JACOB S. SANTOS   **09/16/24**

BSCOE 3-1   **Dr. Ariel Sison**

Assignment

Computing for T21 using previous iteration T20

T20
A - a3d6efd7
B - b78ca1cc
C - fcf1516a
D - 7bc144b8
E - a9136fa9

T21

F = B XOR C XOR D

F = b78ca1cc XOR fcf1516a XOR 7bc144b8

F= 4b7df0a6 XOR 7bc144b8

F(21) = 30bcb41e

A - a3d6efd7 SHIFT 5 TIMES TO LEFT 7ADDFAF4

Temp = Shift left(A, 5) + F + E + W21 +K1

W21 = 000000a0, K1 = 6ed9eba1

Temp = 7ADDFAF4 + 30bcb41e + a9136fa9 + 000000a0 + 6ed9eba1

Temp(21) = c3880afc

B = SHIFT LEFT BY 30 = 00101101111000110010100001110011 = **2DE32873**

Final answer for T21:

T21

A - c3880afc

B - a3d6efd7

C - 2DE32873

D - fcf1516a

E - 7bc144b8

Computing for T22 using previous iteration T21

T21

A - c3880afc

B - a3d6efd7

C - 2DE32873

D - fcf1516a

E - 7bc144b8

T22

F = B XOR C XOR D

F = a3d6efd7 XOR 2DE32873 XOR fcf1516a

F = 8e35c7a4 XOR fcf1516a

F(22)= 72c496ce

A - c3880afc SHIFT 5 TIMES TO LEFT

A –01110001000000010101111110011000

A = **71015F98**

Temp = Shift left(A, 5) + F + E + W22 +K1

W22 = d3fea9d8, K1 = 6ed9eba1

Temp = 71015F98 + 72c496ce + 7bc144b8 + d3fea9d8 + 6ed9eba1

Temp(22) = a25fd097

B = SHIFT LEFT BY 30 = 11101000111101011011101111110101 = **E8F5BBF5**

Final answer for T22:

T22

A - a25fd097

B - c3880afc

C - E8F5BBF5

D - 2DE32873

E - fcf1516a

Computing for T23 using previous iteration T22

T22

A - a25fd097

B - c3880afc

C - E8F5BBF5

D - 2DE32873

E - fcf1516a

T23

F = B XOR C XOR D

F = c3880afc XOR E8F5BBF5 XOR 2DE32873

F = 2b7db109 XOR 2DE32873

F(23) = 69e997a

A - a25fd097 SHIFT 5 TIMES TO LEFT

A – 0100101111110100001001011110100

A - **4BFA12F4**

Temp = Shift left(A, 5) + F + E + W23 +K1

W23 = 64000052, K1 = 6ed9eba1

Temp = 4BFA12F4 + 69e997a + fcf1516a + 64000052 +6ed9eba1

Temp(23) = 2263e9cb

B = SHIFT LEFT BY 30 = 00110000111000100000001010111111 = **30E202BF**

Final answer for T23:

T23

A - 2263e9cb

B - a25fd097

C - 30E202BF

D - E8F5BBF5

E - 2DE32873

Computing for T24 using previous iteration T23

T23

A - 2263e9cb

B - a25fd097

C - 30E202BF

D - E8F5BBF5

E - 2DE32873

T24

F = B XOR C XOR D

F = a25fd097 XOR 30E202BF XOR E8F5BBF5

F = 92bdd228 XOR E8F5BBF5

F(24)= 7a4869dd

A - 2263e9cb SHIFT 5 TIMES TO LEFT

A - 01001100011111010011100101100100

A - **4C7D3964**

Temp = Shift left(A, 5) + F + E + W24 +K1

W24 = 69ff55ac, K1 = 6ed9eba1

Temp = 4C7D3964 + 7a4869dd + 2DE32873 + 69ff55ac + 6ed9eba1

Temp(24) = cd820d01

B = SHIFT LEFT BY 30 = 11101000100101111111010000100101 = **E897F425**

Final answer for T24:

T24

A - cd820d01

B - 2263e9cb

C - E897F425

D - 30E202BF

E - E8F5BBF5

Computing for T25 using previous iteration T24

T24

A - cd820d01

B - 2263e9cb

C - E897F425

D - 30E202BF

E - E8F5BBF5

T25

F = 2263e9cb XOR E897F425 XOR 30E202BF

F = caf41dee XOR 30E202BF

F(25) = fa161f51

A - cd820d01SHIFT 5 TIMES TO LEFT

A - 10110000010000011010000000111001

A - **B041A039**

Temp = Shift left(A, 5) + F + E + W25 +K1

W25 = 95fd53b0, K1 = 6ed9eba1

Temp = B041A039 + fa161f51 + E8F5BBF5 + 95fd53b0 + 6ed9eba1

Temp(25) = 9824bad0

B = SHIFT LEFT BY 30 =11001000100110001111101001110010 = **C898FA72**

Final answer for T25:

T25

A - 9824bad0

B - cd820d01

C - C898FA72

D - E897F425

E - 30E202BF