**Information Security Assignment**



**Session: 2021**

**Submitted by:**

**Wali Muhammad 2021-SE-39**

**Submitted to:**

**Ma’am Anam Iftikhar**

Department of Computer Science,

**University of Engineering and Technology, New Campus Lahore**

TABLE OF Contents

[Question 1 3](#_Toc166017495)

[Apply Data Encryption Standard (DES) using CBC 3](#_Toc166017496)

[DES Encryption using CBC flowchart: 4](#_Toc166017497)

[DES Encryption using CBC flowchart: 6](#_Toc166017498)

[Question 2 11](#_Toc166017499)

[Apply Advanced Encryption Standard (AES) 11](#_Toc166017500)

[**Key Scheduling Algorithm** 11](#_Toc166017501)

[Encryption 13](#_Toc166017502)

[Block 1 13](#_Toc166017503)

[Block 2 15](#_Toc166017504)

[**Result** 17](#_Toc166017505)

[Decryption 18](#_Toc166017506)

[Block 1 18](#_Toc166017507)

[Block 2 20](#_Toc166017508)

[Result 23](#_Toc166017509)

# Question 1

* Plain Text: LAHOREISABIGCITY
* Key: WaliMuha
* Block Size: 64 bits
* Number of Rounds: 2
* Algorithm: DES key scheduling algorithm to generate 2 round keys.
* Mode of Operation: Cipher Block Chaining (CBC).

## Apply Data Encryption Standard (DES) using CBC

**Plain key(64-bit): WALIMUHA**

01010111 01000001 01001100 01001001 01001101 01010101 01001000 01000001

**Sub key(56-bit): After PC-1**

0101011 0100000 0100110 0100100 0100110 0101010 0100100 0100000

C0: 0101 0110 1000 0001 0011 0010 0100

D0: 0100 1100 1010 1001 0010 0010 0000

**Left shift C0 and D0:**

C1: 1010 1101 0000 0010 0110 0100 1000

D1: 1001 1001 0101 0010 0100 0100 0000

**Left shift C1 and D1:**

C2: 0101 1010 0000 0100 1100 1001 0001

D2: 0011 0010 1010 0100 1000 1000 0001

**Round Key-1 (48-bits):**

PC-2(C1,D1): 1010 1100 0000 0100 1000 0000 1001 1010 0100 0010 0010 0000

**Round Key-2 (48-bits):**

PC-2(C2,D2): 0101 1010 0000 1001 0010 1001 0011 0101 1001 0100 0100 0001

## DES Encryption using CBC flowchart:

Plain Text: LAHOREIS ABIGCITY

Block-1: LAHOREIS

Block-2: ABIGCITY

**Block 1**

PT: LAHOREIS

PT-binary: 01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

IV: 01010111 01000001 01001100 01001001 01001101 01010101 01001000 01000001

PT ⊕ IV: 00011011 00000000 00000100 00000110 00011111 00010000 00000001 00010010

**Encryption** : DES Encryption with 2 Rounds

After Initial Permutation of PT ⊕ IV: 00011011 00000000 00000100 00000110 00011111 00010000 00000001 00010010

L0: 00011011 00000000 00000100 00000110

R0: 00011111 00010000 00000001 00010010

**Round 1**

L1 = R0: 00011111 00010000 00000001 00010010

R1 = L0 ⊕ f(R0, K1):

Computing f(R0, K1):

● E(R0): 000011 111110 100010 000000 000000 000010 100010 100100

● K1: 101011 000000 010010 000000 100110 100100 001000 100000

● K1 ⊕ E(R0): 101000 111110 110000 000000 100110 100110 101010 000100

● After S Box permutation on each block: 1101 0000 1111 1110 1000 1000 0110 1101

● After P permutation: 1100 0001 1111 1110 1000 1000 0110 1101

R1 = L0 ⊕ 1100 0001 1111 1110 1000 1000 0110 1101

R1 = 1101 1010 1111 1110 1000 1100 0110 1011

**Round 2**

L2 = R1: 1101 1010 1111 1110 1000 1100 0110 1011

R2 = L1 ⊕ f(R1, K2):

Computing f(R1, K2):

● E(R1): 111011 110101 011111 111101 010001 011000 001101 010111

● K2: 010110 100000 100100 101001 001101 011001 010001 000001

● K2 ⊕ E(R1): 101101 010101 111011 010100 011100 000001 011100 010110

● After S Box permutation on each block: 0001 1100 0000 0110 0000 0000 0000 1100

● After P permutation: 0000 1101 0000 0110 0000 0000 0000 1100

R2 = L1 ⊕ 0000 1101 0000 0110 0000 0000 0000 1100

R2 = 0001 0010 0001 0110 0000 0001 0001 1110

R2L2: 0001 0010 0001 0110 0000 0001 0001 1110 1101 1010 1111 1110 1000 1100 0110 1011

After Inverse Initial Permutation: 00010010 00010111 00000000 00011110 11011010 11111111 10001100 01101010

Cipher Text for block-1: DC2ETBNULRSÚÿŒj

**Block 2**

PT: ABIGCITY

PT-binary: 01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

IV: 00010010 00010111 00000000 00011110 11011010 11111111 10001100 01101010

PT ⊕ IV: 01010011 01010101 01001001 01011001 10011000 10110110 11011000 00110011

**Encryption**: DES Encryption with 2 Rounds

After Initial Permutation of PT ⊕ IV: 01010010 01010101 01001001 01011001 10011001 10110111 11011000 00110010

L0: 01010010 01010101 01001001 01011001

R0: 10011001 10110111 11011000 00110010

**Round 1**

L1 = R0: 10011001 10110111 11011000 00110010

R1 = L0 ⊕ f(R0, K1):

Computing f(R0, K1):

● E(R0): 0100 1111 0011 1101 1010 1111 1110 1111 0000 0001 1010 0101

● K1: 1010 1100 0000 0100 1000 0000 1001 1010 0100 0010 0010 0000

● K1 ⊕ E(R0): 1110 0011 0011 1001 0010 1111 0111 0101 0100 0011 1000 0101

● After S Box permutation on each block: 0011 1011 1110 0111 0011 0110 1000 0111

● After P permutation: 0011 1011 1110 0111 0010 0111 1000 0111

R1 = L0 ⊕ 0011 1011 1110 0111 0010 0111 1000 0111

R1 = 0110 1001 1011 0010 0110 1110 1101 1110

**Round 2**

L2 = R1: 0110 1001 1011 0010 0110 1110 1101 1110

R2 = L1 ⊕ f(R1, K2):

Computing f(R1, K2):

● E(R1): 001101 010011 110110 100100 001101 011101 011011 111100

● K2: 010110 100000 100100 101001 001101 011001 010001 000001

● K2 ⊕ E(R1): 011011 110011 010010 001101 000000 000100 001010 111101

● After S Box permutation on each block: 0101 1011 1010 1101 1110 1101 1111 0110

● After P permutation: 0101 1011 1010 1101 1111 1100 1111 0110

R2 = L1 ⊕ 0101 1011 1010 1101 1111 1100 1111 0110

R2 = 1100 0010 0001 1010 0010 0100 1100 0100

R2L2: 1100 0010 0001 1010 0010 0100 1100 0100 0110 1001 1011 0010 0110 1110 1101 1110

After Inverse Initial Permutation: 11000011 00011010 00100100 11000100 01101000 10110010 01101110 11011110

**Cipher Text** : ÃSUB$Äh²nÞ

**Complete Cipher**: DC2ETBNULRSÚÿŒjÃSUB$Äh²nÞ

## DES Encryption using CBC flowchart:

**Cipher Text**: DC2ETBNULRSÚÿŒjÃSUB$Äh²nÞ

**Block 1**: DC2ETBNULRSÚÿŒj

**Block 2**: ÃSUB$Äh²nÞ

Round Key 1 (48-bits): 1010 1100 0000 0100 1000 0000 1001 1010 0100 0010 0010 0000

Round Key 2 (48-bits): 0101 1010 0000 1001 0010 1001 0011 0101 1001 0100 0100 0001

**Block 1**

Cipher-text: DC2ETBNULRSÚÿŒj

Cipher-text binary: 00010010 00010111 00000000 00011110 11011010 11111111 10001100 01101010

**Decryption**: DES Decryption using 2 round keys

After Initial Permutation: 00010010 00010110 00000001 00011110 11011010 11111110 10001100 01101011

L0: 00010010 00010110 00000001 00011110

R0: 11011010 11111110 10001100 01101011

**Round 1**

L1 = R0: 11011010 11111110 10001100 01101011

R1 = L0 ⊕ f(R0, K2):

Computing f(R0, K2):

● E(R0): 111011 110101 011111 111101 010001 011000 001101 010111

● K2: 010110 100000 100100 101001 001101 011001 010001 000001

● K2 ⊕ E(R0): 101101 010101 111011 010100 011100 000001 011100 010110

● After S Box permutation on each block: 0001 1100 0000 0110 0000 0000 0000 1100

● After P permutation: 0000 1101 0000 0110 0000 0000 0000 1100

R1 = L0 ⊕ 0000 1101 0000 0110 0000 0000 0000 1100

0001 0010 0001 0110 0000 0001 0001 1110

R1 = 0001 1111 0001 0000 0000 0001 0001 0010

**Round 2**

L2 = R1: 0001 1111 0001 0000 0000 0001 0001 0010

R2 = L1 ⊕ f(R1, K1):

Computing f(R1, K1):

● E(R1): 0000 1111 1110 1000 1010 0000 0000 0000 0010 1000 1010 0100

● K1: 1010 1100 0000 0100 1000 0000 1001 1010 0100 0010 0010 0000

● K1 ⊕ E(R1): 1010 0011 1110 1100 0010 0000 1001 1010 0110 1010 1000 0100

● After S Box permutation: 1101 0000 1111 0100 1000 1000 0110 1101

● After P permutation: 1100 0001 1111 0100 1000 1000 0110 1101

R2 = L1 ⊕ 1100 0001 1111 0100 1000 1000 0110 1101

1101 1010 1111 1110 1000 1100 0110 1011

R2 = 0001 1011 0000 1010 0000 0100 00000 0110

R2L2: 0001 1011 0000 1010 0000 0100 00000 0110 0001 1111 0001 0000 0000 0001 0001 0010

After Inverse Initial Permutation: 00011011 00001010 00000100 000000110 00011111 00010000 00000001 00010010

IV: 01010111 01000001 01001100 01001001 01001101 01010101 01001000 01000001

Plain text: Inverse Initial Permutation ⊕ IV: 0100 1100 0100 0001 0100 1000 0100 1111 0101 0010 0100 0101 0100 1001 0101 0011

**Decrypted Text for block 1**: LAHOREIS

**Block 2**

Cipher-text: ÃSUB$Äh²nÞ

Cipher-text binary: 11000011 00011010 00100100 11000100 01101000 10110010 01101110 11011110

**Decryption**: DES Decryption using 2 round keys

After Initial Permutation: 11000010 00011010 00100100 11000100 01101001 10110010 01101110 11011110

L0: 11000010 00011010 00100100 11000100

R0: 01101001 10110010 01101110 11011110

**Round 1**

L1 = R0: 01101001 10110010 01101110 11011110

R1 = L0 ⊕ f(R0, K2):

Computing f(R0, K2):

● E(R0): 001101 010011 110110 100100 001101 011101 011011 111100

● K2: 010110 100000 100100 101001 001101 011001 010001 000001

● K2 ⊕ E(R0): 011011 110011 010010 001101 000000 000100 001010 111101

● After S Box permutation: 0101 1011 1010 1101 1110 1101 1111 0110

● After P permutation: 0101 1011 1010 1101 1111 1100 1111 0110

R1 = L0 ⊕ 0101 1011 1010 1101 1111 1100 1111 0110

R1 = 1001 1001 1011 0111 1101 1000 0011 0010

**Round 2**

L2 = R1: 1001 1001 1011 0111 1101 1000 0011 0010

R2 = L1 ⊕ f(R1, K1):

Computing f(R1, K1):

● E(R1): 010011 110011 110110 101111 111011 110000 000110 100101

● K1: 101011 000000 010010 000000 100110 100100 001000 100000

● K1 ⊕ E(R1): 111000 110011 100100 101111 011101 010100 001110 000101

● After S Box permutation: 0011 1011 1110 0111 0011 0110 1000 0111

● After P permutation: 0011 1011 1110 0111 0010 0111 1000 0111

R2 = L1 ⊕ 0011 1011 1110 0111 0010 0111 1000 0111

0110 1001 1011 0010 0110 1110 1101 1110

R2 = 0101 0010 0101 0101 0100 1001 0101 1001

R2L2: 01010010 01010101 01001001 01011001 10011001 10110111 11011000 00110010

After Inverse Initial Permutation: 01010011 01010101 01001001 01011001 10011000 10110110 11011000 00110011

IV: 00010010 00010111 00000000 00011110 11011010 11111111 10001100 01101010

Plain text: Inverse Initial Permutation ⊕ IV: 01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

**Decrypted Text for block 1**: ABIGCITY

**Complete Decrypted Text**: LAHOREIS ABIGCITY

# Question 2

## Apply Advanced Encryption Standard (AES)

* Plain Text: ISLAMABADISTHECAPITALOFPAKISTAN.
* Key: MY NAME IS WaliMuha
* Block Size: 128 bits
* Number of Rounds: 2
* Algorithm: AES key scheduling algorithm to generate 2 round keys.
* Mode of Operation: Cipher Block Chaining (CBC).
* **Plain Text:**  
  ISLAMABADISTHECAPITALOFPAKISTAN.
* **Plain Text Hex:**

49 53 4c 41 4d 41 42 41 44 49 53 54 48 45 43 41 50 49 54 41 4c 4f 46 50 41 4b 49 53 54 41 4e 2e

* **Key:**

MY NAME IS WaliMuha -> MYNAMEISWaliMuha

* **Key Hex:**

4d 59 4e 41 4d 45 49 53 57 61 6c 69 4d 75 68 61

* **Initialization Vector (IV)**

00 00 00 00

00 00 00 00

00 00 00 00

00 00 00 00

**Key Scheduling Algorithm**

Splitting into Words (32 bits each):

w[0] = 4d4d574d

w[1] = 59456175

w[2] = 4e496c68

w[3] = 41536961

w[4] = w[0] ⊕ g(w[3]) = 4d4d574d ⊕ B65A9D85 = E232FCF1

w[5] = w[4] ⊕ w[1] = E232FCF1 ⊕ 59456175 = 91929188

w[6] = w[5] ⊕ w[2] = 91929188 ⊕ 4e496c68 = B159E4E6

w[7] = w[6] ⊕ w[3] = B159E4E6 ⊕ 41536961 = D679A293

K1 = Concatenation of w[4], w[5], w[6], w[7]: E232FCF191929188B159E4E6D679A293

w[8] = w[4] ⊕ g(w[7]) = E232FCF1 ⊕ 30D238E6 = 56 082007 C71AB18F76435569A03AF7FA

w[9] = w[8] ⊕ g(w[7])

= 56082007C71AB18F76435569A03AF7FA ⊕ 30D238E6

= 30D238E6AC8BD01767B3548FE1FEB876

w[10] = w[9] ⊕ g(w[9])

= 30D238E6AC8BD01767B3548FE1FEB876 ⊕ 8A118AD9

= B1F4505F24A63260F1C1DF574F8E5E4F

w[11] = w[10] ⊕ g(w[10])

= B1F4505F24A63260F1C1DF574F8E5E4F ⊕ BC3EC2B7

= 0708D7480844F1404EFD1A2A38C5CFB8

* After words generation, making keys from words:

**K0 =**

4d 4d 57 4d

59 45 61 75

4e 49 6c 68

41 53 69 61

**K1 =**

d1 9c cb 86

1c 59 38 4d

a1 e8 84 ec

a2 f1 98 f9

**K2 =**

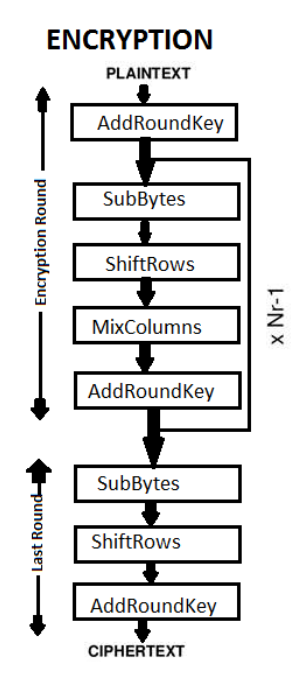
30 ac 67 e1

d2 8b b3 fe

38 d0 54 b8

e6 17 8f 76

## Encryption



## Block 1

**Plain Text** =

49 4d 44 48

53 41 49 43

4c 42 53 43

41 41 54 41

1. **After Plain Text XOR with IV and Round Key**

|  |  |  |
| --- | --- | --- |
| IV | Round Key (K0) | Output |
| 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | 4d 4d 57 4d  59 45 61 75  4e 49 6c 68  41 53 69 61 | 04 00 13 3d  0a 04 28 05  02 0b 3f 30  00 12 3d 20 |

1. **Round 1**
   1. **Substitute Bytes**

|  |  |
| --- | --- |
| Input | Output |
| 04 00 13 3d  0a 04 28 05  02 0b 3f 30  00 12 3d 20 | f2 67 77 63 63 f2 2b c9 7d 34 75 27 6b 04 f1 b7 |

* 1. **Shift Rows**

|  |  |
| --- | --- |
| Input | Output |
| f2 67 77 63 63 f2 2b c9 7d 34 75 27 6b 04 f1 b7 | F2 f2 75 b7 63 34 f1 63 7d 04 77 c9 6b 67 2b 27 |

* 1. **Mix Columns**

|  |  |  |
| --- | --- | --- |
| Input | Constant Matrix | Output |
| F2 f2 75 b7 63 34 f1 63 7d 04 77 c9 6b 67 2b 27 | 02 03 01 01  01 02 03 01  01 01 02 03  03 01 01 02 | 30 25 28 ff 08 60 0b a6 48 25 d7 7d 73 ff 33 bf |

* 1. **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K1) | Output |
| 30 25 28 ff 08 60 0b a6 48 25 d7 7d 73 ff 33 bf | d1 9c cb 86  1c 59 38 4d  a1 e8 84 ec  a2 f1 98 f9 | e1 39 89 5d 94 39 e3 57 83 1d 53 e5 f5 b2 df 46 |

1. **Round 2**
   1. **Substitute Bytes**

|  |  |
| --- | --- |
| Input | Output |
| e1 39 89 5d 94 39 e3 57 83 1d 53 e5 f5 b2 df 46 | f8 12 a7 4c 22 12 11 5b ec a4 ed d9 e6 37 9e 5a |

* 1. **Shift Rows**

|  |  |
| --- | --- |
| Input | Output |
| f8 12 a7 4c 22 12 11 5b ec a4 ed d9 e6 37 9e 5a | f8 12 ed 5a 22 a4 9e 4c ec 37 a7 5b e6 12 11 d9 |

* 1. **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K2) | Output |
| f8 12 ed 5a 22 a4 9e 4c ec 37 a7 5b e6 12 11 d9 | 30 ac 67 e1  d2 8b b3 fe  38 d0 54 b8  e6 17 8f 76 | c8 c0 d5 bc 8e 2f 4e 5b 8b 84 f3 d4 07 ec a9 af |

## Block 2

**Plain Text**

50 4c 41 54

49 4f 4b 41

54 46 49 4e

41 50 53 2e

1. **After Plain text XOR with IV and Round Key**

|  |  |  |
| --- | --- | --- |
| Input | K0 | Output |
| c8 c0 d5 bc 8e 2f 4e 5b 8b 84 f3 d4 07 ec a9 af | 4d 4d 57 4d  59 45 61 75  4e 49 6c 68  41 53 69 61 | d5 d0 cf bc 8f 25 41 58 9d ae d6 ee 1e d8 8f e0 |

1. **Round 1**
   1. **Substitute Bytes**

|  |  |
| --- | --- |
| Input | Output |
| d5 d0 cf bc 8f 25 41 58 9d ae d6 ee 1e d8 8f e0 | 03 70 8a 65 73 3f 83 6a 5e e4 f6 28 72 61 73 e1 |

* 1. **Shift Rows**

|  |  |
| --- | --- |
| Input | Output |
| 03 70 8a 65 73 3f 83 6a 5e e4 f6 28 72 61 73 e1 | 03 3f f6 e1 73 e4 73 65 5e 61 8a 6a 72 70 83 28 |

* 1. **Mix Columns**

|  |  |  |
| --- | --- | --- |
| Input | Constant Matrix | Output |
| 03 3f f6 e1 73 e4 73 65 5e 61 8a 6a 72 70 83 28 | 02 03 01 01  01 02 03 01  01 01 02 03  03 01 01 02 | 50 9d f3 15 c7 50 de c8 ff 73 8e dd df 24 67 35 |

* 1. **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K1) | Output |
| 50 9d f3 15 c7 50 de c8 ff 73 8e dd df 24 67 35 | d1 9c cb 86  1c 59 38 4d  a1 e8 84 ec  a2 f1 98 f9 | 81 81 52 b7 5b 09 36 39 34 4b 0a 45 59 69 8b cc |

1. **Round 2**
   1. **Substitute Bytes**

|  |  |
| --- | --- |
| Input | Output |
| 81 81 52 b7 5b 09 36 39 34 4b 0a 45 59 69 8b cc | 0c 0c 00 a9 39 01 05 12 18 b3 67 6e cb f9 3d 4b |

* 1. **Shift Rows**

|  |  |
| --- | --- |
| Input | Output |
| 0c 0c 00 a9 39 01 05 12 18 b3 67 6e cb f9 3d 4b | 0c 01 67 4b 39 b3 3d a9 18 f9 00 12 cb 0c 05 6e |

* 1. **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K2) | Output |
| 0c 01 67 4b 39 b3 3d a9 18 f9 00 12 cb 0c 05 6e | 30 ac 67 e1  d2 8b b3 fe  38 d0 54 b8  e6 17 8f 76 | 3c d3 5f ad 95 38 ed be 7f 4a 54 9d 2a f2 bd 18 |

**Result**

|  |  |
| --- | --- |
| Block 1 | Block 2 |
| ISLAMABADISTHECA | PITALOFPAKISTAN. |
| c8c0d5bc8e2f4e5b8b84f3d407eca9af | 3cd35fad9538edbe7f4a549d2af2bd18 |
| ��ռ�/N[����쩯 | <�\_��8��JT�\*� |

## Decryption

A diagram of a computer program

Description automatically generated

## Block 1

**Cipher Text =**

c8 c0 d5 bc 8e 2f 4e 5b 8b 84 f3 d4 07 ec a9 af

1. **Add Round key (K2)**

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K2) | Output |
| c8 c0 d5 bc 8e 2f 4e 5b 8b 84 f3 d4 07 ec a9 af | 30 ac 67 e1  d2 8b b3 fe  38 d0 54 b8  e6 17 8f 76 | f8 12 ed 5a 22 a4 9e 4c ec 37 a7 5b e6 12 11 d9 |

1. **Round 1**
   1. **Inverse Shift Row**

|  |  |
| --- | --- |
| Input | Output |
| f8 12 ed 5a 22 a4 9e 4c ec 37 a7 5b e6 12 11 d9 | f8 12 a7 4c 22 12 11 5b ec a4 ed d9 e6 37 9e 5a |

* 1. **Inverse Sub Bytes**

|  |  |
| --- | --- |
| Input | Output |
| f8 12 a7 4c 22 12 11 5b ec a4 ed d9 e6 37 9e 5a | e1 39 89 5d 94 39 e3 57 83 1d 53 e5 f5 b2 df 46 |

* 1. **Inverse Mix Column**

|  |  |  |
| --- | --- | --- |
| Input | Constant Matrix | Output |
| e1 39 89 5d 94 39 e3 57 83 1d 53 e5 f5 b2 df 46 | 0E 0B 0D 09  09 0E 0B 0D  0D 09 0E 0B  0B 0D 09 0E | 30 25 28 ff 08 60 0b a6 48 25 d7 7d 73 ff 33 bf |

* 1. **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K1) | Output |
| 30 25 28 ff 08 60 0b a6 48 25 d7 7d 73 ff 33 bf | d1 9c cb 86  1c 59 38 4d  a1 e8 84 ec  a2 f1 98 f9 | f2 f2 75 b7 63 34 f1 63 7d 04 77 c9 6b 67 2b 27 |

1. **Round 2**
   1. **Inverse Shift Row**

|  |  |
| --- | --- |
| Input | Output |
| f2 f2 75 b7 63 34 f1 63 7d 04 77 c9 6b 67 2b 27 | f2 67 77 63 63 f2 2b c9 7d 34 75 27 6b 04 f1 b7 |

* 1. **Inverse Sub Bytes**

|  |  |
| --- | --- |
| Input | Output |
| f2 67 77 63 63 f2 2b c9 7d 34 75 27 6b 04 f1 b7 | 04 0a 02 00 00 04 0b 12 13 28 3f 3d 05 30 2b 20 |

* 1. **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K0) | Output |
| 04 0a 02 00 00 04 0b 12 13 28 3f 3d 05 30 2b 20 | 4d 4d 57 4d  59 45 61 75  4e 49 6c 68  41 53 69 61 | 49 4d 44 48  53 41 49 43  4c 42 53 43  41 41 54 41 |

**XOR with IV:**

|  |  |
| --- | --- |
| IV | Result |
| 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | 49 4d 44 48  53 41 49 43  4c 42 53 43  41 41 54 41 |

**Convert HEX to Plain Text**

|  |  |
| --- | --- |
| Hex | Plain Text |
| 49 4d 44 48  53 41 49 43  4c 42 53 43  41 41 54 41 | I M D H  S A I E  L B S C  A A T A |

## Block 2

Cipher Text =

3c d3 5f ad 95 38 ed be 7f 4a 54 9d 2a f2 bd 18

1. Add Round Key

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K2) | Output |
| 3c d3 5f ad 95 38 ed be 7f 4a 54 9d 2a f2 bd 18 | 30 ac 67 e1  d2 8b b3 fe  38 d0 54 b8  e6 17 8f 76 | 0c 01 67 4b 39 b3 3d a9 18 f9 00 12 cb 0c 05 6e |

1. Round 1
   1. After Inverse Shift Row

|  |  |
| --- | --- |
| Input | Output |
| 0c 01 67 4b 39 b3 3d a9 18 f9 00 12 cb 0c 05 6e | 0c 0c 00 a9 39 01 05 12 18 b3 67 6e cb f9 3d 4b |

* 1. After Inverse Sub Bytes

|  |  |
| --- | --- |
| Input | Output |
| 0c 0c 00 a9 39 01 05 12 18 b3 67 6e cb f9 3d 4b | 81 81 52 b7 5b 09 36 39 34 4b 0a 45 59 69 8b cc |

* 1. After Inverse Mix Column

|  |  |  |
| --- | --- | --- |
| Input | Constant Matrix | Output |
| 81 81 52 b7 5b 09 36 39 34 4b 0a 45 59 69 8b cc | 0E 0B 0D 09  09 0E 0B 0D  0D 09 0E 0B  0B 0D 09 0E | 50 9d f3 15 c7 50 de c8 ff 73 8e dd df 24 67 35 |

* 1. After Add Round Key =

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K1) | Output |
| 50 9d f3 15 c7 50 de c8 ff 73 8e dd df 24 67 35 | d1 9c cb 86  1c 59 38 4d  a1 e8 84 ec  a2 f1 98 f9 | 03 3f f6 e1 73 e4 73 65 5e 61 8a 6a 72 70 83 28 |

1. Round 2
   1. After Inverse Shift Row

|  |  |
| --- | --- |
| Input | Output |
| 03 3f f6 e1 73 e4 73 65 5e 61 8a 6a 72 70 83 28 | 03 70 8a 65 73 3f 83 6a 5e e4 f6 28 72 61 73 e1 |

* 1. After Inverse Sub Bytes

|  |  |
| --- | --- |
| Input | Output |
| 03 70 8a 65 73 3f 83 6a 5e e4 f6 28 72 61 73 e1 | d5 d0 cf bc 8f 25 41 58 9d ae d6 ee 1e d8 8f e0 |

* 1. Add Round Key

|  |  |  |
| --- | --- | --- |
| Input | Round Key (K0) | Output |
| d5 d0 cf bc 8f 25 41 58 9d ae d6 ee 1e d8 8f e0 | 4d 4d 57 4d  59 45 61 75  4e 49 6c 68  41 53 69 61 | 98 89 81 fd c2 60 08 0b ca cf ba 87 53 ad e7 81 |

XOR with IV:

|  |  |
| --- | --- |
| IV | Result |
| 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | 50 4c 41 54  49 4f 4b 41  54 46 49 4e  41 50 53 2e |

Convert HEX to Plain Text

|  |  |
| --- | --- |
| Hex | Plain Text |
| 50 4c 41 54  49 4f 4b 41  54 46 49 4e  41 50 53 2e | P L A T  I O K A  T F I A  A P S . |

Result

|  |  |
| --- | --- |
| Block 1 | Block 2 |
| 49 4d 44 48  53 41 49 43  4c 42 53 43  41 41 54 41 | 50 4c 41 54  49 4f 4b 41  54 46 49 4e  41 50 53 2e |
| ISLAMABADISTHECA | PITALOFPAKISTAN. |