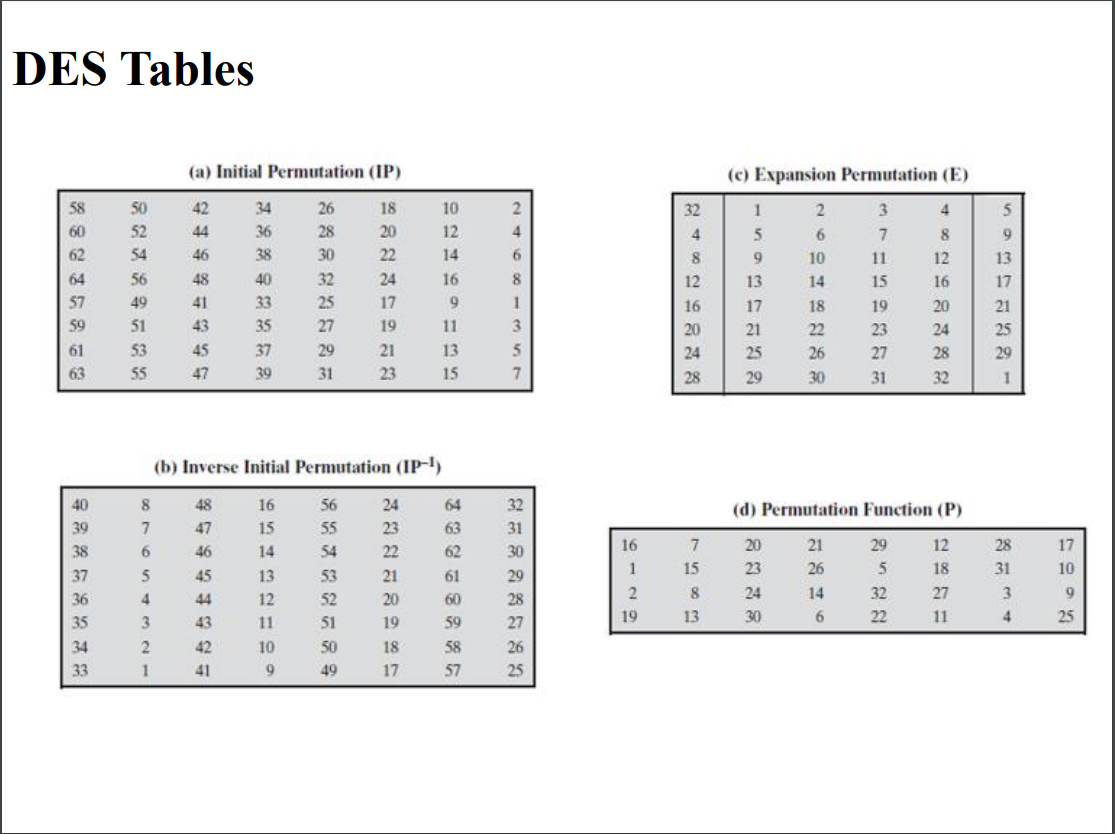
Here,

Block Cipher : **DES**

***Note:*** Only 2 rounds as per requirement.







Plain Text = LAHORE IS A BIG CITY

P1 = LAHOREIS

P1 = 01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

P2 = ABIGCITY

P2 = 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

C0 = 0000000 0111111 1100000 0000000

D0 = 0000000 0101011 0010001 1010000

1 circular left shift C0, D0

C1 = 0000000 1111111 1000000 0000000

D1 = 0000000 1010110 0100011 0100000

C1D1 = 0000000 1111111 1000000 0000000 0000000 1010110 0100011 0100000

Again 1 circular left shift C1, D1

C2 = 0000001 1111111 0000000 0000000

D2 = 0000001 0101100 1000110 1000000

C2D2 = 0000001 1111111 0000000 0000000 0000001 0101100 1000110 1000000

***PC2:***

Apply PC2: (56 => 48)

C1D1 = 0000000 1111111 1000000 0000000 0000000 1010110 0100011 0100000

K1 = 101000 001001 001001 000010 100000 011001 110000 000100

C2D2 = 0000001 1111111 0000000 0000000 0000001 0101100 1000110 1000000

K2 = 101000 000001 001001 010010 000110 010001 001000 001000

***Encryption***

***Block1***

P1 = 01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

⊕

IV = 01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

M1 = 00000001 00011000 00011110 00001010 00010001 00010001 00000110 00000001

***IP:***

Apply Initial Permutation on M1:

IP = 00000000 00110110 01000100 10110001 00000000 00000000 00001110 01001100

Split (64 => 32,32) bit:

L0 = 00000000 00110110 01000100 10110001

R0= 00000000 00000000 00001110 01001100

***Ln = Rn-1***

***Rn = Ln-1* ⊕ *f(Rn-1,Kn)***

***Round1***

L1 = 00000000 00000000 00001110 01001100

R0= 00000000 00000000 00001110 01001100

E(R0) = 000000 000000 000000 000000 000001 011100 001001 011000

K1 = 101000 001001 001001 000010 100000 011001 110000 000100

K1 ⊕ E(R0) = 101000 001001 001001 000010 100001 000101 111001 011100

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 1101 1111 0011 1101 1011 0100 1110 1100

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 11101101 10011000 11010100 11111111

R1 = *L0* ⊕ *f* = 11101101 10101110 10010000 01001110

***Round2***

L2 = 11101101 10101110 10010000 01001110

R1= 11101101 10101110 10010000 01001110

E(R1) = 011101 011011 110101 011101 010010 100000 001001 011101

K2 = 101000 000001 001001 010010 000110 010001 001000 001000

K2 ⊕ E(R1) = 11010101 10101111 00001111 01010011 00010000 01010101

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 0011 0000 1110 0011 0011 1011 1101 0110

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 10110010 01110011 00100011 10100111

R2 = *L1* ⊕ *f* = 10110010 01110011 00101101 11101011

R2L2 = 10110010 01110011 00101101 11101011 11101101 10101110 10010000 01001110

***IP-1:***

Apply Inverse of Initial Permutation on R2L2:

C1 = IP-1 = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

C1 = s¦§Xõé

***Block2***

P2 = 01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

⊕

IV = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

M2 = 11010100 00110001 11101111 11100000 00011011 10111100 11000111 10110000

***IP:***

Apply Initial Permutation on M2:

IP = 01001101 10110011 01100101 01010110 11101101 10101110 00110100 01010100

Split (64 => 32,32) bit:

L0 = 01001101 10110011 01100101 01010110

R0= 11101101 10101110 00110100 01010100

***Ln = Rn-1***

***Rn = Ln-1* ⊕ *f(Rn-1,Kn)***

***Round1***

L1 = 11101101 10101110 00110100 01010100

R0= 11101101 10101110 00110100 01010100

E(R0) = 011101 011011 110101 011100 000110 101000 001010 101001

K1 = 101000 001001 001001 000010 100000 011001 110000 000100

K1 ⊕ E(R0) = 110101 010010 111100 011110 100110 110001 111010 101101

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 0011 0111 1110 1111 1011 1011 0101 1000

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 11111011 01110001 01110011 11010110

L0 = 01001101 10110011 01100101 01010110

R1 = *L0* ⊕ *f* = 10110110 11000010 00010110 10000000

***Round2***

L2 = R1 =10110110 11000010 00010110 10000000

R1= 10110110 11000010 00010110 10000000

E(R1) = 010110 101101 011000 000100 000010 101101 010000 000001

K2 = 101000 000001 001001 010010 000110 010001 001000 001000

K2 ⊕ E(R1) = 111110 101100 010001 010110 000100 111100 011000 001001

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 0000 1101 0010 0101 0100 1011 0101 1010

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 10011010 00111110 01110000 00010100

L1 = 11101101 10101110 00110100 01010100

R2 = *L1* ⊕ *f* = 01110111 10010000 01000100 01000000

R2L2 = 01110111 10010000 01000100 01000000 10110110 11000010 00010110 10000000

***IP-1:***

Apply Inverse of Initial Permutation on R2L2:

C2 = IP-1 = 01000000 11101000 11001100 00000000 11011000 11000000 01100101 10110010

C2 = @èÌØÀe²

***Decryption***

C1 = s¦§Xõé

C1 = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

C2 = @èÌØÀe²

C2 = 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:

K1 = 101000 001001 001001 000010 100000 011001 110000 000100

K2 = 101000 000001 001001 010010 000110 010001 001000 001000

***Block1***

***IP:***

C1 = s¦§Xõé

C1 = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

Apply Initial Permutation C1:

IP = 10110010 01110011 00101101 11101011 11101101 10101110 10010000 01001110

Split (64 => 32,32) bit:

L0 = 10110010 01110011 00101101 11101011

R0= 11101101 10101110 10010000 01001110

***Ln = Rn-1***

***Rn = Ln-1* ⊕ *f(Rn-1,K3-n)***

***Round1***

L1 = 11101101 10101110 10010000 01001110

R0= 11101101 10101110 10010000 01001110

E(R0) = 011101 011011 110101 011101 010010 100000 001001 011101

K2 = 101000 000001 001001 010010 000110 010001 001000 001000

K2 ⊕ E(R0) = 110101 011010 111100 001111 010100 110001 000001 010101

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 0011 0000 1110 0011 0011 1011 1101 0110

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 10110010 01110011 00100011 10100111

L0 = 10110010 01110011 00101101 11101011

R1 = *L0* ⊕ *f* = 00000000 00000000 00001110 01001100

***Round2***

L2 = 00000000 00000000 00001110 01001100

R1= 00000000 00000000 00001110 01001100

E(R1) = 000000 000000 000000 000000 000001 011100 001001 011000

K1 = 101000 001001 001001 000010 100000 011001 110000 000100

K1 ⊕ E(R1) = 101000 001001 001001 000010 100001 000101 111001 011100

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 1101 1111 0011 1101 1011 0100 1110 1100

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 11101101 10011000 11010100 11111111

L1 = 11101101 10101110 10010000 01001110

R2 = *L1* ⊕ *f* = 00000000 00110110 01000100 10110001

R2L2 = 00000000 00110110 01000100 10110001 00000000 00000000 00001110 01001100

***FP:***

Apply Final Permutation on R2L2:

FP = 00000001 00011000 00011110 00001010 00010001 00010001 00000110 00000001

IV = 01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

P1 = FP ⊕ IV = 01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

P1 = LAHOREIS

***Block2***

***IP:***

C2 = @èÌØÀe²

C2 = 01000000 11101000 11001100 00000000 11011000 11000000 01100101 10110010

Apply Initial Permutation C2:

IP = 01110111 10010000 01000100 01000000 10110110 11000010 00010110 10000000

Split (64 => 32,32) bit:

L0 = 01110111 10010000 01000100 01000000

R0= 10110110 11000010 00010110 10000000

***Ln = Rn-1***

***Rn = Ln-1* ⊕ *f(Rn-1,K3-n)***

***Round1***

L1 = R0 = 10110110 11000010 00010110 10000000

R0 = 10110110 11000010 00010110 10000000

E(R0) = 010110 101101 011000 000100 000010 101101 010000 000001

K2 = 101000 000001 001001 010010 000110 010001 001000 001000

K2 ⊕ E(R0) = 111110 101100 010001 010110 000100 111100 011000 001001

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 0000 1101 0010 0101 0100 1011 0101 1010

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 10011010 00111110 01110000 00010100

L0 = 01110111 10010000 01000100 01000000

R1 = *L0* ⊕ *f* = 11101101 10101110 00110100 01010100

***Round2***

L2 = R1 = 11101101 10101110 00110100 01010100

R1 = 11101101 10101110 00110100 01010100

E(R1) = 011101 011011 110101 011100 000110 101000 001010 101001

K1 = 101000 001001 001001 000010 100000 011001 110000 000100

K1 ⊕ E(R1) = 110101 010010 111100 011110 100110 110001 111010 101101

Apply S-Boxes:

S1(B1) S2(B2) S3(B3) S4(B4) S5(B5) S6(B6) S7(B7) S8(B8) = 0011 0111 1110 1111 1011 1011 0101 1000

Apply P-Box:

*f* = P(*S1(B1) S2(B2) ...S8(B8)*) = 11111011 01110001 01110011 11010110

L1 = 10110110 11000010 00010110 10000000

R2 = *L1* ⊕ *f* = 01001101 10110011 01100101 01010110

R2L2 = 01001101 10110011 01100101 01010110 11101101 10101110 00110100 01010100

***FP:***

Apply Final Permutation on R2L2:

FP = 11010100 00110001 11101111 11100000 00011011 10111100 11000111 10110000

C1 = 10010101 01110011 10100110 10100111 01011000 11110101 10010011 11101001

P2 = FP ⊕ IV = 01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

P2 = ABIGCITY

***The End***