JACOB S. SANTOS   **11/04/24**

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

DES

Fourth Iteration

C3 || D3

C3=CD1A45B

D3=22E87FD

= 1100110100011010010001011011001000101110100001111111101

Divide into 2 groups

C3 = 1100 1101 0001 1010 0100 0101 1011

D3 = 0010 0010 1110 1000 0111 1111 1101

Shift Left (Table 3.2) S2

0011010001101001000101101111

Shift Left (Table 3.2) S3

1000101110100001111111110100

S2 || S3 (Concatenate)

00110100011010010001011011111000101110100001111111110100

C4 = 346916F , D4 = 8BA1FF4

Apply Table 3.3

0010001101011001101011100101100011111110001011110

K4 = 2359AE58FE2E

Fifth Iteration

C4 || D4

C4 = 346916F

D4 = 8BA1FF4

= 0011010001101001000101101111100010111010000111111110100

Divide into 2 groups

C4 = 0011010001101001000101101111

D4 = 1000101110100001111111110100

Shift Left (Table 3.2) S2

110100011010010001 0110111100

Shift Left (Table 3.2) S3

0010111010000111111111010010

S2 || S3 (Concatenate)

1101 0001 1010 0100 0101 1011 1100 0010 1110 1000 0111 1111 1101 0010

C5 = D1A45BC , D5 = 2E87FD2

Apply Table 3.3

1011 1000 0010 1001 1100 0101 0111 1100 0111 1100 1011 1000

K5 =B829C57C7CB8