JACOB S. SANTOS **10/14/24**

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

Compute the 3rd iteration values of A, B, C, D in Round 1, 2, 3, and 4.

Round 1: 3rd iteration

iteration values of the 2nd iteration

A = 98badcfe, B = 7c13fe6d, C = db528b2a, D = efcdab89

Computing for 3rd iteration

F = (B and C) or ((not B) and D)

B and C = 7c13fe6d and db528b2a

= 58128a28

Not B = 83EC0192

Not B and D = 83EC0192 and efcdab89

= 83cc0180

F = 58128a28 or 83cc0180

F = **dbde8ba8**

FF = F + A + K2 + M2

= dbde8ba8 + 98badcfe + 242070db + 21646c72

FF = **ba1e45f3**

Temp = 1011 1010 0001 1110 0100 0101 1111 0011 (shift FF s1, 17)

= 1000 1011 1110 0110 0011 0111 0100 0011

Temp = **8BE7743C**

iteration values for 3rd iteration of round 1

A = efcdab89

B = B + Temp = 07fb72a9

C = 7c13fe6d

D = db528b2a

Round 2: 3rd iteration

iteration values of the 2nd iteration

A = 740b8a7b, B = 50c8c22b, C = 0f8a3fba, D = a8e6d4f8

Computing for 3rd iteration

F = (B and D) or (C and not(D))

B and D = 50c8c22b and a8e6d4f8

= 00c0c028

Not (D) = 57192B07

C and not(D) = 0f8a3fba and 57192B07

= 7082b02

F = 00c0c028 or 7082b02

F = **07c8eb2a**

g = (1 +(5*18)) mod 16 = 11

FF = F + A + K18 + M11

= 07c8eb2a + 740b8a7b + 265e5a51 + 00000000

FF = **a232cff6**

Temp = 1010 0010 0011 0010 1100 1111 1111 0110 (shift FF s2, 14)

= 1011 0011 1111 1101 1010 1000 1000 1100

Temp = **B3FDA88C**

iteration values for 3rd iteration of round 2

A = a8e6d4f8

B = B + Temp = 04c66ab7

C = 50c8c22b

D = 0f8a3fba

Round 3: 3rd iteration

iteration values of the 2nd iteration

A = 0bd3192e, B = 9e1a20a7, C = 6d06822a, D = 59a448cd

.

Computing for 3rd iteration

F = B xor C xor D

= 9e1a20a7 xor 6d06822a = f31ca28d

F = f31ca28d xor 59a448cd

F = **aab8ea40**

g = (5 + (3*34)) mod 16 = 11

FF = F + A + K34 + M11

= aab8ea40 + 0bd3192e + 6d9d6122 + 00000000

FF = **24296490**

Temp = 0010 0100 0010 1001 0110 0100 1001 0000 (shift FF s3, 16)

= 0110 0100 1001 0000 0010 0100 0010 1001

Temp = **64902429**

iteration values for 3rd iteration of round 3

A = 59a448cd

B = B + Temp = 02aa44d0

C = 9e1a20a7

D = 6d06822a

Round 4: 3rd iteration

iteration values of the 2nd iteration

A = a2a443e8, B = e070e4ca, C = ca3e0f8f, D = 7fe3004f

Computing for 3rd iteration

F = C xor (B or not(D))

Not D = 801CFFB0

B or not(D) = e070e4ca or 801CFFB0 = e07cfffa

F = ca3e0f8f xor e07cfffa

= **2a42f075**

g = (7*50) mod 16 = 14

FF = F + A + K50 + M14

= 2a42f075 + a2a443e8 + ab9423a7 + 00000060

FF = **787b5864**

Temp = 0111 1000 0111 1011 0101 1000 0110 0100 (shift FF s4, 15)

= 1010 1100 0011 0010 0011 1100 0011 1101

Temp = **AC323C3D**

iteration values for 3rd iteration of round 4

A = 7fe3004f

B = B + Temp = 8ca32107

C = e070e4ca

D = ca3e0f8f