

**Input :** Round Key( $k_0, k_1, \dots, k_{15}$ ), Round(라운드 수)

**Output:** Master Key ( $rk(0), rk(1), rk(2), rk(3)$ )

```
1:  $rk((Round+1) \times 4 - 4) \leftarrow word(k_0, k_1, k_2, k_3)$ 
2:  $rk((Round+1) \times 4 - 3) \leftarrow word(k_4, k_5, k_6, k_7)$ 
3:  $rk((Round+1) \times 4 - 2) \leftarrow word(k_8, k_9, k_{10}, k_{11})$ 
4:  $rk((Round+1) \times 4 - 1) \leftarrow word(k_{12}, k_{13}, k_{14}, k_{15})$ 
5: for  $i = (Round+1) \times 4 - 1$  down to 4 do
6:    $t \leftarrow rk(i - 1)$ 
7:   if  $i \bmod 4 = 0$  then
8:      $t \leftarrow RotWord(t)$ 
9:      $t \leftarrow SubWord(t)$ 
10:     $t \leftarrow t \oplus word(Rcon(i/4), 0, 0, 0)$ 
11:   end if
12:    $rk(i - 4) \leftarrow rk(i) \oplus t$ 
13: end for
```