**Information Security Assignment**



**Session: 2021**

**Submitted by:**

**Numan Ahmad 2021-SE-24**

**Submitted to:**

**Ma’am Anam Iftikhar**

Department of Computer Science,

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

# Question 1

**Data Encryption Standard (DES) Cryptography using CBC**

* Plain Text: LAHOREIS ABIGCITY
* Key: NOMANAHM
* 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).
* Initialization Vector: NOMANAHM
* **Round keys Generation using DES key Scheduling Algorithm**

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

01001110 01001111 01001101 01000001 01001110 01000001 01001000 01001101

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

0100 1110 1001 1101 0011 0010 0000 0100 1110 1000 0001 0010 0010 0110

**C0**: 0100 1110 1001 1101 0011 0010 0000

**D0**: 0100 1110 1000 0001 0010 0010 0110

Left shift C0 and D0:

**C1**: 1001 1101 0011 1010 0110 0100 0000

**D1**: 1001 1101 0000 0010 0100 0100 1100

Left shift C1 and D1:

**C2**: 0011 1010 0111 0100 1100 1000 0001

**D2**: 0011 1010 0000 0100 1000 1001 1001

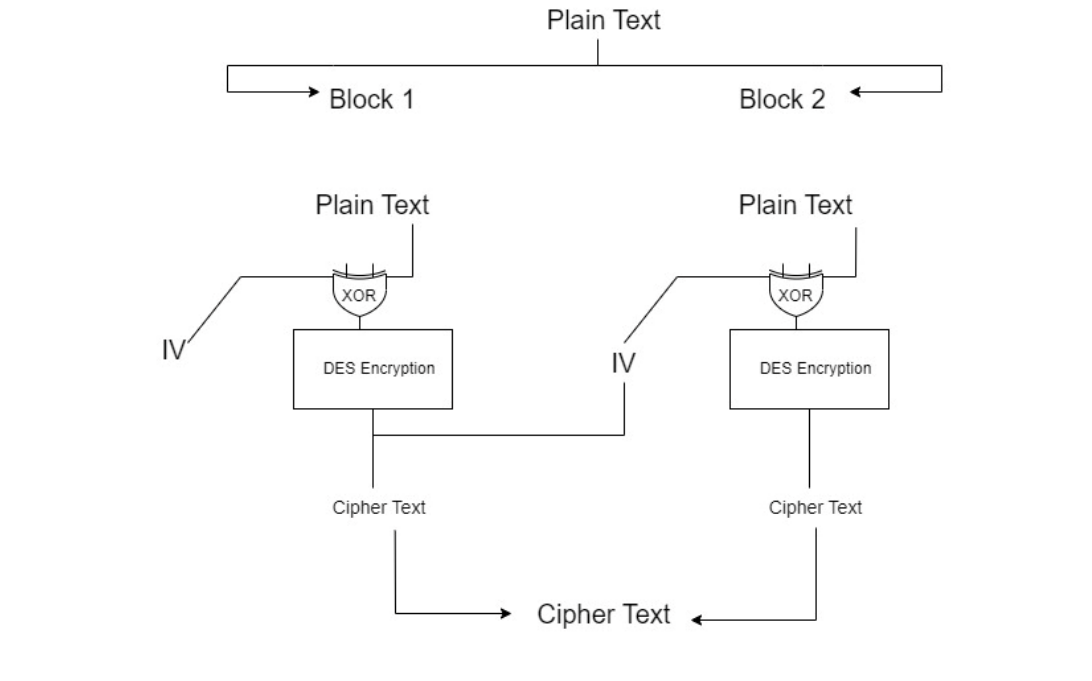
**Round Key-1 (48-bits):**

PC-2(C1,D1): 1001 1100 1110 1001 1000 0000 1001 1110 0000 0010 0010 0100

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

PC-2(C2,D2): 0011 1011 1101 0011 0010 0001 0011 1000 0001 0100 0100 1101

**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:** 01001110 01001111 01001101 01000001 01001110 01000001 01001000 01001101

**PT ⊕ IV:** 00000010 00001110 00000101 00001110 00011100 00000100 00000001 00011110

**Encryption** : DES Encryption with 2 Rounds

**After Initial Permutation of PT ⊕ IV**: 00000010 00001110 00000100 00001110 00011101 00000101 00000000 00011110

**L0**: 00000010 00001110 00000100 00001110

**R0**: 00011101 00000101 00000000 00011110

**Round 1**

**L1 = R0:** 00011101 00000101 00000000 00011110

**R1 = L0 ⊕ f(R0, K1):**

Computing f(R0, K1):

* E(R0): 0000 1111 1010 1000 0000 1010 1000 0000 0000 0000 1111 1100
* K1: 1001 1100 1110 1001 1000 0000 1001 1110 0000 0010 0010 0100
* K1 ⊕ E(R0): 1001 0011 0100 0001 1000 1010 0001 1110 0000 0010 1101 1000
* After S Box permutation on each block: 1110 1001 0001 1111 0100 0100 0010 0101
* After P permutation: 1110 1001 0001 1111 0100 0101 0010 0100

**R1** **=** L0 **⊕** 1110 1001 0001 1111 0100 0101 0010 0100

**R1 =** 1110 1011 0001 0001 0100 0001 0010 1010

**Round 2**

**L2 = R1:** 1110 1011 0001 0001 0100 0001 0010 1010

**R2 = L1 ⊕ f(R1, K2):**

Computing f(R1, K2):

* E(R1): 0111 0101 0110 1000 1010 0010 1010 0000 0010 1001 0101 0101
* K2: 0011 1011 1101 0011 0010 0001 0011 1000 0001 0100 0100 1101
* K2 ⊕ E(R1): 0100 1110 1011 1011 1000 0011 1001 1000 0011 1101 0001 1000
* After S Box permutation on each block: 0110 1001 1011 1111 1000 1111 1001 0101
* After P permutation: 0110 1001 1011 1111 1000 1111 1001 0101

**R2** **=** L1 **⊕**  0110 1001 1011 1111 1000 1111 1001 0101

**R2 =** 0111 0100 1011 1010 10001111 1000 1011

**R2L2:** 0111 0100 1011 1010 10001111 1000 1011 1110 1011 0001 0001 0100 0001 0010 1010

**After Inverse Initial Permutation:** 01110100 10111010 10001111 10001010 11101011 00010001 01000001 00101011

**Cipher Text for block-1**: tº ŠëDC1A+

**Block-2**

**PT:** ABIGCITY

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

**IV:** 01110100 10111010 10001111 10001010 11101011 00010001 01000001 00101011

**PT ⊕ IV:** 00110101 11111000 11000110 11001101 10101000 01011000 00010101 01110010

**Encryption:** DES Encryption with 2 Rounds

**After Initial Permutation of PT ⊕ IV**: 00110100 11111001 11000110 11001100 10101001 01011000 00010100 01110011

**L0**: 00110100 11111001 11000110 11001100

**R0**: 10101001 01011000 00010100 01110011

**Round 1**

**L1 = R0:** 10101001 01011000 00010100 01110011

**R1 = L0 ⊕ f(R0, K1):**

Computing f(R0, K1):

* E(R0): 1101 0101 0010 1010 1111 0000 0000 1010 1000 0011 1010 0111
* K1: 1001 1100 1110 1001 1000 0000 1001 1110 0000 0010 0010 0100
* K1 ⊕ E(R0): 0100 1001 1100 0011 0111 0000 1001 0100 1000 0001 1000 0011
* After S Box permutation on each block: 1010 0000 1101 1111 1000 0010 0001 1111
* After P permutation: 1010 0001 1101 1110 1000 0011 0001 1110

**R1** **=** L0 **⊕** 1010 0001 1101 1110 1000 0011 0001 1110

**R1 =** 1001 0101 0010 0111 0100 0101 1101 0010

**Round 2**

**L2 = R1:** 1001 0101 0010 0111 0100 0101 1101 0010

**R2 = L1 ⊕ f(R1, K2):**

Computing f(R1, K2):

* E(R1): 0100 1010 1010 1001 0000 1110 1010 0000 1011 1110 1010 0101
* K2: 0011 1011 1101 0011 0010 0001 0011 1000 0001 0100 0100 1101
* K2 ⊕ E(R1): 0111 0001 0111 1010 0010 1111 1001 1000 1010 1010 1110 1000
* After S Box permutation on each block: 0000 1011 1101 0111 1000 1111 1001 1101
* After P permutation: 0000 1011 1101 0111 1000 1111 1001 1101

**R2** **=** L1 **⊕** 0000 1011 1101 0111 1000 1111 1001 1101

**R2 =** 1010 0010 1000 1111 1001 1011 1110 1110

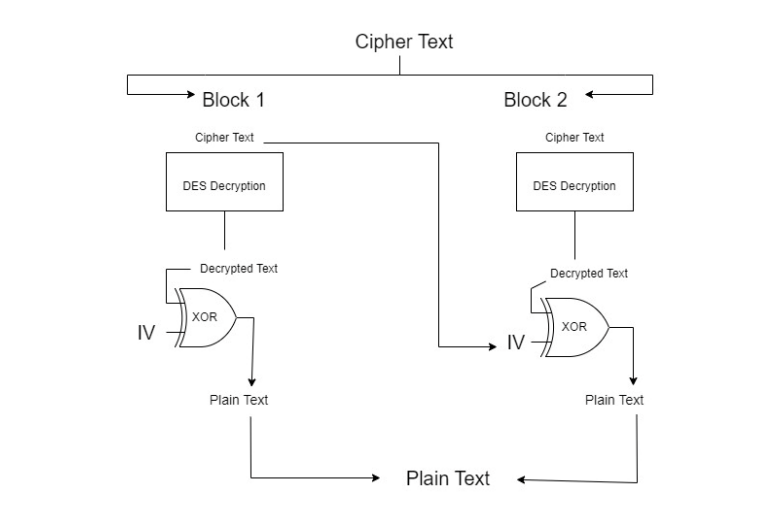
**R2L2:** 1010 0010 1000 1111 1001 1011 1110 1110 1001 0101 0010 0111 0100 0101 1101 0010

**After Inverse Initial Permutation:** 10100011 10001110 10011011 11101110 10010101 00100111 01000101 11010010

**Cipher Text for block-2**: £Ž›î•'EÒ

**Complete Cipher:** tº ŠëDC1A+£Ž›î•'EÒ

**DES Encryption using CBC flowchart:**

****

**Cipher Text:**  tº ŠëDC1A+£Ž›î•'EÒ

**Block-1:** tº ŠëDC1A+

**Block-2:** £Ž›î•'EÒ

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

1001 1100 1110 1001 1000 0000 1001 1110 0000 0010 0010 0100

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

0011 1011 1101 0011 0010 0001 0011 1000 0001 0100 0100 1101

**Block-1**

**Cipher-text:** tº ŠëDC1A+

**Cipher-text binary:** 01110100 10111010 10001111 10001010 11101011 00010001 01000001 00101011

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

**After Initial Permutation:** 01110100 10111010 10001111 10001011 11101011 00010001 01000001 00101010

**L0:** 01110100 10111010 10001111 10001011

**R0:** 11101011 00010001 01000001 00101010

**Round 1**

**L1 = R0:** 11101011 00010001 01000001 00101010

**R1 = L0 ⊕ f(R0, K2):**

Computing f(R0, K2):

* E(R0): 0111 0101 0110 1000 1010 0010 1010 0000 0010 1001 0101 0101
* K2: 0011 1011 1101 0011 0010 0001 0011 1000 0001 0100 0100 1101
* K2 ⊕ E(R0): 0100 1110 1011 1011 1000 0011 1001 1000 0011 1101 0001 1000
* After S Box permutation on each block: 0110 1001 1011 1111 1000 1111 1001 0101
* After P permutation: 0110 1001 1011 1111 1000 1111 1001 0101

**R1** **=** L0 **⊕** 0110 1001 1011 1111 1000 1111 1001 0101

**R1 =** 0001 1101 0000 0101 0000 0000 0001 1110

**Round 2**

**L2 = R1:** 0001 1101 0000 0101 0000 0000 0001 1110

**R2 = L1 ⊕ f(R1, K1):**

Computing f(R1, K1):

* E(R1): 0000 1111 1010 1000 0000 1010 1000 0000 0000 0000 1111 1100
* K1: 1001 1100 1110 1001 1000 0000 1001 1110 0000 0010 0010 0100
* K1 ⊕ E(R1): 1001 0011 0100 0001 1000 1010 0001 1110 0000 0010 1101 1000
* After S Box permutation: 1110 1001 0001 1111 0100 0100 0010 0101
* After P permutation: 1110 1001 0001 1111 0100 0101 0010 0100

**R2** **=** L1 **⊕**  1110 1001 0001 1111 0100 0101 0010 0100

**R2 =** 0000 0010 0000 1110 0000 0100 0000 1110

**R2L2:** 0000 0010 0000 1110 0000 0100 0000 1110 0001 1101 0000 0101 0000 0000 0001 1110

**After Inverse Initial Permutation:** 0000 0010 0000 1110 0000 0101 0000 1110 0001 1100 0000 0100 0000 0001 0001 1110

**IV:** 0100 1110 0100 1111 0100 1101 0100 0001 0100 1110 0100 0001 0100 1000 0100 1101

**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:** £Ž›î•'EÒ

**Cipher-text binary:** 10100011 10001110 10011011 11101110 10010101 00100111 01000101 11010010

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

**After Initial Permutation:** 10100010 10001111 10011011 11101110 10010101 00100111 01000101 11010010

**L0:** 10100010 10001111 10011011 11101110

**R0:**  10010101 00100111 01000101 11010010

**Round 1**

**L1 = R0:**  10010101 00100111 01000101 11010010

**R1 = L0 ⊕ f(R0, K2):**

Computing f(R0, K2):

* E(R0): 0100 1010 1010 1001 0000 1110 1010 0000 1011 1110 1010 0101
* K2: 0011 1011 1101 0011 0010 0001 0011 1000 0001 0100 0100 1101
* K2 ⊕ E(R0): 0111 0001 0111 1010 0010 1111 1001 1000 1010 1010 1110 1000
* After S Box permutation on each block: 0000 1011 1101 0111 1000 1111 1001 1101
* After P permutation: 00001011 11010111 10001111 10011101

**R1** **=** L0 **⊕** 00001011 11010111 10001111 10011101

**R1 =** 01111111 01101101 00000000 00010110

**Round 2**

**L2 = R1:** 01111111 01101101 00000000 00010110

**R2 = L1 ⊕ f(R1, K1):**

Computing f(R1, K1):

* E(R1): 0011 1111 1110 1011 0101 1010 1000 0000 0000 0000 1010 1100
* K1: 1001 1100 1110 1001 1000 0000 1001 1110 0000 0010 0010 0100
* K1 ⊕ E(R1): 1010 0011 0000 0010 1101 1010 0001 1110 0000 0010 1000 1000
* After S Box permutation: 1101 1111 0010 1001 0100 0100 1111 0010
* After P permutation: 1101 1111 0010 1001 0100 0100 1111 0010

**R2** **=** L1 **⊕**  1101 1111 0010 1001 0100 0100 1111 0010

**R2 =** 0100 1010 0000 1110 0000 0001 0010 0000

**R2L2:** 01001010 00001110 00000001 00100000 01111111 01101101 00000000 00010110

**After Inverse Initial Permutation:** 01001010 00001110 00000001 00100000 01111110 01101101 00000001 00010110

**IV:** 01110100 10111010 10001111 10001010 11101011 00010001 01000001 00101011

**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 NumanAhm
* 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 43 41 50 49 54 41 4c 4f 46 50 41 4b 49 53 54 41 4e 2e
* Key: MY NAME IS NumanAhm
* Key Hex: 4D 59 20 4E 41 4D 45 20 49 53 20 4E 75 6D 61 6E

**Key Scheduling Algorithm**

K0 = 4D 59 20 4E 41 4D 45 20 49 53 20 4E 75 6D 61 6E

K1 = 41 68 6D 41 64 66 5A 7A 6D 45 5A 4A 72 77 6F 51

K2 = 1D 84 45 0B C4 C2 95 D0 8B 10 8B D9 68 AD C3 0E

Initialization Vector = 69 20 61 6D 20 67 61 79 69 20 61 6D 20 67 61 79

## Encryption

## Block 1

**Plain Text =**

49 4D 44 48

53 41 49 45

4C 42 53 43

41 41 54 41

**After Plain Text XOR with IV** =

20 6D 25 25

73 20 24 65

2B 23 3E 63

61 26 35 38

1. **Add Round Key**

| Plain Text | K0 | Output |
| --- | --- | --- |
| 20 6D 25 25  73 20 24 65  2B 23 3E 63  61 26 35 38 | 4D 59 20 4E  41 4D 45 20  49 53 20 4E  75 6D 61 6E | 6D 34 05 6B  32 6D 61 45  62 70 1E 2D  14 4B 54 56 |

1. **Round 1**
   1. **After Substitute Bytes** =

51 4F EF D6

A4 51 B8 E2

B5 98 38 A2

7D A0 6E 85

* 1. **After Shift Rows** =

51 4F EF D6

51 B8 E2 A4

38 A2 B5 98

85 7D A0 6E

* 1. **After Mix Columns Matrix Multiplication** =

BA 84 F4 7A

EC 35 92 C6

20 F6 37 1A

D1 C1 C9 A4

* 1. **Add Round Key**

| Input | Round Key (K1) | Output |
| --- | --- | --- |
| BA 84 F4 7A  EC 35 92 C6  20 F6 37 1A  D1 C1 C9 A4 | 41 68 6D 41  64 66 5A 7A  6D 45 5A 4A  72 77 6F 51 | BB EC 05 3B  88 53 C8 BC  0D 63 6D 30  A3 B6 66 F5 |

1. **Round 2**
   1. **After Substitute Bytes =**

**6E 42 60 1A**

**19 26 8F 6A**

**B0 67 D1 52**

**53 D8 29 84**

* 1. **After Shift Rows =**

**6E 42 60 1A**

**26 8F 6A 19**

**D1 52 B0 67**

**84 53 D8 29**

* 1. Add Round Key

| Input | K2 | Output |
| --- | --- | --- |
| 6E 42 60 1A  26 8F 6A 19  D1 52 B0 67  84 53 D8 29 | 1D 84 45 0B  C4 C2 95 D0  8B 10 8B D9  68 AD C3 0E | 73 C6 25 11  E2 4D FF 12  5D 42 3B BE  E0 F1 1B 25 |

## Block 2

**Plain Text =**

50 4C 41 54

49 4F 4B 41

54 46 49 4E

41 50 53 2E

**After Plain Text XOR with IV =**

39 6C 20 39

69 2E 26 61

33 27 24 6E

61 37 32 57

1. **Add Round Key**

| Input | K0 | Output |
| --- | --- | --- |
| 39 6C 20 39  69 2E 26 61  33 27 24 6E  61 37 32 57 | 4D 59 20 4E  41 4D 45 20  49 53 20 4E  75 6D 61 6E | 74 35 00 77  28 63 63 41  7A 74 04 20  14 5A 53 39 |

1. **Round 1**
   1. **After Substitute Bytes =**

**4A E9 63 F2**

**D4 8F 8F 35**

**C2 D4 09 23**

**B6 29 76 25**

* 1. **After Shift Rows =**

**4A E9 63 F2**

**8F 8F 35 D4**

**09 23 C2 D4**

**25 B6 29 76**

* 1. **After Mix Columns Matrix Multiplication =**

**BD A4 96 F3**

**AF 6C 25 5B**

**8B 6D 13 3F**

**41 34 79 D0**

* 1. **Add Round Key**

| Input | K1 | Output |
| --- | --- | --- |
| **BD A4 96 F3**  **AF 6C 25 5B**  **8B 6D 13 3F**  **41 34 79 D0** | 41 68 6D 41  64 66 5A 7A  6D 45 5A 4A  72 77 6F 51 | **FC C0 FB 81**  **C9 00 7F 21**  **E6 28 49 75**  **33 43 16 81** |

1. **Round 2**
   1. **After Substitute Bytes =**

**9A 51 A0 43**

**A7 63 E5 92**

**D7 18 B7 EA**

**D0 E1 7A A2**

* 1. **After Shift Rows =**

**9A 51 A0 43**

**63 E5 92 A7**

**B7 EA D7 18**

**A2 D0 E1 7A**

* 1. **Add Round Key**

| Input | K2 | Output |
| --- | --- | --- |
| **9A 51 A0 43**  **63 E5 92 A7**  **B7 EA D7 18**  **A2 D0 E1 7A** | 1D 84 45 0B  C4 C2 95 D0  8B 10 8B D9  68 AD C3 0E | **87 95 E5 48**  **A1 27 07 77**  **3C FA 5C C1**  **CA 7D 22 74** |

**Result**

| Block 1 | Block 2 |
| --- | --- |
| ISLAMABADISTHECA | PITALOFPAKISTAN. |
| 73 C6 25 11  E2 4D FF 12  5D 42 3B BE  E0 F1 1B 25 | 87 95 E5 48  A1 27 07 77  3C FA 5C C1  CA 7D 22 74 |

## Decryption

## Block 1

**Cipher Text** =

73 C6 25 11

E2 4D FF 12

5D 42 3B BE

E0 F1 1B 25

1. Add Round key (K2)

| Input | K2 | Output |
| --- | --- | --- |
| 73 C6 25 11  E2 4D FF 12  5D 42 3B BE  E0 F1 1B 25 | 1D 84 45 0B  C4 C2 95 D0  8B 10 8B D9  68 AD C3 0E | 6E 02 60 1A  20 D8 74 CB  35 EF F8 B0  FD 35 0B AE |

1. **Round 1**
   1. **After Inverse Shift Row =**

**6E 02 60 1A**

**CB 20 D8 74**

**F8 B0 35 EF**

**AE FD 35 0B**

* 1. **After Inverse Sub Bytes =**

**3A 45 D4 5B**

**C2 92 3C F1**

**E4 7D 3F 2E**

**16 7F 3F 86**

* 1. **After Inverse Mix Column =**

**BE D4 54 E9**

**E9 9A 17 8A**

**6B 9B C7 7D**

**F1 E5 64 58**

* 1. **After Add Round Key =**

| Input | K1 | Output |
| --- | --- | --- |
| **BE D4 54 E9**  **E9 9A 17 8A**  **6B 9B C7 7D**  **F1 E5 64 58** | 41 68 6D 41  64 66 5A 7A  6D 45 5A 4A  72 77 6F 51 | **FF B0 39 A8**  **8D FC 4D F0**  **06 DE 9D 37**  **83 92 0B 09** |

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

**FF B0 39 A8**

**F0 8D FC 4D**

**9D 37 06 DE**

**09 83 92 0B**

* 1. **After Inverse Sub Bytes =**

**16 A4 22 53**

**07 8A E0 8F**

**E1 34 91 2C**

**6C C2 99 8C**

* 1. **Add Round Key**

| Input | K0 | Output |
| --- | --- | --- |
| 16 A4 22 53  07 8A E0 8F  E1 34 91 2C  6C C2 99 8C | 4D 59 20 4E  41 4D 45 20  49 53 20 4E  75 6D 61 6E | 39 6C 20 39  69 2E 26 61  33 27 24 6E  61 37 32 57 |

**XOR with IV:**

**20 6D 25 25**

**73 20 24 65**

**2B 23 3E 63**

**61 26 35 38**

| Result | Plain Text |
| --- | --- |
| 49 4D 44 48  53 41 49 1C  42 43 59 02  41 41 54 41 | I M D H  S A I E  L B S C  A A T A |

Plain Test = I S L A M A B A D I S T H E C A

## Block 2

**Cipher Text** =

87 95 E5 48

A1 27 07 77

3C FA 5C C1

CA 7D 22 74

1. **Add Round Key**

| Input | K2 | Output |
| --- | --- | --- |
| 87 95 E5 48  A1 27 07 77  3C FA 5C C1  CA 7D 22 74 | 1D 84 45 0B  C4 C2 95 D0  8B 10 8B D9  68 AD C3 0E | 9A 11 A0 43  65 E5 92 A7  B7 EA D7 18  A2 D0 E1 7A |

1. **Round 1**
   1. **After Inverse Shift Row =**

**9A 11 A0 43**

**A7 65 E5 92**

**D7 18 B7 EA**

**7A A2 D0 E1**

* 1. **After Inverse Sub Bytes =**

**CF FD 00 4D**

**C5 30 0D 8F**

**A9 B4 2C 27**

**5C 96 7E 73**

* 1. **After Inverse Mix Column =**

**47 29 E0 C3**

**01 60 D1 A5**

**9A 95 50 91**

**81 E7 4D 6C**

* 1. **Add Round Key**

| Input | K1 | Output |
| --- | --- | --- |
| 47 29 E0 C3  01 60 D1 A5  9A 95 50 91  81 E7 4D 6C | 41 68 6D 41  64 66 5A 7A  6D 45 5A 4A  72 77 6F 51 | 06 41 8D 82  65 06 8B DF  F7 D0 0A DB  F3 90 22 3D |

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

**06 41 8D 82**

**DF 65 06 8B**

**0A DB F7 D0**

**3D F3 90 22**

* 1. **After Inverse Sub Bytes =**

**C5 E9 56 E2**

**A4 86 C5 0D**

**B8 21 1C BC**

**15 A3 4E 36**

* 1. **Add Round Key**

| Input | K0 | Output |
| --- | --- | --- |
| C5 E9 56 E2  A4 86 C5 0D  B8 21 1C BC  15 A3 4E 36 | 4D 59 20 4E  41 4D 45 20  49 53 20 4E  75 6D 61 6E | 39 6C 20 39  69 2E 26 61  33 27 24 6E  61 37 32 57 |

**XOR with IV:**

**50 4C 41 54**

**49 4F 4B 41**

**54 46 49 4E**

**08 17 53 3A**

**Result**

| Block 1 | Block 2 |
| --- | --- |
| 49 4D 44 48  53 41 49 1C  42 43 59 02  41 41 54 41 | 50 4C 41 54  49 4F 4B 41  54 46 49 4E  08 17 53 3A |
| ISLAMABADISTHECA | PITALOFPAKISTAN. |