

Given: The initial AES key is 128 bits of all 1s. So:

$$W(0) = W(1) = W(2) = W(3) = \text{FF FF FF FF}$$

**(1) Compute  $W(4)$  to  $W(7)$ :**

$$W(4) = W(0) \oplus T(W(3))$$

Using the AES key schedule, this results in:

$$W(4) = \text{E8 E9 E9 E9}$$

$$W(5) = W(1) \oplus W(4) = \text{17 16 16 16}$$

$$W(6) = W(2) \oplus W(5) = \text{E8 E9 E9 E9}$$

$$W(7) = W(3) \oplus W(6) = \text{17 16 16 16}$$

So:

$$W(4) = W(6) = \text{E8 E9 E9 E9}$$

$$W(5) = W(7) = \text{17 16 16 16}$$

Also:

$$W(5) = \sim W(4) \quad (\text{bitwise complement})$$

**(2) Show  $W(10) = W(8)$  and  $W(11) = W(9)$ :**

From the key schedule:

$$W(8) = W(4) \oplus W(7)$$

$$W(9) = W(5) \oplus W(8)$$

$$W(10) = W(6) \oplus W(9)$$

$$W(11) = W(7) \oplus W(10)$$

Since:

$$W(5) \oplus W(6) = \text{FF FF FF FF},$$

and XORing the same value twice cancels it out:

$$W(10) = W(8)$$

$$W(11) = W(9)$$

**Confirmed.**