JACOB S. SANTOS **10/21/2024**

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

Round 4:

C3 03 1E FB

Circular byte left shift: 03 1E FB C3

Byte substitution: 7B 72 0F 2E

Adding round constant: 08 00 00 00

0111 1011 0111 0010 0000 1111 0010 1110

0000 1000 0000 0000 0000 0000 0000 0000

0111 0011 0111 0010 0000 1111 0010 1110

7 3 7 2 0 F 2 E

W15 = **73 72 0F 2E**

W16 = 73720F2E XOR D2600DE7 = **a11202c9**

W17 = a11202c9 XOR 157ABC68 = **b468bea1**

W18 = b468bea1 XOR 6339E901 = **d75157a0**

W19 = d75157a0 XOR C3031EFB = **14 52 49 5b**

Round 5:

14 52 49 5b

Circular byte left shift: 52 49 5b 14

Byte substitution: 00 3b 39 fa

Adding round constant: 10 00 00 00

0000 0000 0011 1011 0011 1001 1111 1010

0001 0000 0000 0000 0000 0000 0000 0000

0001 0000 0011 1011 0011 1001 1111 1010

1 0 3 b 3 9 f a

W19 = **10 3B 39 FA**

W20 = 103B39FA XOR a11202c9 **=** b1293b33

W21 = b1293b33 XOR b468bea1 = 5418592

W22 = 5418592 XOR d75157a0 = d210d232

W23 = d210d232 XOR 1452495b **= c6 42 9b 69**