primary key K

$$K = \begin{bmatrix} 2b & 28 & ab & 09 \\ 7e & ae & f7 & cf \\ 15 & d2 & 15 & 4f \\ 16 & a6 & 88 & 3c \end{bmatrix}$$

$w_0 = [2b, 7e, 15, 16]^T$

$w_1 = [28, ae, d2, a6]^T$

$w_2 = [ab, f7, 15, 88]^T$

$w_3 = [09, cf, 4f, 3c]^T$

Now we have to compute $w4, w5, w6, w7$

Formula

$w_i = w_{i-4} \oplus G(w_{i-1})$ if $i \equiv 0 \pmod 4$

$w_i = w_{i-4} \oplus w_{i-1}$ if $i \not\equiv 0 \pmod 4$

$G(w)$ → will be applied only when the index i is a multiple of 4 ($w_4, w_8, w_{12} \ldots$)

involves Three step

1. Rot word
2. Sub word (using S box)
3. X-OR with RC1 = (01 00 00 00)

Formula:

$w4 = w0 \oplus g(w3)$

$w5 = w1 \oplus w4$

$w6 = w2 \oplus w5$

$w7 = w3 \oplus w6$

Step 1 → take w3

$w3 = [09, cf, 4f, 3c]$

Step 2 → Rotword(w3)

Rotate upword

$[cf \quad 4f \quad 3c \quad 09]$

Step 3 → subword() using S box

cf → row C, col F → 8a

for all byte

cf → 8a

4f → dc → 84

3c → eb

09 → 83 → 01

∴ subword = [8a, dc, eb, 83]

Step 4: XOR with RC1 - (01 00 00 00)

[8a dc eb 83]
⊕
[01 00 00 00]

8a 1000 1010
01 0000 0001
⊕
1000 1011
↓ ↓
8 b

=[8b dc eb 83]

∴ g(w3) = [8b dc eb 83]

Compute w4

w0 = [2b 7e 15 16]

g(w3) = [8b dc eb 83]

(XOR)

w4 = [a0 a2 fe 95]

Compute w5

w1 = [28, ae, d2, a6]

w4 = [a0, a2, fe, 95]

(XOR)

w5 = [88, 0c, 2c, 33]

Compute w6

$w2 = [ab, f7, 15, 88]$

$w5 = [88, 0c, 2c, 33]$

XOR

$w6 = [23, fb, 39, bb]$

Compute w7

$w3 = [09, cf, 4f, 3c]$

$w6 = [23, fb, 39, bb]$

XOR

$w7 = [2a, 34, 76, 87]$

$$[w_4\ w_5\ w_6\ w_7] \equiv \begin{matrix} a0 & fa & fe & 17 \\ 88 & 54 & 2c & b1 \\ a3 & a3 & 39 & 39 \\ aa & 6c & 76 & 05 \end{matrix}$$