# AES Key Expansion

**K[n] : W[i] = K[n-1] : W[i] XOR K[n] : W[i-1]**

Ex: W[1] = K[1-1] : W[1] XOR K[1] : W[1-1]

**K[n] : W0 = K[n-1] : W0 XOR SubByte ( K[n] : W3 >>8) XOR Rcon[i]**

Just for W0

K1 = 97 C9 2F 1B (words hexa) every word 8 bits

**Example:**

K1:

W0 = 0F 15 71 C9

W1 = 47 D9 E8 59

W2 = 0C B7 AD

W3 = AF 7F 67 98

**Find K2:**

**اول شيب نطلع W0 فبالتالي بنطبق ع القانون الثاني.**

**K2: W0 = K[n-1] : W0 XOR SubByte ( K[1] : W3 >>8) XOR Rcon[2]**

**ليش قلنا Rcon[2] لأننا قلنا K[2] قيمة ال I تساوي ٢**

0F 15 71 C9 **XOR SubByte(** AF 7F 67 98 >> 8) **XOR Rcon[2]**

0F 15 71 C9 **XOR SubByte(**7F 67 98 AF ) **XOR Rcon[2]**

**بعدين نسوي subByte**

0F 15 71 C9 **XOR** D2 85 46 79 **XOR Rcon[2]**

**Rcon[2] نشوفها من الجدول**

0F 15 71 C9 **XOR** D2 85 46 79 **XOR 02 00 00 00**

**بعدين احولهم لـ Binary**

**(00001111 00010101 01110001 11001001)XOR (11010010 10000101 01000110 01111001) XOR ( 00000010 00000000 00000000 00000000)**

**11010010 10000101 01000110 01111001= step of subbyte**

**00000010 00000000 00000000 00000000= Rcon[2]**

XOR

**11010000 10000101 01000110 01111001= result**

**00001111 00010101 01110001 11001001 = W0**

XOR

**11011111 10010000 00110111 10110000 = final result**

**بعدها احولها الى Hexa**

**K2: W0= DF 90 37 B0**

**و اكمل باقي الـ words**



Good Luck ☺

**K2: W1= K[1] : W[1] XOR K[2] : W[0]**

47 D9 E8 59 **XOR** DF 90 37 B0

احولها الى Binaryبعدين اسوي عملية XOR

**K2: W0= DF 90 37 B0**

**K2: W1= 98 49 DF E9**

**و هكذا اطلع w2 and w3**



Good Luck ☺