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

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

Code Simulation (Output):

```
Enter a 64-bit key in hexadecimal format: abcdef1234567890
Initial 64-bit key (binary): 1010101111001101111011110001001000110100010101100111100010010000
Initial 64-bit key (hex):    abcdef1234567890

Apply Table 3.1 (56-bit key):
Binary: 10000111011001100101010111110010110100110110010001111000
Hex:     876655F2D36478

--- Round  1 ---
Divide into 2 groups
C0 (binary): 1000011101100110010101011111
D0 (binary): 0010110100110110010001111000
C0 (hex): 876655F
D0 (hex): 2D36478

Refer to Table 3.2
Shift Left (S2): 0000111011001100101010111111 (binary)
Shift Left (S3): 0101101001101100100011110000 (binary)
S2 || S3 00001110110011001010101111110101101001101100100011110000 (binary) 0ECCABF5A6C8F0 (hex)
C1: 0000111011001100101010111111 (binary) 0ECCABF (hex)
D1: 0101101001101100100011110000 (binary) 5A6C8F0 (hex)

Apply Table 3.3
K 1 (binary): 110101010111110010011010110000101110011000011001
K 1 (hex):    D57C9AC2E619

--- Round  2 ---
Using C1 and D1 from previous round to generate C2 and D2.

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 (binary)
Shift Left (S3): 1011010011011001000111100000 (binary)
S2 || S3 00011101100110010101011111101011010011011001000111100000 (binary) 1D9957EB4D91E0 (hex)
C2: 0001110110011001010101111110 (binary) 1D9957E (hex)
D2: 1011010011011001000111100000 (binary) B4D91E0 (hex)

Apply Table 3.3
K 2 (binary): 000101000100101111101110101100011001110010001011
K 2 (hex):    144BEEB19C8B
```

```
--- Round  3 ---
Using C2 and D2 from previous round to generate C3 and D3.

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 (binary)
Shift Left (S3): 1101001101100100011110000010 (binary)
S2 || S3 01110110011001010101111110001101001101100100011110000010 (binary) 76655F8D364782 (hex)
C3: 0111011001100101010111111000 (binary) 76655F8 (hex)
D3: 1101001101100100011110000010 (binary) D364782 (hex)

Apply Table 3.3
K 3 (binary): 101100100111100100110101000011100001011000110111
K 3 (hex):    B279350E1637

--- Round  4 ---
Using C3 and D3 from previous round to generate C4 and D4.

Divide into 2 groups
C3 (binary): 0111011001100101010111111000
D3 (binary): 1101001101100100011110000010
C3 (hex): 76655F8
D3 (hex): D364782

Refer to Table 3.2
Shift Left (S2): 1101100110010101011111100001 (binary)
Shift Left (S3): 0100110110010001111000001011 (binary)
S2 || S3 11011001100101010111111000010100110110010001111000001011 (binary) D9957E14D91E0B (hex)
C4: 1101100110010101011111100001 (binary) D9957E1 (hex)
D4: 0100110110010001111000001011 (binary) 4D91E0B (hex)

Apply Table 3.3
K 4 (binary): 100011010010111101100101000111110110100111100100
K 4 (hex):    8D2F651F69E4
```
```
--- Round  5 ---
Using C4 and D4 from previous round to generate C5 and D5.

Divide into 2 groups
C4 (binary): 1101100110010101011111100001
D4 (binary): 0100110110010001111000001011
C4 (hex): D9957E1
D4 (hex): 4D91E0B

Refer to Table 3.2
Shift Left (S2): 0110011001010101111111000011 (binary)
Shift Left (S3): 0011011001000111100000101101 (binary)
S2 || S3 01100110010101011111110000110011011001000111100000101101 (binary) 6655F87364782D (hex)
C5: 0110011001010101111111000011 (binary) 6655F87 (hex)
D5: 0011011001000111100000101101 (binary) 364782D (hex)

Apply Table 3.3
K 5 (binary): 110000110111011010101110100100000110010011010001
K 5 (hex):    C376BD20C9D1
```

```
--- Round  6 ---
Using C5 and D5 from previous round to generate C6 and D6.

Divide into 2 groups
C5 (binary): 0110011001010101111110000111
D5 (binary): 0011011001000111100000101101
C5 (hex): 6655F87
D5 (hex): 364782D

Refer to Table 3.2
Shift Left (S2): 1001100101010111110000011101 (binary)
Shift Left (S3): 1101100100011110000010110100 (binary)
S2 || S3 10011001010101111110000011101101100100011110000010110100 (binary) 9957E1DD91E0B4 (hex)
C6: 1001100101010111110000011101 (binary) 9957E1D (hex)
D6: 1101100100011110000010110100 (binary) D91E0B4 (hex)

Apply Table 3.3
K 6 (binary): 110111011100101111110000011000011101001000010111
K 6 (hex):    DD97E0C3A417

--- Round  7 ---
Using C6 and D6 from previous round to generate C7 and D7.

Divide into 2 groups
C6 (binary): 1001100101010111110000011101
D6 (binary): 1101100100011110000010110100
C6 (hex): 9957E1D
D6 (hex): D91E0B4

Refer to Table 3.2
Shift Left (S2): 0110010101011111100001110110 (binary)
Shift Left (S3): 0110010001111000001011010011 (binary)
S2 || S3 01100101010111111000011101100110010001111000001011010011 (binary) 655F87664782D3 (hex)
C7: 0110010101011111100001110110 (binary) 655F876 (hex)
D7: 0110010001111000001011010011 (binary) 64782D3 (hex)

Apply Table 3.3
K 7 (binary): 110100101101101011101011111011110000011110001000
K 7 (hex):    D2DAEBEF0788
```

```
--- Round  8 ---
Using C7 and D7 from previous round to generate C8 and D8.

Divide into 2 groups
C7 (binary): 0110010101011111100001110110
D7 (binary): 0110010001111000001011010011
C7 (hex): 655F876
D7 (hex): 64782D3

Refer to Table 3.2
Shift Left (S2): 1001010101111111000011101101001 (binary)
Shift Left (S3): 1001000111100000101101001101 (binary)
S2 || S3 10010101011111110000111011001100100011110000010110100110 (binary) 957E1D991E0B4D (hex)
C8: 1001010101111111000011101101001 (binary) 957E1D9 (hex)
D8: 1001000111100000101101001101 (binary) 91E0B4D (hex)

Apply Table 3.3
K 8 (binary): 101110011111100110100011000011000010100110101111
K 8 (hex):    B9F34618534F
```

```
--- Round  9 ---
Using C8 and D8 from previous round to generate C9 and D9.

Divide into 2 groups
C8 (binary): 10010101011111100001110110011001
D8 (binary): 10010001111000001011101001101
C8 (hex): 957E1D9
D8 (hex): 91E0B4D

Refer to Table 3.2
Shift Left (S2): 0010101011111100001110110011 (binary)
Shift Left (S3): 0010001111000001011010011011 (binary)
S2 || S3 0010101011111100001110110011001000111100000101101001 1011 (binary) 2AFC3B323C169B (hex)
C9: 0010101011111100001110110011 (binary) 2AFC3B3 (hex)
D9: 0010001111000001011010011011 (binary) 23C169B (hex)

Apply Table 3.3
K 9 (binary): 1011011100111110000111100111110000001101011001 00
K 9 (hex):    B73E1E7C0D64

--- Round 10 ---
Using C9 and D9 from previous round to generate C10 and D10.

Divide into 2 groups
C9 (binary): 0010101011111100001110110011
D9 (binary): 0010001111000001011010011011
C9 (hex): 2AFC3B3
D9 (hex): 23C169B

Refer to Table 3.2
Shift Left (S2): 1010101111111000011101100110011001100 (binary)
Shift Left (S3): 1000111100000101101001101100 (binary)
S2 || S3 1010101111111000011101100110011001000111100000101101001101100 (binary) ABF0ECC8F05A6C (hex)
C10: 1010101111111000011101100110011 (binary) ABF0ECC (hex)
D10: 1000111100000101101001101100 (binary) 8F05A6C (hex)

Apply Table 3.3
K10 (binary): 01101110001101101101000000001000111010001 1011110
K10 (hex):    6E36D008E8DE
```

```
--- Round 11 ---
Using C10 and D10 from previous round to generate C11 and D11.

Divide into 2 groups
C10 (binary): 1010101111111000011101100110011
D10 (binary): 1000111100000101101001101100
C10 (hex): ABF0ECC
D10 (hex): 8F05A6C

Refer to Table 3.2
Shift Left (S2): 1010111111100001110110011001 0 (binary)
Shift Left (S3): 0011110000010110100110110010 (binary)
S2 || S3 1010111111100001110110011001000111100000101101001101100010 (binary) AFC3B323C169B2 (hex)
C11: 1010111111100001110110011 0010 (binary) AFC3B32 (hex)
D11: 0011110000010110100110110010 (binary) 3C169B2 (hex)

Apply Table 3.3
K11 (binary): 01011110110111000111110001100101111101001 0010001
K11 (hex):    5EDC7C65F491
```

```
--- Round 12 ---
Using C11 and D11 from previous round to generate C12 and D12.

Divide into 2 groups
C11 (binary): 1010111111000011101100110010
D11 (binary): 0011110000010110100110110010
C11 (hex): AFC3B32
D11 (hex): 3C169B2

Refer to Table 3.2
Shift Left (S2): 1011111100001110110011001010 (binary)
Shift Left (S3): 1111000001011010011011001000 (binary)
S2 || S3 10111111000011101100110010101111000001011010011011001000 (binary) BF0ECCAF05A6C8 (hex)
C12: 1011111100001110110011001010 (binary) BF0ECCA (hex)
D12: 1111000001011010011011001000 (binary) F05A6C8 (hex)

Apply Table 3.3
K12 (binary): 110011101110000101011010101010110000010001101011
K12 (hex):    CEE15AAB046B

--- Round 13 ---
Using C12 and D12 from previous round to generate C13 and D13.

Divide into 2 groups
C12 (binary): 1011111100001110110011001010
D12 (binary): 1111000001011010011011001000
C12 (hex): BF0ECCA
D12 (hex): F05A6C8

Refer to Table 3.2
Shift Left (S2): 1111111000011101100110010100 (binary)
Shift Left (S3): 1100000101101001101100100011 (binary)
S2 || S3 11111110000111011001100101001100000101101001101100100011 (binary) FC3B32AC169B23 (hex)
C13: 1111111000011101100110010100 (binary) FC3B32A (hex)
D13: 1100000101101001101100100011 (binary) C169B23 (hex)

Apply Table 3.3
K13 (binary): 001011101100111100101111100011101101101100000110
K13 (hex):    2ECF2F8EDB06
```

```
--- Round 14 ---
Using C13 and D13 from previous round to generate C14 and D14.

Divide into 2 groups
C13 (binary): 1111111000011101100110010100
D13 (binary): 1100000101101001101100100011
C13 (hex): FC3B32A
D13 (hex): C169B23

Refer to Table 3.2
Shift Left (S2): 1111000011101100110010101011 (binary)
Shift Left (S3): 0000010110100110110010001111 (binary)
S2 || S3 11110000111011001100101010110000010110100110110010001111 (binary) F0ECCAB05A6C8F (hex)
C14: 1111000011101100110010101011 (binary) F0ECCAB (hex)
D14: 0000010110100110110010001111 (binary) 05A6C8F (hex)

Apply Table 3.3
K14 (binary): 111010110011100100001011000101000100011111110100
K14 (hex):    EB390B1447F4
```

```
--- Round 15 ---
Using C14 and D14 from previous round to generate C15 and D15.

Divide into 2 groups
C14 (binary): 11110000111011001100010101011
D14 (binary): 00000101101001101100010001111
C14 (hex): F0ECCAB
D14 (hex): 05A6C8F

Refer to Table 3.2
Shift Left (S2): 11000011101100110010010101111 (binary)
Shift Left (S3): 00010110100110110010000111100 (binary)
S2 || S3 1100001110110011001001010111100010110100110110010000111100 (binary) C3B32AF169B23C (hex)
C15: 11000011101100110010010101111 (binary) C3B32AF (hex)
D15: 00010110100110110010000111100 (binary) 169B23C (hex)

Apply Table 3.3
K15 (binary): 001010011010111011111100111011001100010001000001
K15 (hex):    29AEF9D988C1

--- Round 16 ---
Using C15 and D15 from previous round to generate C16 and D16.

Divide into 2 groups
C15 (binary): 11000011101100110010010101111
D15 (binary): 00010110100110110010000111100
C15 (hex): C3B32AF
D15 (hex): 169B23C

Refer to Table 3.2
Shift Left (S2): 10000111011001100101010101111 (binary)
Shift Left (S3): 00101101001101100100001111000 (binary)
S2 || S3 1000011101100110010101010111100101101001101100100001111000 (binary) 876655F2D36478 (hex)
C16: 10000111011001100101010101111 (binary) 876655F (hex)
D16: 00101101001101100100001111000 (binary) 2D36478 (hex)

Apply Table 3.3
K16 (binary): 101110011101000011011100011000011010001011111100
K16 (hex):    B9D0DC61A2FC
```