**Deriving 2nd Round Key**

**Round 1 Key:** 0F 15 71 C9 47 D9 E8 59 0C B7 AD D6 AF 7F 67 98

|  |  |  |  |
| --- | --- | --- | --- |
| 0F | 47 | 0C | AF |
| 15 | D9 | B7 | 7F |
| 71 | E8 | AD | 67 |
| C9 | 59 | D6 | 98 |

W0 = [ 0F 15 71 C9 ]

W1 = [47 D9 E8 59]

W2 = [0C B7 AD D6]

W3 = [AF 7F 67 98]

RotWord(w3) = x1

RotWord([AF 7F 67 98]) = [7F 67 98 AF] = x1

SubWord(x1) = y1

SubWord([7F 67 98 AF]) = [D2 85 46 79] = y1

Rcon(1) = 01 00 00 00

z1 = y1 ⊕ Rcon(1)

z1 = [D2 85 46 79] ⊕ [01 00 00 00] = [D3 85 46 79]

W4 = z1 ⊕ W0 = [D3 85 46 79] ⊕ [ 0F 15 71 C9 ] = [DC 90 37 B0]

W5 = W4 ⊕ W1 = [DC 90 37 B0] ⊕ [ 47 D9 E8 59] = [9B 49 DF E9]

W6 = W5 ⊕ W2 = [9B 49 DF E9] ⊕ [ 0C B7 AD D6] = [97 FE 72 3F]

W7 = W6 ⊕ W3 = [97 FE 72 3F] ⊕ [ AF 7F 67 98 ] = [38 81 15 A7]