

**WOLDIA UNIVERSITY**

**FACULTY OF TECHNOLOGY**

**DEPARTMENT OF SOFTWARE ENGINEERING**

**Computer Security Individual Assignment on Cryptography and Encryption Techniques**

**Using DES Encryption Techniques.**

**Name: SULEYMAN ABDU ID: 147312**

**Submitted to: Instructor DANIEL TEFERA**

**MAY 2, 2024**

**Woldia, Ethiopia**

Plain Text (M) =SULEYMAN

Cipher Text =?

Let us change the alphabet in to binary

* S: 01010011
* U: 01010101
* L: 01001100
* E: 01000101
* Y: 01011001
* M: 01001101
* A: 01000001
* N: 01001110

Binary Version of plain text (M) =01010011 01010101 01001100 01000101 01011001 01001101 01000001 01001110

L= 01010011 01010101 01001100 01000101

R= 01011001 01001101 01000001 01001110

K =PASSPHRA

K(binary) = 0101 0000 01000001 01010011 01010011 01010000 01001000 01010010 01000001

Step 1: Create 16 sub keys, each of which is 48-bits long.

The 64-bit key K is permuted according to PC-1(given in the Hand out).

Here we get the 56-bit permutation.

K+ =00000000,11111111,000000000,101010,011,000000000000,100,000,1101

Next, split this key into left and right halves, C0 and D0, where each half has 28 bits.

C0=00000000,11111111,000000000,101

D0=010,011,000000000000,100,000,1101

* With C0 and D0 defined, we now create sixteen blocks Cn and Dn, 1<=n<=16.
* Each pair of blocks Cn and Dn is formed from the previous pair Cn-1 and Dn-1,

respectively, for n = 1, 2, ..., 16, (using the given schedule in the hand out) of "left shifts" of the previous block.

* C0=00000000,11111111,000000000,101

D0=010,011,000000000000,100,000,1101

* C1=0000000,11111111,000000000,1010

D1=10,011,000000000000,100,000,11010

* C2=000000,11111111,000000000,10100

D2=0,011,000000000000,100,000,110101

* C3=0000,11111111,000000000,1010000

D3=11,000000000000,100,000,11010100

* C4=00,11111111,000000000,101000000

D4=,000000000000,100,000,1101010011

* C5=,11111111,000000000,10100000000

D5=0000000000,100,000,110101001100

* C6=111111,000000000,1010000000011

D6=00000000,100,000,11010100110000

* C7=1111,000000000,101000000001111

D7=000000,100,000,1101010011000000

* C8=11,000000000,10100000000111111

D8=0000,100,000,110101001100000000

* C9=1,000000000,101000000001111111

D9=000,100,000,1101010011000000000

* C10=00000000,10100000000111111110

D10=0,100,000,110101001100000000000

* C11=000000,1010000000011111111000

D11=00,000,11010100110000000000001

* C12=0000,101000000001111111100000

D12=,000,1101010011000000000000100

* C13=00,10100000000111111110000000

D13=,0,110101001100000000000010000

* C14=,1010000000011111111000000000

D14=1010100110000000000001000001

* C15=1000000001111111100000000010

D15=1010011000000000000100000110

* C16=0000000011111111000000000101

D16=0100110000000000001000001101

We now form the keys Kn, for 1<=n<=16, by applying the following permutation table to each of the concatenated pairs CnDn. Each pair has 56 bits, but PC-2( given in the hand out) only uses 48 of these.

**C1D1**=0000000,11111111,000000000,1010 10,011,000000000000,100,000,11010

which, after we apply the permutation PC-2, becomes

K1=101000001001001001001010010001000010000001100011

For the other keys we have

K2=101100000001001011010010011000001100000100000001

K3=001101000101001001010000010000100000010000001010

K4=000001100101000101010100110011000001000100001000

K5=000011100100000101010101000000000101001001101000

K6=000011110100000100101001010100001001100000100000

K7=100010110000000110101001100000000000110000111000

K8=100110010000101010001001000010010011101000010000

K9=001110010000100010001010100010000000001000100001

K10=001100000010100010001100100100100100101000000100

K11=000100000010110000010100000100000000001110010000

K12=010001000010110000110100100100010010000000000001

K13=110001101010010000100100011000100010001000000000

K14=110010101000011000100010001100000010000100001110

K15=111010001001001000101010001001000001000010000010

K16=101000011001001010100010000010100010000111000000

So much for the sub keys.

Now we look at the message (PASSPHRA) itself.

Step 2: Encode each 64-bit block of data.

There is an initial permutation IP of the 64 bits of the message data SULEYMAN . This rearranges the bits according to the table given in the hand out, where the entries in the table show the new arrangement of the bits from their initial order. The 58th bit of M becomes the first bit of IP. The 50th bit of M becomes the second bit of IP. The 7th bit of M is the last bit of IP. IP is given in the handout

M=01010011 01010101 01001100 01000101 01011001 01001101 01000001 01001110

IP=11111111 00010011 10101110 01111011 00000000 00000000 10110100 10000001

L0 =11111111 00010011 10101110 01111011

R0 = 00000000 00000000 10110100 10000001

We now proceed through 16 iterations, for 1<=n<=16, using a function f which operates on two

blocks--a data block of 32 bits and a key Kn of 48 bits--to produce a block of 32 bits.

Let + denote XOR addition.

Then for n going from 1 to 16 we calculate Ln = Rn-1

Rn = Ln-1 + f (Rn-1,Kn) This results in a final block, for n = 16, of L16R16. That is, in each

iteration, we take the right 32 bits of the previous result and make them the left 32 bits of the

current step. For the right 32 bits in the current step, we XOR the left 32 bits of the previous step

with the calculation f .

To calculate f, we first expand each block Rn-1 from 32 bits to 48 bits. This is done by using a E

bit-selection table (given in the hand out) that repeats some of the bits in Rn-1. We'll call the use

of this selection table the function E. Thus E (Rn-1) has a 32 bit input block, and a 48 bit output

block.

Note that each block of 4 original bits has been expanded to a block of 6 output bits.

Next in the f calculation, we XOR the output E(Rn-1) with the key Kn:

 Kn + E(Rn-1).

For n = 1:

K1 =101000001001001001001010010001000010000001100011

L1 = R0 = 00000000 00000000 10110100 10000001

R1 = L0 + f (R0, K1) = ?

K1 = 101000 001001 001001 001010 010001 000010 000001 100011

E (R0) = 100000 000000 000000 000001 010110 101001 010000 000010

K1 + E (R0) = 001000 001001 001001 001011 000111 101011 010001 100001

Kn + E(Rn-1) =B1B2B3B4B5B6B7B8, where each Bi is a group of six bits. We now calculate S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) where Si(Bi) refers to the output of the i th S box (given in the hand out). The first and the last digit (in decimal) represent the row in the S table.

The middle four digit (in decimal) represents the column in the S table.

B1 =001000, row = 00 = 0, column = 0100 = 4, S1 (B1) = 2

B2 = 001001, row = 01 = 1, column = 0100 = 4, S2 (B2) = 15

B3 = 001001, row = 01 = 1, column = 0100 = 4, S3 (B3) = 3

B4 = 001011, row = 01 = 1, column = 0101= 5, S4 (B4) = 15

B5 = 000111, row = 01= 1, column = 0011 = 3, S5 (B5) = 12

B6 = 101011, row = 11 = 3, column = 0101 = 5, S6 (B6) = 5

B7 = 010001, row = 01 = 1, column = 1000 = 8, S7 (B7) = 14

B8 = 100001, row = 11= 3, column = 0000 = 0, S8 (B8) = 2

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 2 15 3 15 12 5 14 2 (in Hexa Decimal) = (in binary) 0010 1111 0011 1111 1100 0101 1110 0010

The final stage in the calculation of f is to do a permutation P table (given in the hand out) of the S-box output to obtain the final value of f :

f = P(S1(B1)S2(B2)...S8(B8))

f = 1100 0101 0101 1110 0111 0110 0101 1101

• R1 = L0 + f

L0 =11111111 00010011 10101110 01111011

f = 11000101 01011110 01110110 01011101

R1=00111010 01001101 11011000 00100110

• In the next round, we will have L2 = R1, which is the block we just calculated, and then we must calculate R2 =L1 + f(R1, K2), and so on for 16 rounds.

For n = 2:

L2 = R1 = 00111010 01001101 11011000 00100110

K2 = 101100 000001 001011 010010 011000 001100 000100 000001

*R2* =*L1 + f (R1, K2) = ?*

R1=00111010 01001101 11011000 00100110

K2=101100 000001 001011 010010 011000 001100 000100 000001

E (*R1*) =000111 110100 001001 011011 111011 110000 000100 001100

K2 + E (R1) =101011 110101 000010 001001 100011 111100 000000 001101

B1 = 101011 , row = 11 = 3, column = 0101= 5, S1 (B1) = **9**

B2 = 110101 , row = 11 = 3, column = **1010**= 10, S2 (B2) = **7**

B3 = 000010 , row = 00 = 0, column = **0001**= 1, S3 (B3) = **0**

B4 = 001001 , row = 01 = 1, column = **0100**= 4, S4 (B4) = **6**

B5 = 100011 , row = 11 = 3, column = **0001**= 1, S5 (B5) = **8**

B6 = 111100 , row = 10 = 2, column = **1110**= 14, S6 (B6) = **11**

B7 = 000000 , row = 00 = 0, column = **0000**= 0, S7 (B7) = **4**

B8 = 001101, row = 01 = 1, column = **0110**= 6, S8 (B8) = **7**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **9 7 0 6 8 11 4 7** (in Hexa Decimal) = 1001 0111 0000 0110 1000 1011 0100 0111 (in Binary).

***f*** = **P**(***S1(B1)S2(B2)...S8(B8)***)

***f*** = 01010001 11110010 01111000 00110010

R2 = L1 + f

***L1*** = 00000000 00000000 10110100 10000001

***f*** = 01010001 11110010 01111000 00110010

R2 = 01010001 11110010 11001100 10110011

For n = 3:

L3 = R2 = 01010001 11110010 11001100 10110011

***K3*** =001101000101001001010000010000100000010000001010

*R3* =*L2 + f (R2, K3) = ?*

***K3*** = 001101 000101 001001 010000 010000 100000 010000 001010

E (R2) = 101010 100011 111110 100101 011001 011001 010110 100110

***K3*** + E (R2)= 100111 100110 110111 110101 001001 111001 000110 101100

B1 = 100111 , row = 11 = 3, column = **0011**= 3, S1 (B1) = **2**

B2 = 100110 , row = 10 = 2, column = **0011**= 3, S2 (B2) = **11**

B3 = 110111 , row = 11= 3, column = **1011**= 11, S3 (B3) = **3**

B4 = 110101 , row = 11 = 3, column = **1010**= 10, S4 (B4) = **5**

B5 = 001001 , row = 01= 1, column = **0100**= 4, S5 (B5) = **4**

B6 = 111001 , row = 11= 3, column = **1100**= 12, S6 (B6) = **6**

B7 = 000110, row = 00 = 0, column = **0011**= 3, S7 (B7) = **14**

B8 = 101100, row = 10 = 2, column = **0110**= 6, S8 (B8) = **14**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** =  **2 11 3 5 4 6 14 14** (in Hexa Decimal) = 0010 1011 0011 0101 0100 0110 1110 1110 (in Binary).

***f*** = **P**(***S1(B1)S2(B2)...S8(B8)***)

***f =* 11001100 00111110 01010110 00101101**

R3 = L2 + f

L2 = 1000 1100 1001 0011 1111 1101 0000 1001

1000 1100 1001 0011 1111 1101 0000 1001

***f* = 1100 1100 0011 1110 0101 0110 0010 1101**

R3 = 0100 0000 1010 1101 1010 1011 0010 0100

For ***n*** = 4:

L4 = R3 = 0100 0000 1010 1101 1010 1011 0010 0100

K4=000001100101000101010100110011000001000100001000

R4 =L3 + f (R3, K4) = ?

K4= 000001 100101 000101 010100 110011 000001 000100 001000

E (R3) = 001000 000001 010101 011011 110101 010110 100100 001000

***K4*** + E (R3)= 001001 100100 010000 001111 000110 010111 100000 000000

B1 = 001001, row = 01= 1, column = **0100**= 4, S1 (B1) = **2**

B2 = 100100 , row = 10 = 2, column = **0010**= 2, S2 (B2) = **7**

B3 = 010000, row = 00 = 0, column = **1000**= 8, S3 (B3) = **1**

B4 = 001111, row = 01 = 1, column = **0111**= 7, S4 (B4) = **3**

B5 = 000110, row = 00 = 0, column = **0011**=2 , S5 (B5) = **4**

B6 = 010111, row = 01 = 1, column = **1011**= 11, S6 (B6) = **14**

B7 = 100000 , row = 10 = 2, column = **0000**= 0, S7 (B7) = **1**

B8 = 000000, row = 00 = 0, column = **0000**= 0, S8 (B8) = **13**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **2 7 1 3 4 14 1 13** (in Hexa Decimal)

= 0010 0111 0001 0011 0100 1110 0001 1101 (in Binary).

***f*** = **P**(***S1(B1)S2(B2)...S8(B8)***)

***f*** = 11011110 01100100 01001010 00111000

R4 = L3 + f

L3 =01010001 11110010 11001100 10110011

f =11011110 01100100 01001010 00111000

R4 = 10001111 10010110 10000110 10001011

For n = 5:

L5 = R4 = 10001111 10010110 10000110 10001011

K5=000011100100000101010101000000000101001001101000

R5 =L4 + f (R4, K5) = ?

K5= 000011 100100 000101 010101 000000 000101 001001 101000

E (R4) = 110001 011111 110010 101101 010000 001101 010001 010111

K5 + E (R4) = 110010 111011 110111 101000 010000 001000 011000 111111

B1 = 110010, row = 10 = 2, column = **1001**= 9, S1 (B1) = **12**

B2 = 111011, row = 11 = 3, column = **1101**= 13, S2 (B2) = **5**

B3 = 110111, row = 11 = 3, column = **1011**= 11, S3 (B3) = **11**

B4 = 101000, row = 10 = 2, column = **0100**= 4 S4 (B4) = **12**

B5 = 010000, row = 00 = 0, column = **1000**= 8, S5 (B5) = **8**

B6 = 001000, row = 00 = 0, column = **0100**= 4, S6 (B6) = **9**

B7 = 011000, row = 00 = 0, column = **1100**= 12, S7 (B7) = **5**

B8 = 111111, row = 11 = 3, column = **1111**= 15, S8 (B8) = **11**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **12 5 11 12 8 9 5 11** (in Hexa Decimal)

= 1100 0101 1011 1100 1000 1001 0101 1011(in Binary).

f = P(S1(B1)S2(B2)...S8(B8))

f = 00011111 10010010 11111001 01010100

R5 = L4 + f

L4 = 0100 0000 1010 1101 1010 1011 0010 0100

f = 0001 1111 1001 0010 1111 1001 0101 0100

R5 = 0101 1111 0011 1111 0101 0010 0111 0000

For n = 6:

L6 = R5 = 0101 1111 0011 1111 0101 0010 0111 0000

K6 = 000011110100000100101001010100001001100000100000

R6 =L5 + f (R5, K6) = ?

K6 = 000011110100000100101001010100001001100000100000

E (R5) = 001011 111110 100111 111110 101010 100100 001110 100000

K6 + E (R5) =

B1 = 001011, row = 01= 1, column = **0101**= 5, S1 (B1) = **2**

B2 = 111110, row = 10 = 2, column = **1111**= 15, S2 (B2) = **15**

B3 = 100111, row = 11 = 3, column = **0011**= 3, S3 (B3) = **0**

B4 = 111110, row = 10 = 2, column = **1111**= 15, S4 (B4) = **4**

B5 = 101010, row = 10 = 2, column = **0101**= 5, S5 (B5) = **13**

B6 = 100100, row = 10 = 2, column = **0010**= 2, S6 (B6) = **15**

B7 = 001110, row = 00 = 0, column = **0111**= 7, S7 (B7) = **13**

B8 = 100000, row = 10 = 2, column = **0000**= 0, S8 (B8) = **7**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **2 15 0 4 13 15 13 7** (in Hexa Decimal)

= 0010 1111 0000 0100 1101 1111 1101 0111 (in Binary).

***f*** = **P** (***S1(B1)S2(B2)...S8(B8)***)

***f*** = 01110011 00111110 01111010 00111001

R6 = L5 + f

L5 = 10001111 10010110 10000110 10001011

f = 01110011 00111110 01111010 00111001

R6 = 11111100 10101000 11111100 10110010

For n = 7:

L7 = R6 = 11111100 10101000 11111100 10110010

K7=100010110000000110101001100000000000110000111000

R7 =L6 + f (R6, K7) = ?

K7= 100010 110000 000110 101001 100000 000000 110000 111000

E (R6) = 011111 111001 010101 010001 011111 111001 010110 100101

K7 + E (R6) = 111101 001001 010011 111000 111111 111001 100110 011101

B1 = 111101, row = 11 = 3, column = **1110**= 14, S1 (B1) = **6**

B2 = 001001 , row = 01 = 1, column = **0100**= 4, S2 (B2) = **15**

B3 = 010011, row = 01= 1, column = **1001**= 9, S3 (B3) = **8**

B4 = 111000, row = 10= 2, column = **1100**= 12, S4 (B4) =**5**

B5 = 111111, row = 11= 3, column = **1111**= 15, S5 (B5) = **3**

B6 = 111001, row = 11 = 3, column = **1100**= 12, S6 (B6) = **6**

B7 = 100110 , row = 10= 2, column = **0011**= 3, S7 (B7) = **13**

B8 = 011101, row = 01 = 1, column = **1110**= 14, S8 (B8) = **9**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **6 15 8 5 3 6 13 9** (in Hexa Decimal)

= 0110 1111 1000 0101 0011 0110 1101 1001 (in Binary).

***f*** = **P** (***S1(B1)S2(B2)...S8(B8)***)

***f*** = 11101010 00111000 11011011 10011001

R7 = L6 + f

L6 = 0101 1111 0011 1111 0101 0010 0111 0000

f = 1110 1010 0011 1000 1101 1011 1001 1001

R7 = 1011 0101 0000 0111 1000 1001 1110 1001

For n = 8:

L8 = R7 = 1011 0101 0000 0111 1000 1001 1110 1001

K8=100110010000101010001001000010010011101000010000

R8 =L7 + f (R7, K8) = ?

K8=100110 010000 101010 001001 000010 010011 101000 010000

E (R7) = 110110 101010 100000 001111 010001 010011 111101 010011

***K8*** + E (R7)= 010000 111010 001010 000110 010011 000000 010101 000011

B1 = 010000, row = 00 = 0, column = **1000**= 8, S1 (B1) = 8

B2 = 111010 , row = 10 = 2, column = **1101**= 13, S2 (B2) =3

B3 = 001010, row = 00 = 0, column = **0101**= 5, S3 (B3) = 3

B4 = 000110, row = 00 = 0, column = **0011**= 3, S4 (B4) = **3**

B5 = 010011, row = 01 = 1, column = **1001**= 9, S5 (B5) =  **0**

B6 = 000000, row = 00 = 0, column = **0000**= 0, S6 (B6) =  **12**

B7 = 010101, row = 01 = 1, column = **1010**= 10, S7 (B7) = 2

B8 = 000011, row = 01 = 1, column = **0001**= 1, S8 (B8) = 15

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **8 3 3 3 0 12 2 15** (in Hexa Decimal)

= 1000 0011 0011 0011 0000 1100 0010 1111 (in Binary).

***f*** = **P** (***S1(B1)S2(B2)...S8(B8)***)

***f*** = 11011100 11000010 01001100 00101100

R8 = L7 + f

L7 = 11111100 10101000 11111100 10110010

f = 11011100 11000010 01001100 00101100

R8 =00100000 01101010 10110000 10011110

**For n = 9:**

L9 = R8 = 00100000 01101010 10110000 10011110

K9=001110010000100010001010100010000000001000100001

R9 =L8 + f (R8, K9) = ?

K9 =00111001 00001000 10001010 10001000 00000010 00100001

E (R8) = 00010000 00000001 10101010 10101101 00001100 11111100

K9 + E (R8) = 001010 010000 100100 100000 001001 010000 111011 011101

B1 = 001010, row = 00 = 0, column = **0101**= 5, S1 (B1) = 15

B2 = 010000, row = 00 = 0, column = **1000**= 8, S2 (B2) =9

B3 = 100100, row = 10 = 2, column = **0010**= 2, S3 (B3) = 4

B4 = 100000 , row = 10 = 2, column = **0000**= 0, S4 (B4) = **10**

B5 = 001001, row = 01 = 1, column = **0100**= 4, S5 (B5) =  **4**

B6 = 010000, row = 00 = 0, column = **1000**= 8, S6 (B6) =  **0**

B7 = 111011, row = 11 = 3, column = **1101**= 13, S7 (B7) = 2

B8 = 011101, row = 01 = 1, column = **1110**= 14, S8 (B8) = 9

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **15 9 4 10 4 0 2 9** (in Hexa Decimal)

= 1111 1001 0100 1010 0100 0000 0010 1001 (in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 00001000 11001101 11001010 01000010

R9 = L8 + f

L8 = 1011 0101 0000 0111 1000 1001 1110 1001

f = 0000 1000 1100 1101 1100 1010 0100 0010

R9 = 1011 1101 1100 1010 0100 0011 1010 1011

For n = 10:

L10 = R9 = 1011 1101 1100 1010 0100 0011 1010 1011

K10=001100000010100010001100100100100100101000000100

R10 =L9 + f (R9, K10) = ?

K10= 001100 000010 100010 001100 100100 100100 101000 000100

E (R9) = 110111 111011 111001 010100 001000 000111 110101 010111

K10 + E (R9) = 111011 111001 011011 011000 101100 100011 011101 010011

B1 = 111011, row = 11= 3, column = **1101**= 13, S1 (B1) = 0

B2 = 111001, row = 11 = 3, column = **1100**= 12, S2 (B2) =0

B3 = 011011, row = 01 = 1, column = **1101**= 13, S3 (B3) = 11

B4 = 011000, row = 00 = 0, column = **1100**= 12, S4 (B4) = **11**

B5 = 101100, row = 10 = 2, column = **0110**= 6, S5 (B5) =  **7**

B6 = 100011 , row = 11 = 3, column = **0001**= 1, S6 (B6) =  **3**

B7 = 011101, row = 01 = 1, column = **1110**= 14, S7 (B7) = **8**

B8 = 010011, row = 01 = 1, column = **1001**= 9 , S8 (B8) = 5

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **0 0 11 11 7 3 8 5** (in Hexa Decimal)

= 0000 0000 1011 1011 0111 0011 1000 0101 (in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 00100100 01100100 00101001 11100101

R10 = L9 + f

L9 = 00100000 01101010 10110000 10011110

f = 00100100 01100100 00101001 11100101

R10 =00000100 00001110 10011001 01111011

For n = 11:

L11 = R10 =00000100 00001110 10011001 01111011

K11=000100000010110000010100000100000000001110010000

R11 =L10 + f (R10, K11) = ?

K11=000100 000010 110000 010100 000100 000000 001110 010000

E (R10) =100000 001000 000001 011101 010011 110010 101111 110110

K11 + E (R10) =100100 001010 110001 001001 010111 110010 100001 100110

B1 = 100100, row = 10 = 2, column = **0010**= 2, S1 (B1) = **14**

B2 = 001010, row = 00 = 0, column = **0101**= 5, S2 (B2) = **11**

B3 = 110001 , row = 11 = 3, column = **1000**= 8, S3 (B3) = **4**

B4 = 001001, row = 01 = 1, column = **0100**= 4, S4 (B4) = **6**

B5 = 010111, row = 01 = 1, column = **1011**= 11, S5 (B5) = **10**

B6 = 110010, row = 10 = 2, column = **1001**= 9, S6 (B6) = **0**

B7 = 100001, row = 11 = 3, column = **0100**= 4, S7 (B7) = **1**

B8 = 100110, row = 10 = 2, column = **0110**= 6, S8 (B8) = **14**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **14 11 4 6 10 0 1 14** (in Hexa Decimal) = 1110 1011 0100 0110 1010 0000 0001 1110 (in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 01001011 11001011 11010010 10100000

R11 = L10 + f

L10= 1011 1101 1100 1010 0100 0011 1010 1011

f = 0100 1011 1100 1011 1101 0010 1010 0000

R11 = 1111 0110 0000 0001 1001 0001 0000 1011

For n = 12:

L12 = R11 = 1111 0110 0000 0001 1001 0001 0000 1011

K12=010001000010110000110100100100010010000000000001

R12 =L11 + f (R11, K12) = ?

K12= 010001 000010 110000 110100 100100 010010 000000 000001

E (R11) = 111110 101100 000000 000011 110010 100010 100001 010111

K12 + E (R11) = 101111 101110 110000 110111 010110 110000 100001 010110

B1 = 101111, row = 11 = 3, column = **0111**= 7, S1 (B1) = **7**

B2 = 101110, row = 10 = 2, column = **0111**= 7, S2 (B2) = **1**

B3 = 110000, row = 10 = 2, column = **1000**= 8, S3 (B3) = **0**

B4 = 110111 , row = 11 = 3, column = **1011**= 11 S4 (B4) = **11**

B5 = 010110, row = 00 = 0, column = **1011**= 11, S5 (B5) = **13**

B6 = 110000, row = 10 = 2, column = **1000**= 8, S6 (B6) = **7**

B7 = 100001, row = 11 = 3, column = **0000**= 0, S7 (B7) = **6**

B8 = 010110, row = 00 = 0, column = **1011**= 11, S8 (B8) = **14**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **7 1 0 11 13 7 6 14**(in Hexa Decimal) =0111 0001 0000 1011 1101 0111 0110 1110 (in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 10101001 01110110 11100110 01101010

R12 = L11 + f

L11 = 00000100 00001110 10011001 01111011

f = 10101001 01110110 11100110 01101010

R12 = 10101101 01111000 01111111 00010001

For n = 13:

L13 = R12 = 10101101 01111000 01111111 00010001

K13=110001101010010000100100011000100010001000000000

R13 =L12 + f (R12, K13) = ?

K13=110001 101010 010000 100100 011000 100010 001000 000000

E (R12) =110101 011010 101111 110000 001111 111110 100010 100011

K13 + E (R12) =000100 110000 111111 010100 010111 011100 101010 100011

B1 = 000100, row = 00 = 0, column = **0010**= 2, S1 (B1) = **13**

B2 = 110000 , row = 10 = 2, column = **1000**= 8, S2 (B2) = **5**

B3 = 111111 , row = 11 = 3, column = **1111**= 15, S3 (B3) = **12**

B4 = 010100 , row = 00 = 0, column = **1010**= 10, S4 (B4) = **8**

B5 = 010111 , row = 01 = 1, column = **1011**= 11, S5 (B5) = **10**

B6 = 011100, row = 00 = 0, column = **1110**= 14, S6 (B6) = **5**

B7 = 101010, row = 10 = 2, column = **0101**= 9, S7 (B7) = **15**

B8 = 100011, row = 11 = 3, column = **0001**= 1, S8 (B8) = **1**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **13 5 12 8 10 5 15 1** (in Hexa Decimal) = 1101 0101 1100 1000 1010 0101 1111 0001 (in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 00000011 10010001 11101101 11011011

R13 = L12 + f

L12 = 1111 0110 0000 0001 1001 0001 0000 1011

f = 0000 0011 1001 0001 1110 1101 1101 1011

R13 = 1111 0101 1001 0000 0111 1100 1101 0000

For n = 14:

L14 = R13 = 1111 0101 1001 0000 0111 1100 1101 0000

K14=110010101000011000100010001100000010000100001110

R14 =L13 + f (R13, K14) =?

K14=110010 101000 011000 100010 001100 000010 000100 001110

E (R13) =011110 101011 110010 100000 001111 111001 011010 100001

K14 + E (R13) =101100 000011 101010 000010 000011 111011 011110 101111

B1 = 101100 , row = 10 = 2, column = **0110**= 6, S1 (B1) = **2**

B2 = 000011, row = 01 = 1, column = **0001**= 1, S2 (B2) = **13**

B3 = 101010, row = 10 = 2, column = **0101**= 5, S3 (B3) = **15**

B4 = 000010 , row = 00 = 0, column = **0001**= 1, S4 (B4) = **13**

B5 = 000011, row = 01 = 1, column = **0001**= 1, S5 (B5) = **11**

B6 = 111011, row = 11 = 3, column = **1101**= 13, S6 (B6) = **0**

B7 = 011110, row = 00 = 0, column = **1111**= 15, S7 (B7) = **1**

B8 = 101111, row = 11 = 3, column = **0111**= 7, S8 (B8) = **13**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **2 13 15 13 11 0 1 13** (in Hexa Decimal) =0010 1101 1111 1101 1011 0000 0001 1101(in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 10101111 00001001 01011011 11110100

R14 = L13 + f

L13 = 10101101 01111000 01111111 00010001

f = 10101111 00001001 01011011 11110100

R14 = 00000010 01110001 00100100 11100101

For n = 15:

L15 = R14 =00000010 01110001 00100100 11100101

K15=111010001001001000101010001001000001000010000010

R15 =L14 + f (R14, K15) =?

K15=111010 001001 001000 101010 001001 000001 000010 000010

E (R14)=100000 000100 001110 100010 100100 001001 011100 001010

K15 + E (R14) =011010 001101 000110 001000 101101 001000 011110 001000

B1 = 011010, row = 00= 0, column = **1101**= 13, S1 (B1) = **9**

B2 = 001101 , row = 01 = 1, column = **0110**= 6, S2 (B2) = **8**

B3 = 000110 , row = 00 = 0, column = **0011**= 3, S3 (B3) = **14**

B4 = 001000 , row = 00 = 0, column = **0100**= 4, S4 (B4) = **0**

B5 = 101101 , row = 11 = 3, column = **0110**= 6, S5 (B5) = **2**

B6 = 001000 , row = 00 = 0, column = **0100**= 4, S6 (B6) = **9**

B7 = 011110 , row = 00 = 0, column = **1111**= 15, S7 (B7) = **1**

B8 = 001000, row = 00 = 0, column = **0100**= 4, S8 (B8) = **6**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **9 8 14 0 2 9 1 6** (in Hexa Decimal) =

1001 1000 1110 0000 0010 1001 0001 0110 (in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 0001 0010 1100 1011 0010 0001 1010 0110

R15 = L14 + f

L14 =1111 0101 1001 0000 0111 1100 1101 0000

f =0001 0010 1100 1011 0010 0001 1010 0110

R15 =1110 0111 0101 1011 0101 1101 0111 0110

For n = 16:

L16 = R15 = 1110 0111 0101 1011 0101 1101 0111 0110

K16=101000011001001010100010000010100010000111000000

R16 =L15 + f (R15, K16) =?

K16 = 101000 011001 001010 100010 000010 100010 000111 000000

E (R15)= 011100 001110 101011 110100 101011 111010 101110 101101

K16 + E (R15) = 110100 010111 100001 010110 101001 011000 101001 101101

B1 = 110100, row = 10 = 2, column = **1010**= 10, S1 (B1) = **9**

B2 = 010111, row = 01 = 1, column = **1011**= 11, S2 (B2) = **10**

B3 = 100001, row = 11 = 3, column = **0000**= 0, S3 (B3) = **1**

B4 = 010110, row = 00 = 0, column = **1011**= 11, S4 (B4) = **5**

B5 = 101001, row = 11 = 3, column = **0100**= 4, S5 (B5) = **1**

B6 = 011000 , row = 00= 0, column = **1100**= 12, S6 (B6) = **14**

B7 = 101001 , row = 11 = 3, column = **0100**= 4, S7 (B7) = **1**

B8 = 101101, row = 11 = 3, column = **0110**= 6, S8 (B8) = **8**

***S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)*** = **9 10 1 5 1 14 1 8** (in Hexa Decimal)

=1001 1010 0001 0101 0001 1110 0001 1000 (in Binary).

f = P (S1(B1)S2(B2)...S8(B8))

f = 1111 1110 1010 1000 0001 0000 0000 1010

R16 = L15 + f

L15 = 00000010 01110001 00100100 11100101

f = 11111110 10101000 00010000 00001010

R16 = 11111100 11011001 00110100 11101111

We then ***reverse*** the order of the two blocks into the 64-bit block ***R16L16*** and apply a final permutation **IP-1** (given in the hand out):

***R16L16*** = **1111 1100 1101 1001 0011 0100 1110 1111** 1110 0111 0101 1011 0101 1101 0111 0110

***IP-1*** = 1011 1001 1010 0011 1100 1111 0111 1001 0111 1110 1100 0111 1111 1011 1101 0001

**BOOM!! BOOM!! BOOM!! BOOM!! BOOM!! BOOM!! BOOM!! BOOM!!**

Which is in hexadecimal format is

# = B9A3 FC79 7EF3 D

This is the encrypted form of **M** =SULEYMAN