WOLDIA UNIVERSITY

SCHOOL OF COMPUTING

DEPARTMENT OF SOFTWARE

INDIVIDUAL ASSIGNMENT on

Cryptography and Encryption Techniques:

Encrypting my name (the first 64 bit only) using DES Encryption Techniques.

COURSE NAME: fundamental of software security

COURSE CODE: SEng3071

NAME :NATNAEL ARGAW HABTE

ID NO:147000

Submitted to Mr. DANIEL TEFERA.

Submitted Date: 20/5/2024

Woldia, Ethio

Plain Text (M) = NATNELA(the first 64 bit)

Cipher Text =?

Binary Version of plain text (M) = 01001110 01000001 01010100 01001110 01000001 01000101 01001100 01000001

L = 01001110 01000001 01010100 01001110

R = 01000001 01000101 01001100 01000001

K=PASSPHRA

K(binary)=01010000010000010101001101010011010100000100100001010010010000010101 001101000101

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.

 PC-1: Permutation Choice 1

K(binary)=01010000010000010101001101010011010100000100100001010010010000010101 001101000101

K+=00000000111111110000000001010100110000000000001000001101

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

C0=0000000011111111000000000101

D0=0100110000000000001000001101

 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.

C1=0000000111111110000000001010

D1=1001100000000000010000011010

C1D1=0000000111111110000000001010,1001100000000000010000011010

C2=0000001111111100000000010100

D2=0011000000000000100000110101

C2D2=0000001111111100000000010100, 0011000000000000100000110101

C3=0000111111110000000001010000

D3=1100000000000010000011010100

C3D3=0000111111110000000001010000, 1100000000000010000011010100

C4=0011111111000000000101000000

D4=0000000000001000001101010011

C4D4=0011111111000000000101000000, 0000000000001000001101010011

C5=1111111100000000010100000000

D5=0000000000100000110101001100

C5D5=1111111100000000010100000000, 0000000000100000110101001100

C6=1111110000000001010000000011

D6=0000000010000011010100110000

C6D6=1111110000000001010000000011, 0000000010000011010100110000

C7=1111000000000101000000001111

D7=0000001000001101010011000000

C7D7=1111000000000101000000001111, 0000001000001101010011000000

C8=1100000000010100000000111111

D8=0000100000110101001100000000

C8D8=1100000000010100000000111111, 0000100000110101001100000000

C9=1000000000101000000001111111

D9=0001000001101010011000000000

C9D9=1000000000101000000001111111, 0001000001101010011000000000

C10=0000000010100000000111111110

D10=0100000110101001100000000000

C10D10=0000000010100000000111111110, 0100000110101001100000000000

C11=0000001010000000011111111000

D11=0000011010100110000000000001

C11D11=0000001010000000011111111000, 0000011010100110000000000001

C12=0000101000000001111111100000

D12=0001101010011000000000000100

C12D12=0000101000000001111111100000, 0001101010011000000000000100

C13=0010100000000111111110000000

D13=0110101001100000000000010000

C13D13=0010100000000111111110000000, 0110101001100000000000010000

C14=1010000000011111111000000000

D14=1010100110000000000001000001

C14D14=1010000000011111111000000000, 1010100110000000000001000001

C15=1000000001111111100000000010

D15=1010011000000000000100000110

C15D15=1000000001111111100000000010, 1010011000000000000100000110

C16=0000000011111111000000000101

D16=0100110000000000001000001101

C16D16=0000000011111111000000000101, 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.

Which after we apply the permutation PC-2, becomes

□ PC-2: Permutation Choice 2

K1=101000001001001001001010010001000010000001100011

K2=101100000001001011010010011000001100000100000001

K3=001101000101001001010000010000100000010000001010

K4=000001100101000101010100110011000001000100001000

K5=000011100100000101010101000000000101001001101000

K6=000011110100000100101001010100001001100000100000

K7=100010110000000110101001100000000000110000111000

K8=100110010000101010001001000010010011101000010000

K9=001110010000100010001010100010000000001000100001

K10=001100000001010001000110010010010010010100000000100

K11=000100000001011000000101000000100000000000001110010000

K12=0100010000010110000011010010010001001000000000000001

K13=110001101010010000100100011000100010001000000000

K14=110010101000011000100010001100000001000010000111 0

K15=111010001001001000101010001001000000100001000000010

K16=101000011001001010100010000010100010000111000000

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

There is an initial permutation IP of the 64 bits of the message data NATNAELA (the first

64 bit).

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 = 01001110 01000001 01010100 01001110 01000001 01000101 01001100 01000001

IP = 11111111 00000100 01101101 10110010 00000000 00000000 01001001 00001001

Next divide the permuted block IP into a left half L0 of 32 bits, and a right half R0 of 32 bits.

L0 = 11111111 00000100 01101101 10110010

R0 = 00000000 00000000 0100100100001001

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 01001001 00001001

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

K1 = 101000 001001 001001 001010 010001 000010 000001 100011

E (R0) = 100000 000000 000000 000000 001001 010010 100001 010010

K1 + E (R0) = 001000 001001 001001 001010 011000 010000 100000 110001

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) = 14

B3 = 001001, row = 01 = 1, column = 0100 = 4, S3 (B3) = 14

B4 = 001010, row = 00 = 0, column = 0101 = 5, S4 (B4) = 15

B5 = 011000, row = 00 = 0, column = 1100 = 12, S5 (B5) = 5

B6 = 010000, row = 00 = 0, column = 1000 = 8, S6 (B6) = 3

B7 = 100000, row = 10 = 2, column = 0000 = 0, S7 (B7) = 4

B8 = 110001, row = 11 = 3, column = 1000 = 8, S8 (B8) = 5

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 2 14 14 15 5 3 4 5 (in Hexa Decimal) =

0010 1110 1110 1111 0101 0011 0100 0101 (in binary)

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 = 11100000 01111101 00111011 01110100

 R1 = L0 + f

L0 = 11111111 00000100 01101101 10110010

f =   11100000 01111101 00111011 01110100

R1 = 00011111 01111001 01010110 11000110

 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 = 00011111 01111001 01010110 11000110

K2 = 011110 011010 111011 011001 110110 111100 100111 100101

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

K2 =   011110 011010 111011 011001 110110 111100 100111 100101

E (R1) = 000011 111110 101111 110010 101010 101101 011000 001100

K2 + E (R1) = 011101 100100 010100 101011 011100 010001 111111 101001

B1 = 011101, row = 01 = 1, column = 1110= 14, S1 (B1) = 3

B2 = 100100, row = 10 = 2, column = 0010= 2, S2 (B2) = 14

B3 = 010100, row = 00 = 0, column = 1010= 10, S3 (B3) = 6

B4 = 101011, row = 11 = 3, column = 0101= 5, S4 (B4) = 9

B5 = 011100, row = 00 = 0, column = 1110= 14, S5 (B5) = 0

B6 = 010001, row = 01 = 1, column = 1000= 8, S6 (B6) = 10

B7 = 111111, row = 11 = 3, column = 1111= 15, S7 (B7) = 13

B8 = 101001, row = 11 = 3, column = 0100= 4, S8 (B8) = 4

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 3 14 6 9 0 10 13 4 (in Hexa Decimal)

= 0011 1110 0110 1001 0000 1010 1101 0100(in Binary).

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

f = 1101 0010 0010 1001 0000 0010 0011 0111

⍰ R2 = L1 + f

L1= 0000 0000 0000 0000 0100 1001 0000 1001

f = 1101 0010 0010 1001 0000 0010 0011 0111

R2 = 1101 0010 0010 1001 0100 1011 0011 1110

For n = 3:

L3 = R2 = 1101 0010 0010 1001 0100 1011 0011 1110

K3 = 001101000101001001010000010000100000010000001010

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

K3 = 001101 000101 001001 010000 010000 100000 010000 001010

E (R2) = 011010 100100 000101 010010 101001 010110 100111 111101

K3 + E (R2) = 010111 100001 001101 000010 111001 110110 110111 110111

B1 = 010111, row = 01 = 1, column = 1011= 11, S1 (B1) = 11

B2 = 100001, row = 11 = 3, column = 0000= 0, S2 (B2) = 15

B3 = 001101, row = 01 = 1, column = 0110= 6, S3 (B3) = 13

B4 = 000010, row = 00 = 0, column = 0001= 1, S4 (B4) = 4

B5 = 111001, row = 11 = 3, column = 1100= 12, S5 (B5) = 10

B6 = 110110, row = 10 = 2, column = 1011= 11, S6 (B6) = 7

B7 = 110111, row = 11 = 3, column = 1011= 11, S7 (B7) = 14

B8 = 110111, row = 11 = 3, column = 1011= 11, S8 (B8) = 14

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 11 15 13 4 10 7 14 14 (in Hexa Decimal)

= 1011 1111 1101 0100 1010 0111 1110 1110 (in Binary).

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

f = 01001101101110110111011110111011

□ R3 = L2 + f

L2 = 00011111 01111001 01010110 11000110

f = 01001101101110110111011110111011

R3 = 0101 0010 1100 0010 0010 0001 0101 1101

For n = 4:

L4 = R3 = 0101 0010 1100 0010 0010 0001 0101 1101

K4 = 000001100101000101010100110011000001000100001000

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

K4 = 000001 100101 000101 010100 110011 000001 000100 001000

E (R3) = 101010 100101 011000 000100 000100 000010 101011 111010

K4 + E (R3) = 101011 000000 011101 010000 110111 000011 101111 110010

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

B2 = 000000, row = 00 = 0, column = 0000= 0, S2 (B2) = 14

B3 = 011101, row = 01 = 1, column = 1110= 14, S3 (B3) = 3

B4 = 010000, row = 00 = 0, column = 1000= 8, S4 (B4) = 3

B5 = 110111, row = 11 = 3, column = 1011= 11, S5 (B5) = 14

B6 = 000011, row = 01 = 1, column = 0001= 1, S6 (B6) = 15

B7 = 101111, row = 11 = 3, column = 0111= 8, S7 (B7) = 5

B8 = 110010, row = 10 = 2, column = 1001= 9, S8 (B8) = 12

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 9 14 3 3 14 15 5 12 (in Hexa Decimal) =

1001 1110 0011 0011 1110 1111 0101 1100 (in Binary).

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

f = 1101 1111 1111 1100 0010 0000 1011 1110

⍰ R4 = L3 + f

L3 = 1101 0010 0010 1001 0100 1011 0011 1110

f = 0100 1110 1110 0101 1110 0100 1010 1100

R4 = 1001 1100 1100 1100 1010 1111 1001 0010

For n = 5:

L5 = R4 = 1001 1100 1100 1100 1010 1111 1001 0010

K5 = 000011100100000101010101000000000101001001101000

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

K5 = 000011 100100 000101 010101 000000 000101 001001 101000

E (R4) = 010011 111001 011001 011001 010101 011111 110010 100101

K5 + E (R4) = 010011 011101 011101 001100 010101 011010 111011 001101

B1 = 010011, row = 01 = 1, column = 1001= 9, S1 (B1) = 6

B2 = 011101, row = 01 = 1, column = 1110= 14, S2 (B2) = 3

B3 = 011101, row = 01 = 1, column = 1110= 14, S3 (B3) = 3

B4 = 001100, row = 00 = 0, column = 0110= 6, S4 (B4) = 11

B5 = 010101, row = 01 = 1, column = 1010= 10, S5 (B5) = 12

B6 = 011010, row = 00 = 0, column = 1101= 13, S6 (B6) = 9

B7 = 111011, row = 11 = 3, column = 1101= 13, S7 (B7) = 0

B8 = 001101, row = 01 = 1, column = 0110= 6, S8 (B8) = 13

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 6 3 3 11 12 9 0 13 (in Hexa Decimal) =

0110 0011 0011 1011 1100 1001 0000 1101 (in Binary).

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

f = 11011101 01000100 11101010 01100100

⍰ R5 = L4 + f

L4 = 0101 0010 1100 0010 0010 0001 0101 1101

f =   1101 1101 0100 0100 1110 1010 0110 0100

R5 = 1000 1111 1000 0110 1100 1011 0011 1001

For n = 6:

L6 = R5 = 1000 1111 1000 0110 1100 1011 0011 1001

K6 = 000011110100000100101001010100001001100000100000

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

K6 =   000011 110100 000100 101001 010100 001001 100000 100000

E (R5) = 110001 011111 110000 001101 011001 010110 100111 110011

K6 + E (R5) = 110011 101011 110100 100100 001101 011111 000111 010011

B1 = 110011, row = 11 = 3, column = 1001= 9, S1 (B1) = 11

B2 = 101011, row = 11 = 3, column = 0101= 5, S2 (B2) = 9

B3 = 110100, row = 10 = 2, column = 1010= 10, S3 (B3) = 9

B4 = 100100, row = 10 = 2, column = 0010= 2, S4 (B4) = 14

B5 = 001101, row = 01 = 1, column = 0110= 6, S5 (B5) = 13

B6 = 011111, row = 01 = 1, column = 1111= 15, S6 (B6) = 8

B7 = 000111, row = 01 = 1, column = 0011= 3, S7 (B7) = 4

B8 = 010011, row = 01 = 1, column = 1001= 9, S8 (B8) = 6

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 11 9 9 14 13 8 4 6 (in Hexa Decimal) =

1011 1001 1001 1110 1101 1000 0100 0110 (in Binary).

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

f = 00110101 11011110 01010011 01100010

R6 = L5 + f

L5 = 1001 1100 1100 1100 1010 1111 1001 0010

f = 0011 0101 1101 1110 0101 0011 0110 0010

R6 = 1010 1001 0001 0010 1111 1100 1111 0000

For n = 7:

L7 = R6 = 1010 1001 0001 0010 1111 1100 1111 0000

K7 = 111011 001000 010010 110111 111101 100001 100010 111100

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

K7 = 100010 110000 000110 101001 100000 000000 110000 111000

E (R6) = 010101 010010 100010 100101 011111 111001 011110 100001

K7 + E (R6) = 110111 100010 100100 001101 111111 111001 101110 011001

B1 = 110111, row = 11 = 3, column = 1011= 11, S1 (B1) = 14

B2 = 100010, row = 10 = 2, column = 0001= 1, S2 (B2) = 1

B3 = 100100, row = 10 = 2, column = 0010= 2, S3 (B3) = 14

B4 = 001101, row = 01 = 1, column = 0110= 6, S4 (B4) = 13

B5 = 111111, row = 11 = 3, column = 1111= 15, S5 (B5) = 13

B6 = 111001, row = 11 = 3, column = 1100= 12, S6 (B6) = 10

B7 = 101110, row = 10 = 2, column = 0111= 7, S7 (B7) = 11

B8 = 011001, row = 01 = 1, column = 1100= 12, S8 (B8) = 9

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 14 1 14 13 13 10 11 9 (in Hexa Decimal)

= 1110 0001 1110 1101 1101 1010 1011 1001(in Binary).

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

f = 1011 1011 1010 0101 1101 1111 0100 0101

R7 = L6 + f

L6 = 1000 1111 1000 0110 1100 1011 0011 1001

f =   1011 1011 1010 0101 1101 1111 0100 0101

R7 = 0011 0100 0010 0011 0001 0100 0111 1100

For n = 8:

L8 = R7 = 0011 0100 0010 0011 0001 0100 0111 1100

K8 = 111101 111000 101000 111010 110000 010011 101111 111011

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

K8 =   100110 010000 101010 001001 000010 010011 101000 010000

E (R7) = 000110 101000 000100 000110 100010 101000 001111 111000

K8 + E (R7) = 100000 111000 101110 001111 100000 111011 100111 101000

B1 = 100000, row = 10 = 2, column = 0000= 0, S1 (B1) = 4

B2 = 111000, row = 10 = 2, column = 1100= 12, S2 (B2) = 3

B3 = 101110, row = 10 = 2, column = 0111= 7, S3 (B3) = 11

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

B5 = 100000, row = 10 = 2, column = 0000= 0, S5 (B5) = 4

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

B7 = 100111, row = 11 = 3, column = 0011= 3, S7 (B7) = 2

B8 = 101000, row = 10 = 2, column = 0100= 4, S8 (B8) = 13

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 4 3 11 1 4 0 2 13 (in Hexa Decimal)

= 0100 0011 1011 0001 0100 0000 0010 1101 (in Binary).

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

f = 11001100 00000100 11001101 00100100

R8 = L7 + f

L7 = 1010 1001 0001 0010 1111 1100 1111 0000

f = 1100 1100 0000 0100 1100 1101 0010 0100

R8 = 0110 0101 0001 0110 0011 0001 1101 0100

For n = 9:

L9 = R8 = = 0110 0101 0001 0110 0011 0001 1101 0100

K9 = 001110010000100010001010100010000000001000100001

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

K9 = 001110 010000 100010 001010 100010 000000 001000 100001

E (R8) = 001100 001010 100010 101100 000110 100011 111010 101000

K9 + E (R8) = 000010 011010 000000 100110 100100 100011 110010 001001

B1 = 000010, row = 00 = 0, column = 0001= 1, S1 (B1) = 4

B2 = 011010, row = 01 = 1, column = 1101= 13, S2 (B2) = 5

B3 = 000000, row = 00 = 0, column = 0000= 0, S3 (B3) = 14

B4 = 100110, row = 10 = 2, column = 0011= 3, S4 (B4) = 8

B5 = 100100, row = 10 = 2, column = 0010= 2, S5 (B5) = 14

B6 = 100011, row = 11 = 3, column = 0001= 1, S6 (B6) = 12

B7 = 110010, row = 10 = 2, column = 1001= 9, S7 (B7) = 12

B8 = 001001, row = 01 = 1, column = 0100= 4, S8 (B8) = 14

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 4,5,14,8,14,12,12,14(in Hexa Decimal)

= 0100 0101 1110 1000 1110 1100 1100 1110 (in Binary).

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

f = 00011001 00010111 11000001 11111101

R9 = L8 + f

L8 = 0011 0100 0010 0011 0001 0100 0111 1100

f = 1100 1101 1010 1101 1010 1011 0010 0111

R9 = 1111 1001 1000 1110 1011 1111 0101 1011

For n = 10:

L10 = R9 = 1111 1001 1000 1110 1011 1111 0101 1011

K10 = 001100000010100010001100100100100101000000100

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

K10 = 001100 000010 100010 001100 100100 100100 101000 000100

E (R9) = 111111 110011 110001 011101 010111 111110 101011 110111

K10 + E (R9) = 110011 110001 010011 010001 110011 011010 000011 110011

B1 = 110011, row = 11 = 3, column = 1001= 9, S1 (B1) = 11

B2 = 110001, row = 11 = 3, column = 1000= 8, S2 (B2) = 5

B3 = 010011, row = 01 = 1, column = 1001= 9, S3 (B3) = 6

B4 = 010001, row = 01 = 1, column = 1000= 8, S4 (B4) = 10

B5 = 110011, row = 11 = 3, column = 1001= 9, S5 (B5) = 11

B6 = 011010, row = 00 = 0, column = 1101= 13, S6 (B6) = 9

B7 = 000011, row = 01 = 1, column = 0001= 1, S7 (B7) = 15

B8 = 110011, row = 11 = 3, column = 1001= 9, S8 (B8) = 11

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 11,5,6,10,11,9,15,11(in Hexa Decimal) =

1011 0101 0110 1010 1011 1001 1111 1011 (in Binary).

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

f = 0011 1011 1101 0011 0110 1110 1101 0111

R10 = L9 + f

L9 = 1001 0010 1110 0000 0111 1000 0001 1011

f = 0011 1011 1101 0011 0110 1110 1101 0111

R10 = 1010 1001 0011 0011 0001 0110 1100 1100

For n = 11:

L11 = R10 = 1010 1001 0011 0011 0001 0110 1100 1100

K11 = 000100000010110000010100000100000000001110010000

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

K11 = 000100 000010 110000 010100 000100 000000 001110 010000

E (R10) = 010101 010010 100110 100110 100010 101101 011001 011001

K11 + E (R10) = 010001 010000 010110 110010 100110 101101 010111 001001

B1 = 010001, row = 01 = 1, column = 1000= 8, S1 (B1) = 10

B2 = 010000, row = 00 = 0, column = 1000= 8, S2 (B2) = 3

B3 = 010110, row = 00 = 0, column = 1011= 11, S3 (B3) = 12

B4 = 110010, row = 10 = 2, column = 1000= 8, S4 (B4) = 10

B5 = 100110, row = 10 = 2, column = 0011= 3, S5 (B5) = 8

B6 = 101101, row = 11 = 3, column = 0110= 6, S6 (B6) = 1

B7 = 010111, row = 01 = 1, column = 1011= 11, S7 (B7) = 11

B8 = 001001, row = 01 = 1, column = 0100= 4, S8 (B8) = 14

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 10,3,12,10,8,1,11,14,(in Hexa Decimal) =

1010 0011 1100 1010 1000 0001 1011 1110 (in Binary).

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

f = 01001011 11000011 01100111 01100001

R11 = L10 + f

L10 = 1001 1110 1001 1010 1010 0001 0110 1100

f = 0100 1011 1100 0011 0110 0111 0110 0001

R11 = 1101 0101 0101 1001 1100 0110 0000 1101

For n = 12:

L12 = R11 = 1101 0101 0101 1001 1100 0110 0000 1101

K12 = 010001000010110000110100100100010010000000000001

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

K12 = 010001 000010 110000 110100 100100 010010 000000 000001

E (R11) = 111010 101010 101011 110011 111000 001100 000001 011011

K12 + E (R11) = 101011 101000 011011 000111 011100 011110 000001 011010

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

B2 = 101000, row = 10 = 2, column = 0100= 4, S2 (B2) = 13

B3 = 011011, row = 01 = 1, column = 1101= 13, S3 (B3) = 5

B4 = 000111, row = 01 = 1, column = 0011= 3, S4 (B4) = 4

B5 = 011100, row = 00 = 0, column = 1110= 14, S5 (B5) = 0

B6 = 011110, row = 00 = 0, column = 1111= 15, S6 (B6) = 7

B7 = 000001, row = 01 = 1, column = 0000= 0, S7 (B7) = 0

B8 = 011010, row = 00 = 0, column = 1101= 13, S8 (B8) = 9

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 9,13,5,4,0,7,0,9,(in Hexa Decimal)

= 1001 1101 0101 0100 0000 0111 0000 1001(in Binary).

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

f = 00001100 10101001 01111000 00011010

R12 = L11 + f

L11 = 1010 1001 0011 0011 0001 0110 1100 1100 f = 0000 1100 1010 1001 0111 1000 0001 1010

R12 = 1010 0101 1001 1010 0110 1110 1101 0110

For n = 13:

L13 = R12 = 1010 0101 1001 1010 0110 1110 1101 0110

K13 = 110001101010010000100100011000100010001000000000

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

K13 = 110001 101010 010000 100100 011000 100010 001000 000000

E (R12) = 010100 001011 110011 110100 001101 011101 011010 101101

K13 + E (R12) = 100101 100001 100011 010000 010101 111111 010010 101101

B1 = 100101, row = 11 = 3, column = 0010= 2, S1 (B1) = 8

B2 = 100001, row = 11 = 3, column = 0000= 0, S2 (B2) = 15

B3 = 100011, row = 11 = 3, column = 0001= 1, S3 (B3) = 12

B4 = 010000, row = 00 = 0, column = 1000= 8, S4 (B4) = 3

B5 = 010101, row = 01 = 1, column = 1010= 10, S5 (B5) = 12

B6 = 111111, row = 11 = 3, column = 1111= 15, S6 (B6) = 13

B7 = 010010, row = 00 = 0, column = 1001= 9, S7 (B7) = 10

B8 = 101101, row = 11 = 3, column = 0110= 2, S8 (B8) = 8

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 8,15,12,3,12,13,10,8(in Hexa Decimal)

= 1000 1111 1100 0011 1100 1101 1010 1000 (in Binary).

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

f = 1101 1001 1100 1101 0110 0101 0001 1001

R13 = L12 + f

L12 = 1101 0101 0101 1001 1100 0110 0000 1101

f = 1101 1001 1100 1101 0110 0101 0001 1001

R13 = 0000 1100 1001 0100 1010 0011 0001 0100

For n = 14:

L14 = R13 = 0000 1100 1001 0100 1010 0011 0001 0100

K14 = 110010101000011000100010001100000010000100001110

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

K14 = 110010 101000 011000 100010 001100 000010 000100 001110

E (R13) = 000001 011001 010010 101001 010100 000110 100010 101000

K14 + E (R13) = 110011 110001 001010 001011 011000 000100 100110 100110

B1 = 110011, row = 11 = 3, column = 1001= 9, S1 (B1) = 11

B2 = 110001, row = 11 = 3, column = 1000= 8, S2 (B2) = 5

B3 = 001010, row = 00 = 0, column = 0101= 5, S3 (B3) = 15

B4 = 001011, row = 01 = 1, column = 0101= 5, S4 (B4) = 2

B5 = 011000, row = 00 = 0, column = 1100= 12, S5 (B5) = 5

B6 = 000100, row = 00 = 0, column = 0010= 2, S6 (B6) = 13

B7 = 100110, row = 10 = 2, column = 0011= 3, S7 (B7) = 8

B8 = 100110, row = 10 = 2, column = 0011= 3, S8 (B8) = 8

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 11,5,15,2,5,13,8,8 (in Hexa Decimal) =

1011 0101 1111 0010 0101 1101 1000 1000 (in Binary).

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

f = 0011 1100 1100 0101 0110 0011 0001 1111

R14 = L13 + f

L13 = 1010 0101 1001 1010 0110 1110 1101 0110

f = 0011 1100 1100 0101 0110 0011 0001 1111

R14 = 1001 1001 0101 1111 0000 1101 1100 1001

For n = 15:

L15 = R14 = 1001 1001 0101 1111 0000 1101 1100 1001

K15 = 111010001001001000101010001001000001000010000010

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

K15 = 111010 001001 001000 101010 001001 000001 000010 000010

E (R14) = 110011 110010 101011 111110 100001 011011 111001 010011

K15 + E (R14) = 001001 111011 100011 010100 101000 011010 111011 010001

B1 = 001001, row = 01 = 1, column = 0100= 4, S1 (B1) = 14

B2 = 111011, row = 11 = 3, column = 1101= 13, S2 (B2) = 0

B3 = 100011, row = 11 = 3, column = 0001= 1, S3 (B3) = 12

B4 = 010100, row = 00 = 0, column = 1010= 10, S4 (B4) = 6

B5 = 101000, row = 10 = 2, column = 0100= 4, S5 (B5) = 13

B6 = 011010, row = 00 = 0, column = 1101= 13, S6 (B6) = 9

B7 = 111011, row = 11 = 3, column = 1101= 13, S7 (B7) = 0

B8 = 010001, row = 01 = 1, column = 1000= 8, S8 (B8) = 10

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 14,0,12,6,13,9,0,10(in Hexa Decimal)

= 1110 0000 1100 0110 1101 1001 0000 1010 (in Binary).

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

f = 0011 1001 1100 0111 1011 0011 0000 0000

R15 = L14 + f

L14 = 0000 1100 1001 0100 1010 0011 0001 0100

f = 0011 1001 1100 0111 1011 0011 0000 0000

R15 = 0011 0101 0101 0011 0001 0000 0001 0100

For n = 16:

L16 = R15 = 0011 0101 0101 0011 0001 0000 0001 0100

K16 = 101000011001001010100010000010100010000111000000

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

K16 = 101000 011001 001010 100010 000010 100010 000111 000000

E (R15) = 000110 101010 101010 100110 100010 100000 000010 101000

K16 + E (R15) = 101110 110011 100000 000100 100000 000010 000101 101000

B1 = 101110, row = 10 = 2, column = 0111= 7, S1 (B1) = 11

B2 = 110011, row = 11 = 3, column = 1001= 9, S2 (B2) = 11

B3 = 100000, row = 10 = 2, column = 0000= 0, S3 (B3) = 4

B4 = 000100, row = 00 = 0, column = 0010= 2, S4 (B4) = 13

B5 = 100000, row = 10 = 2, column = 0000= 0, S5 (B5) = 4

B6 = 000010, row = 00 = 0, column = 0001= 1, S6 (B6) = 4

B7 = 000101, row = 01 = 1, column = 0010= 2, S7 (B7) = 7

B8 = 101000, row = 10 = 2, column = 0100= 4, S8 (B8) = 13

S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8) = 11,11,4,13,4,4,7,13 (in Hexa Decimal)

= 1011 1011 0100 1101 0100 0100 0111 1101 (in Binary).

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

f = 1100 1010 1001 1101 0101 1110 0110 1010

R16 = L15 + f

L15 = 1001 1001 0101 1111 0000 1101 1100 1001

f = 1100 1010 1001 1101 0101 1110 0110 1010

R16 = 0101 0011 1100 0010 0101 0011 1010 0011

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):

4 8 12 16 20 24 28 32 36 40 44 48 52 56 60

R16L16 = 0101 0011 1100 0010 0101 0011 1010 0011 0011 0101 0101 0011 0001 0000 0001 0100

IP-1

= 0110 0101 0111 0101 1000 0010 0000 0000 1110 1110 1000 0001 0111 0100 0001 0001

BOOM!! BOOM!! BOOM!! BOOM!! BOOM!! BOOM!! BOOM!! BOOM!!

Which is in hexadecimal format is 65758200EE817411

C = 65758200EE817411

This is the encrypted form of M =NATNAEL A (The first 64 bit of my full name: NATNAEL ARGAW).