Jacob S. Santos   **11/11/2024**

BSCOE 4-1   **Dr. Ariel Sison**

Generate the 16 keys using abcdef1234567890

Key Value = abcdef1234567890

= 1010101111001101111011110001001000110100010101100111100010010000

Apply Table 3.1

= 10000111011001100101010111110010110100110110010001111000

First Iteration:

Divide into 2 groups

C0 (binary):
10000111011001100101010111111

C0 (hex): 876655F

D0 (hex): 2D36478

D0 (binary):
0010110100110110010001111000

Refer to Table 3.2

Shift Left (S2): 00001110110011001010101011111

Shift Left (S3): 0101101001101100100011110000

S2 || S3

= 00001110110011001010101111110101101001101100100011110000

C1 (hex): 0ECCABF

D1 (hex): 5A6C8F0

Apply Table 3.3

110101010111110010011010110000101110011000011001

K1 = D57C9AC2E619

Second Iteration:

C1 || D1

0000111011001100101010111111010110100110110010001110000

= 0ECCABF5A6C8F0

Divide into 2 groups:

C1 (binary): 0000111011001100101010111111

D1 (binary): 0101101001101100100011110000

C1 (hex): 0ECCABF

D1 (hex): 5A6C8F0

Refer to Table 3.2

Shift Left (S2): 0001110110011001010101111110

Shift Left (S3): 1011010011011001000111100000

S2 || S3

00011101100110010101011111101011010011011001000111100000

C2 (hex): 1D9957E

D2 (hex): B4D91E0

Apply Table 3.3

000101000100101111011101011000110011100010001011

K2 = 144BEEB19C8B

Third Iteration:

C2 || D2

= 0001110110011001010101111110101101001101100100011110000

= 1D9957EB4D91E0

Divide into 2 groups

C2 (binary): 0001110110011001010101111110

D2 (binary): 1011010011011001000111100000

C2 (hex): 1D9957E

D2 (hex): B4D91E0

Refer to Table 3.2

Shift Left (S2): 0111011001100101010111111000

Shift Left (S3): 1101001101100100011110000010

S2 || S3

0111011001100101010111111000110100110110010001111000 0010

C3 (hex): 76655F8

D3 (hex): D364782

Apply Table 3.3

1011001001111001001101010000111000010110001 10111

K3 = B279350E1637

Fourth Iteration:

C3 || D3

= 0111011001100101010111111000110100110110010001111000010

= 76655F8D364782

Divide into 2 groups

C3 (binary): 0111011001100101010111111000

D3 (binary): 11010011011001000111110000010

C3 (hex): 76655F8

D3 (hex): D364782

Refer to Table 3.2

Shift Left (S2): 1101100110010101011111100001

Shift Left (S3): 01001101100100011110000001011

S2 || S3

11011001100101010111110000010100110110010001111000001011

C4 (hex): D9957E1

D4 (hex): 4D91E0B

Apply Table 3.3

100011010010111101100101000111110110100111100100

K4 = 8D2F651F69E4

Fifth Iteration:

C4 || D4

1101100110010101011111000010100110110010001111000001011

= D9957E14D91E0B

Divide into 2 groups

C4 (binary): 1101100110010101011111100001

D4 (binary): 0100110110010001111000001011

C4 (hex): D9957E1

D4 (hex): 4D91E0B

Refer to Table 3.2

Shift Left (S2): 0110011001010101111110000111

Shift Left (S3): 0011011001000111100000101101

S2 || S3

01100110010101011111100001110011011001000111100000101101

C5 (hex): 6655F87

D5 (hex): 364782D

Apply Table 3.3

110000110111011010111101001000001100100111010001

K5 = C376BD20C9D1

Sixth Iteration:

C5 || D5

0110011001010101111110000111001101100100011110000010101101

= 6655F87364782D

Divide into 2 groups

C5 (binary): 0110011001010101111110000111

D5 (binary): 0011011001000111100000101101

C5 (hex): 6655F87

D5 (hex): 364782D

Refer to Table 3.2

Shift Left (S2): 1001100101010111111000011101

Shift Left (S3): 1101100100011110000010110100

S2 || S3

1001100101010111111000011101110110010001111000001 0110100

C6 (hex): 9957E1D

D6 (hex): D91E0B4

Apply Table 3.3

110111011001011111000001100001110100 10000010111

K6 = DD97E0C3A417

Seventh Iteration:

C6 || D6

1001100101010111110000111011011001000111100000 10110100

= 9957E1DD91E0B4

Divide into 2 groups

C6 (binary): 1001100101010111111000011101

D6 (binary): 1101100100011110000010110100

C6 (hex): 9957E1D

D6 (hex): D91E0B4

Refer to Table 3.2

Shift Left (S2): 0110010101011111100001110110

Shift Left (S3): 0110010001110000010110100 11

S2 || S3

01100101010111110000111011001100100011110000 01011010011

C7 (hex): 655F876

D7 (hex): 64782D3

Apply Table 3.3

110100101101101011010111101111000001110001000

K7 = D2DAEBEF0788

Eighth Iteration:

C7 || D7

0110010101011111000011011001100100011110000010110110011

= 655F87664782D3

Divide into 2 groups

C7 (binary): 0110010101011111100001110110

D7 (binary): 0110010001110000010110100011

C7 (hex): 655F876

D7 (hex): 64782D3

Refer to Table 3.2

Shift Left (S2): 1001010101111110000111011001

Shift Left (S3): 1001000111100000101101001101

S2 || S3

10010101011111100001110110011001000111100000101101001101

C8 (hex): 957E1D9

D8 (hex): 91E0B4D

Apply Table 3.3

101110011111001101000110000110000101001101001111

K8 = B9F34618534F

Ninth Iteration:

C8 || D8

1001010101111100001110110011001000111100000101101001101

957E1D991E0B4D

Divide into 2 groups

C8 (binary): 1001010101111100001110110011

D8 (binary): 1001000111100000101101001101

C8 (hex): 957E1D9

D8 (hex): 91E0B4D

Refer to Table 3.2

Shift Left (S2): 0010101011111000011101100111

Shift Left (S3): 0010001111000001011010011011

S2 || S3

0010101011111000011101100110010001111000001011010011011

C9 (hex): 2AFC3B3

D9 (hex): 23C169B

Apply Table 3.3

1011011100111110000111100111110000001101011001000

K9 = B73E1E7C0D64

Tenth Iteration:

C9 || D9

0010101011111000011011001100100011110000010110100110111

2AFC3B323C169B

Divide into 2 groups

C9 (binary): 0010101011111000011101100110011

D9 (binary): 0010001110000010110100110111

C9 (hex): 2AFC3B3

D9 (hex): 23C169B

Refer to Table 3.2

Shift Left (S2): 1010101111100001110110011001100

Shift Left (S3): 1000111100000101101001101100

S2 || S3

1010101111100001110110011001100100011110000010110100110110 0

C10 (hex): ABF0ECC

D10 (hex): 8F05A6C

Apply Table 3.3

011011100011011011010000000010001110100011011110

K10 = 6E36D008E8DE

Eleventh Iteration:

C10 || D10

1010101111100001110110011001000111100000101101001101100

= ABF0ECC8F05A6C

Divide into 2 groups

C10 (binary): 1010101111100001110110011001100

D10 (binary): 1000111100000101101001101100

C10 (hex): ABF0ECC

D10 (hex): 8F05A6C

Refer to Table 3.2

Shift Left (S2): 1010111111000011101100110010

Shift Left (S3): 0011110000010110100110110010

S2 || S3

10101111110000111011001100100011110000010110100110110010

C11 (hex): AFC3B32

D11 (hex): 3C169B2

Apply Table 3.3

01011110110111000111100011001011111010010010001

K11 = 5EDC7C65F491

:

Twelfth Iteration:

C11 || D11

1010111110000111011001100100011110000010110100110110010

= AFC3B323C169B2

Divide into 2 groups

C11 (binary): 1010111110000111011001100100

D11 (binary): 0011110000010110100110110010

C11 (hex): AFC3B32

D11 (hex): 3C169B2

Refer to Table 3.2

Shift Left (S2): 1011111100001110110011001010

Shift Left (S3): 1111000001011010011011001000

S2 || S3

1011111100001110110011001010111100000101101001101100100 0

C12 (hex): BF0ECCA

D12 (hex): F05A6C8

Apply Table 3.3

110011101110000101011010101010110000010001101011

K12 = CEE15AAB046B

Thirteenth Iteration:

C12 || D12

1011111100001110110011001010111000001011010011011001000

= BF0ECCAF05A6C8

Divide into 2 groups

C12 (binary): 1011111100001110110011001010

D12 (binary): 1111000001011010011011001000

C12 (hex): BF0ECCA

D12 (hex): F05A6C8

Refer to Table 3.2

Shift Left (S2): 1111110000111011001100101010

Shift Left (S3): 1100000101101001101100100011

S2 || S3

1111110000111011001100101010110000010110100110110010011

C13 (hex): FC3B32A

D13 (hex): C169B23

Apply Table 3.3

0010111011001111001011110001101101101100000110

K13 = 2ECF2F8EDB06

Fourteenth Iteration:

C13 || D13

11111100001110110011001010101100000101101001101100100011

 = FC3B32AC169B23

Divide into 2 groups

C13 (binary): 1111110000111011001100101010

D13 (binary): 1100000101101001101100100011

C13 (hex): FC3B32A

D13 (hex): C169B23

Refer to Table 3.2

Shift Left (S2): 1111000011101100110010101011

Shift Left (S3): 0000010110100110110010001111

S2 || S3

11110000111011001100101010110000010110100110110010001111

C14 (hex): F0ECCAB

D14 (hex): 05A6C8F

Apply Table 3.3

111010110011001000010110001010001000111111110100

K14 = EB390B1447F4

Fifteenth Iteration:

C14 || D14

1111000011101100110010101011000010110100110110010001111

= F0ECCAB05A6C8F

Divide into 2 groups

C14 (binary): 1111000011101100110010101011

D14 (binary): 0000010110100110110010001111

C14 (hex): F0ECCAB

D14 (hex): 05A6C8F

Refer to Table 3.2

Shift Left (S2): 1100001110110011001010101111

Shift Left (S3): 0001011010011011001000111100

S2 || S3

11000011101100110010101011110001011010011011001000111100

C15 (hex): C3B32AF

D15 (hex): 169B23C

Apply Table 3.3

001010011010111011111001110110011000100011000001

K15 = 29AEF9D988C1

Sixteenth Iteration:

C15 || D15

110000111011001100101010111100010110100110110010001111100

C3B32AF169B23C

Divide into 2 groups

C15 (binary): 1100001110110011001010101111

D15 (binary): 0001011010011011001000111100

C15 (hex): C3B32AF

D15 (hex): 169B23C

Refer to Table 3.2

Shift Left (S2): 1000011101100110010101011111

Shift Left (S3): 0010110100110110010001111000

S2 || S3

10000111011001100101010111110010110100110110010001111000

C16 (hex): 876655F

D16 (hex): 2D36478

Apply Table 3.3

101110011010000110111000110000110100010111111100

K16 = B9D0DC61A2FC