**Information Security Assignment**



**Session: 2021**

**Submitted by:**

**Farjad Waseem 2021-SE-56**

**Submitted to:**

**Ma’am Anam Iftikhar**

Department of Computer Science,

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

***DES***

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

A diagram of a block chain

Description automatically generated***Figures:***

Here,

Block Cipher : **DES**

***A diagram of a flowchart

Description automatically generatedNote:*** Only 2 rounds as per requirement.

A diagram of a computer program

Description automatically generated

A table with numbers and letters

Description automatically generated

A table of mathematical equations

Description automatically generated with medium confidence

***Encryption***

NAME key in text form: FARJADWASEEM

IV in text form: MYVECTOR

plaintext in text form: LAHOREISABIGCITY

***Block1***

Plaintext: LAHOREIS

Key: FARJADWA

IV: MYVECTOR

Key Scheduling:

Key in 64 bit:01000110 01000001 01010010 01001010 01000001 01000100 01010111 01000001

**PC-1:**

Key after PC-1: 00000000 11111111 00000000 01000100 11010110 00010000 10000100

Spliting Into C0 and D0

C0:00000000 11111111 00000000 0100

D0:01001101 01100001 00001000 0100

Left Shift by 1 Bit

C1:00000001 11111110 00000000 1000

D1:10011010 11000010 00010000 1000

Again Left Shift by 1 Bit

C2: 00000011 11111100 00000001 0000

D2:00110101 10000100 00100001 0001

Concatenating C1 and D1

C1D1:00000001 11111110 00000000 10001001 10101100 00100001 00001000

Concatenating C2 and D2

C2D2:00000011 11111100 00000001 00000011 01011000 01000010 00010001

**PC-2:**

After Appling PC-2

*K1: 101000001001001001000010000100000011000001000011*

*K2: 101100000001001001010010011110000000000110010101*

**Encryption:**

IV in 64 bit:01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

Plaintext in 64 bit:01001100 01000001 01001000 01001111 01010010 01000101 01001001 01010011

IV XOR PlainText: 0000000100011000000111100000101000010001000100010000011000000001

**After Initial Permutation:** 0000000000110110010001001011000100000000000000000000111001001100

Now Split this into L0 and R0 each of 32 bits

L0:00000000 00110110 01000100 10110001

R0:00000000 00000000 00001110 01001100

***Round1***

L1:00000000 00000000 00001110 01001100

R1 = L0 XOR F(R0, K1)

F(R0, K1) :

E(R0) in 48 bits: 00000000 00000000 00000000 00000101 11000010 01011000

K1 XOR E(R0): 10100000 10010010 01000010 00010101 11110010 00011011

After Appling S-Boxes on Each Block

S(K1 XOR E(R0)): 11011111001111010010100011111110

Now Applying P-BOX

F(R0,K1): 11011110100110101101010011110111

R1:11011110 10101100 10010000 01000110

***Round2***

L2:11011110 10101100 10010000 01000110

R2 = L1 XOR F(R1, K2)

F(R1, K2) :

E(R1) in 48 bits: 01101111 11010101 01011001 01001010 00000010 00001101

K2 XOR E(R1): 11011111 11000111 00001011 00110010 00000011 10011000

After Appling S-Boxes on Each Block

S(K2 XOR E(R1)): 11100010001011111011100111010101

Now Applying P-BOX

F(R1,K2): 11110011110100001011101011100101

R2:11110011 11010000 10110100 10101001

***Swapping***

Swap and Concatenating R2L2 :11110011 11010000 10110100 10101001 11011110 10101100 10010000 01000110

**After Inverse Initial Pemutation:**

CipherText: 01000001 11000010 10100110 10100001 11011100 01100101 11010010 11111101

***Block2***

PlainText: ABIGCITY

Key: FARJADWA

IV: MYVECTOR

Key Scheduling:

Key in 64 bit:01000110 01000001 01010010 01001010 01000001 01000100 01010111 01000001

**PC-1:**

Key after PC-1:00000000 11111111 00000000 01000100 11010110 00010000 10000100

Spliting Into C0 and D0

C0:00000000 11111111 00000000 0100

D0:01001101 01100001 00001000 0100

Left Shift by 1 Bit

C1:00000001 11111110 00000000 1000

D1:10011010 11000010 00010000 1000

Again Left Shift by 1 Bit

C2:00000011 11111100 00000001 0000

D2:00110101 10000100 00100001 0001

Concatenating C1 and D1

C1D1:00000001 11111110 00000000 10001001 10101100 00100001 00001000

Concatenating C2 and D2

C2D2:00000011 11111100 00000001 00000011 01011000 01000010 00010001

**PC-2:**

After Appling PC-2

K1: 101000001001001001000010000100000011000001000011

K2: 101100000001001001010010011110000000000110010101

**Encryption:**

IV in 64 bit:01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

Plaintext in 64 bit:01000001 01000010 01001001 01000111 01000011 01001001 01010100 01011001

IV XOR PlainText: 0000110000011011000111110000001000000000000111010001101100001011

**Initial Permutation:**

0000000001100110001001011110011000000000000000001110011111001110

Now Split this into L0 and R0 each of 32 bits

L0:00000000 01100110 00100101 11100110

R0:00000000 00000000 11100111 11001110

***Round1***

L1:00000000 00000000 11100111 11001110

R1 = L0 XOR F(R0, K1)

F(R0, K1) :

E(R0) in 48 bits: 00000000 00000000 00000001 01110000 11111110 01011100

K1 XOR E(R0): 10100000 10010010 01000011 01100000 11001110 00011111

After Appling S-Boxes on Each Block

S(K1 XOR E(R0)): 11011111001110001101011000000010

Now Applying P-BOX

F(R0,K1): 01100101101011101100000001011110

R1:01100101 11001000 11100101 10111000

***Round2***

L2:01100101 11001000 11100101 10111000

R2 = L1 XOR F(R1, K2)

F(R1, K2) :

E(R1) in 48 bits: 00110000 10111110 01010001 01110000 10111101 11110000

K2 XOR E(R1): 10000000 10101100 00000011 00001000 10111100 01100101

After Appling S-Boxes on Each Block

S(K2 XOR E(R1)): 01001011101110001100110010011110

Now Applying P-BOX

F(R1,K2): 01011111000011101100000101101101

R2:01011111 00001110 00100110 10100011

***Swapping***

Swap and Concatenating R2L2 :01011111 00001110 00100110 10100011 01100101 11001000 11100101 10111000

**Inverse Initial Permutation:**

CipherText: 11001001 01010101 11011100 01110010 01000010 10001111 11101000 00101011

***Final Result***

CipherText**: 01000001 11000010 10100110 10100001 11011100 01100101 11010010 11111101 11001001 01010101 11011100 01110010 01000010 10001111 11101000 00101011**

***Decryption***

key in text form: FARJADWA

IV in text form: MYVECTOR

64 bit ciphertext: 01000001 11000010 10100110 10100001 11011100 01100101 11010010 11111101 11001001 01010101 11011100 01110010 01000010 10001111 11101000 00101011

***Block1***

CipherText: 01000001 11000010 10100110 10100001 11011100 01100101 11010010 11111101

Key: FARJADWA

IV: MYVECTOR

Key Scheduling:

Key in 64 bit:01000110 01000001 01010010 01001010 01000001 01000100 01010111 01000001

**PC-1:**

Key after PC-1:00000000 11111111 00000000 01000100 11010110 00010000 10000100

Spliting Into C0 and D0

C0:00000000 11111111 00000000 0100

D0:01001101 01100001 00001000 0100

Left Shift by 1 Bit

C1:00000001 11111110 00000000 1000

D1:10011010 11000010 00010000 1000

Again Left Shift by 1 Bit

C2:00000011 11111100 00000001 0000

D2:00110101 10000100 00100001 0001

Concatenating C1 and D1

C1D1:00000001 11111110 00000000 10001001 10101100 00100001 00001000

Concatenating C2 and D2

C2D2:00000011 11111100 00000001 00000011 01011000 01000010 00010001

**PC-2:**

After Appling PC-2

K1: 101000001001001001000010000100000011000001000011

K2: 101100000001001001010010011110000000000110010101

**Decryption:**

After Initial Permutation: 11110011 11010000 10110100 10101001 11011110 10101100 10010000 01000110

Now Split this into L0 and R0 each of 32 bits

L0:11110011 11010000 10110100 10101001

R0:11011110 10101100 10010000 01000110

***Round1***

L1:11011110 10101100 10010000 01000110

R1 = L0 XOR F(R0, K2)

F(R0, K2) :

E(R0) in 48 bits: 01101111 11010101 01011001 01001010 00000010 00001101

K2 XOR E(R0): 11011111 11000111 00001011 00110010 00000011 10011000

After Appling S-Boxes on Each Block

S(K2 XOR E(R0)): 11100010001011111011100111010101

Now Applying P-BOX

F(R0,K2): 11110011110100001011101011100101

R1:00000000 00000000 00001110 01001100

***Round2***

L2:00000000 00000000 00001110 01001100

R2 = L1 XOR F(R1, K1)

F(R1, K1) :

E(R1) in 48 bits: 00000000 00000000 00000000 00000101 11000010 01011000

K1 XOR E(R1): 10100000 10010010 01000010 00010101 11110010 00011011

After Appling S-Boxes on Each Block

S(K1 XOR E(R1)): 11011111001111010010100011111110

Now Applying P-BOX

F(R1,K1): 11011110100110101101010011110111

R2:00000000 00110110 01000100 10110001

***Swapping***

Swap and Concatenating R2L2: 00000000 00110110 01000100 10110001 00000000 00000000 00001110 01001100

**After Inverse Initial Permutation:** 00000001 00011000 00011110 00001010 00010001 00010001 00000110 00000001

IV in 64 bit:01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

IV XOR FinalData: 0100110001000001010010000100111101010010010001010100100101010011

PlainText:LAHOREIS

***Block2***

key in text form: FARJADWA

IV in text form: MYVECTOR

64 bit ciphertext: 11001001 01010101 11011100 01110010 01000010 10001111 11101000 00101011

CipherText: 11001001 01010101 11011100 01110010 01000010 10001111 11101000 00101011

Key Scheduling:

Key in 64 bit:01000110 01000001 01010010 01001010 01000001 01000100 01010111 01000001

**PC-1:**

Key after PC-1:00000000 11111111 00000000 01000100 11010110 00010000 10000100

Spliting Into C0 and D0

C0:00000000 11111111 00000000 0100

D0:01001101 01100001 00001000 0100

Left Shift by 1 Bit

C1:00000001 11111110 00000000 1000

D1:10011010 11000010 00010000 1000

Again Left Shift by 1 Bit

C2:00000011 11111100 00000001 0000

D2:00110101 10000100 00100001 0001

Concatenating C1 and D1

C1D1:00000001 11111110 00000000 10001001 10101100 00100001 00001000

Concatenating C2 and D2

C2D2:00000011 11111100 00000001 00000011 01011000 01000010 00010001

**PC-2:**

After Appling PC-2

K1: 101000001001001001000010000100000011000001000011

K2: 101100000001001001010010011110000000000110010101

**Decryption:**

**After Initial Permutation:** 01011111 00001110 00100110 10100011 01100101 11001000 11100101 10111000

Now Split this into L0 and R0 each of 32 bits

L0:01011111 00001110 00100110 10100011

R0:01100101 11001000 11100101 10111000

***Round1***

L1:01100101 11001000 11100101 10111000

R1 = L0 XOR F(R0, K2)

F(R0, K2) :

E(R0) in 48 bits: 00110000 10111110 01010001 01110000 10111101 11110000

K2 XOR E(R0): 10000000 10101100 00000011 00001000 10111100 01100101

After Appling S-Boxes on Each Block

S(K2 XOR E(R0)): 01001011101110001100110010011110

Now Applying P-BOX

F(R0,K2): 01011111000011101100000101101101

R1:00000000 00000000 11100111 11001110

***Round2***

L2:00000000 00000000 11100111 11001110

R2 = L1 XOR F(R1, K1)

F(R1, K1) :

E(R1) in 48 bits: 00000000 00000000 00000001 01110000 11111110 01011100

K1 XOR E(R1): 10100000 10010010 01000011 01100000 11001110 00011111

After Appling S-Boxes on Each Block

S(K1 XOR E(R1)): 11011111001110001101011000000010

Now Applying P-BOX

F(R1,K1): 01100101101011101100000001011110

R2:00000000 01100110 00100101 11100110

***Swapping***

Swap and Concatenating R2L2: 00000000 01100110 00100101 11100110 00000000 00000000 11100111 11001110

**After Inverse Initial Permutation:** 00001100 00011011 00011111 00000010 00000000 00011101 00011011 00001011

IV in 64 bit:01001101 01011001 01010110 01000101 01000011 01010100 01001111 01010010

IV XOR FinalData: 0100000101000010010010010100011101000011010010010101010001011001

PlainText:ABIGCITY

***Final Result***

PlainText**: LAHOREISABIGCITY**

***AES***

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

***Encryption***

1. Plain Text: ISLAMABADISTHECAPITALOFPAKISTAN.
2. Block Size: 128 bits
3. Number of Rounds: 2
4. Algorithm: AES key scheduling algorithm to generate 2 round keys.
5. Mode of Operation: Cipher Block Chaining (CBC).
6. Plain Text: ISLAMABADISTHECAPITALOFPAKISTAN.
7. Plain Text Hex:

49 53 4C 41

4D 41 42 41

44 20 49 53

20 54 48 45

1. IV For the process:

00 11 22 33

44 55 66 77

88 99 AA BB

CC DD EE FF

1. Key: MY NAME IS FARJADWA

**Key Scheduling Algorithm**

K0 =

4D 59 20 4E

41 4D 45 20

49 53 20 46

41 52 4A 44

K1 =

4D 41 4C 49

4B 20 49 53

20 54 48 45

20 43 41 50

K2 =

1D 84 45 0B

C4 C2 95 D0

8B 10 8B D9

68 AD C3 0E

***Block1***

**Step 1:** Convert the plaintext into a 4x4 matrix

- Plain Text Matrix (First Block):

49 53 4C 41

4D 41 42 41

44 20 49 53

20 54 48 45

**Step 2:** Perform XOR operation between PT matrix and IV matrix

- Result of XOR operation:

|  |  |  |
| --- | --- | --- |
| 49 53 4C 41 |  | 00 11 22 33 |
| 4D 41 42 41 | ⊕ | 44 55 66 77 |
| 44 20 49 53 |  | 88 99 AA BB |
| 20 54 48 45 |  | CC DD EE FF |

49 42 6E 72

09 14 24 36

5C F9 E9 68

CC 99 A6 76

**Step 3:** Apply AES encryption for 2 rounds

***Round1***

**1. Add Round Key (XOR with Round 0 key):**

- Key:

4D 59 20 4E

41 4D 45 20

49 53 20 46

41 52 4A 44

- Result of XOR:

1D 1A 6E 28

48 5B 69 16

15 AE C9 29

80 DD E6 39

**2. Substitute Bytes (S-Box):**

- Result:

63 4F 2D C5

D1 99 7B A4

0C 66 41 78

21 31 6A 0B

**3. Shift Rows:**

- Result:

63 99 41 0B

D1 66 6A C5

0C 31 7B 78

21 4F 2D A4

**4. Mix Columns:**

|  |  |  |
| --- | --- | --- |
| 02 03 01 01 |  | 63 99 41 0B |
| 01 02 03 01 | x | D1 66 6A C5 |
| 01 01 02 03 |  | 0C 31 7B 78 |
| 03 01 01 02 |  | 21 4F 2D A4 |

***Round2***

**1. Add Round Key (XOR with Round 0 key):**

- Key:

4D 41 4C 49

4B 20 49 53

20 54 48 45

20 43 41 50

- Result of XOR:

CC C8 0F 1A

F2 4F 60 85

49 8D 09 31

7B 8A 69 6F

**2. Substitute Bytes (S-Box):**

- Result:

84 A7 A2 26

A6 2D 88 4F

9B 51 52 58

6D 0F 60 9D

**3. Shift Rows:**

- Result:

84 2D 60 9D

A6 0F 52 26

9B A7 88 4F

6D 51 A2 58

**4. Mix Columns(**Not Applied in the last round**)**

**Final Encrypted Result** :

* for the first block (Hexadecimal):

73 C6 25 11

E2 4D FF 12

5D 42 3B BE

E0 F1 1B 25

***Block2***

**Step 1:** Convert the plaintext into a 4x4 matrix

- Plain Text Matrix (First Block):

50 49 54 41

4C 20 4F 46

20 50 41 4B

49 53 54 41

**Step 2:** Perform XOR operation between PT matrix and IV matrix

- Result of XOR operation:

|  |  |  |
| --- | --- | --- |
| 50 49 54 41 |  | 00 11 22 33 |
| 4C 20 4F 46 | ⊕ | 44 55 66 77 |
| 20 50 41 4B |  | 88 99 AA BB |
| 49 53 54 41 |  | CC DD EE FF |

* **Result:**

50 58 76 72

10 75 2F 31

A0 F9 EB B8

88 CC BA BE

**Step 3:** Apply AES encryption for 2 rounds

***Round1***

**1. Add Round Key (XOR with Round 0 key):**

- Key:

4D 41 4C 49

4B 20 49 53

20 54 48 45

20 43 41 50

- Result of XOR:

1D 1A 6E 28

48 5B 69 16

15 AE C9 29

80 DD E6 39

**2. Substitute Bytes (S-Box):**

- Result:

63 4F 2D C5

D1 99 7B A4

0C 66 41 78

21 31 6A 0B

**3. Shift Rows:**

- Result:

63 99 41 0B

D1 66 6A C5

0C 31 7B 78

21 4F 2D A4

**4. Mix Columns:**

|  |  |  |
| --- | --- | --- |
| 02 03 01 01 |  | 63 99 41 0B |
| 01 02 03 01 | x | D1 66 6A C5 |
| 01 01 02 03 |  | 0C 31 7B 78 |
| 03 01 01 02 |  | 21 4F 2D A4 |

* Result

BD A4 96 F3

AF 6C 25 5B

8B 6D 13 3F

41 34 79 D0

***Round2***

1. **Add Round Key (XOR with Round 0 key):**

- Key:

4D 41 4C 49

4B 20 49 53

20 54 48 45

20 43 41 50

- Result of XOR:

CC C8 0F 1A

F2 4F 60 85

49 8D 09 31

7B 8A 69 6F

**2. Substitute Bytes (S-Box):**

- Result:

84 A7 A2 26

A6 2D 88 4F

9B 51 52 58

6D 0F 60 9D

**3. Shift Rows:**

- Result:

84 2D 60 9D

A6 0F 52 26

9B A7 88 4F

6D 51 A2 58

**4. Mix Columns(**Not Applied in the last round**)**

**Final Encrypted Result** :

* for the first block (Hexadecimal):

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***

***Block1***

**Step 1:** Convert the plaintext into a 4x4 matrix

- **Cipher Text** =

73 C6 25 11

E2 4D FF 12

5D 42 3B BE

E0 F1 1B 25

**Step 2:** Add Round Key 2

- Result of XOR operation:

|  |  |  |
| --- | --- | --- |
| Input |  | K2 |
| 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

***Round1***

* + **After Inverse Shift Row =**

6E 02 60 1A

CB 20 D8 74

F8 B0 35 EF

AE FD 35 0B

* + **After Inverse Sub Bytes =**

3A 45 D4 5B

C2 92 3C F1

E4 7D 3F 2E

16 7F 3F 86

* + **After Inverse Mix Column =**

BE D4 54 E9

E9 9A 17 8A

6B 9B C7 7D

F1 E5 64 58

* + **After Add Round Key =**

|  |  |  |
| --- | --- | --- |
| Input |  | K1 |
| **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 |

* **Result**

FF B0 39 A8

8D FC 4D F0

06 DE 9D 37

83 92 0B 09

***Round2***

* + **Inverse Shift Row =**

FF B0 39 A8

F0 8D FC 4D

9D 37 06 DE

09 83 92 0B

* + **After Inverse Sub Bytes =**

16 A4 22 53

07 8A E0 8F

E1 34 91 2C

6C C2 99 8C

* + **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input |  | K0 |
| 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 |

* **Result:**

39 6C 20 39

69 2E 26 61

33 27 24 6E

61 37 32 57

**XOR with IV:**

49 4D 44 48

53 41 49 1C

42 43 59 02

41 41 54 41

|  |  |
| --- | --- |
| 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 |

* **Result:**

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

***Block2***

**Step 1:** Convert the plaintext into a 4x4 matrix

- **Cipher Text** =

87 95 E5 48

A1 27 07 77

3C FA 5C C1

CA 7D 22 74

**Step 2:** Add Round Key 2

- Result of XOR operation:

|  |  |  |
| --- | --- | --- |
| Input |  | K2 |
| 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

***Round1***

* + **Inverse Shift Row =**

9A 11 A0 43

A7 65 E5 92

D7 18 B7 EA

7A A2 D0 E1

* + **Inverse Sub Bytes =**

CF FD 00 4D

C5 30 0D 8F

A9 B4 2C 27

5C 96 7E 73

* + **Inverse Mix Column =**

47 29 E0 C3

01 60 D1 A5

9A 95 50 91

81 E7 4D 6C

* + **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input |  | K1 |
| 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 |

* **Result:**

06 41 8D 82

65 06 8B DF

F7 D0 0A DB

***Round2***

* + **Inverse Shift Row =**

06 41 8D 82

DF 65 06 8B

0A DB F7 D0

3D F3 90 22

* + **Inverse Sub Bytes =**

C5 E9 56 E2

A4 86 C5 0D

B8 21 1C BC

15 A3 4E 36

* + **Add Round Key**

|  |  |  |
| --- | --- | --- |
| Input |  | K1 |
| 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 |

* **Result:**

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. |

***The End***