CIS 3362 10/6/23

```
KeyExp (byte key[16], word w[44]) {     // key = input, w = output; word -> 4 bytes
    word tmp;
    // Init R0 key to orig input key
    for (i=0; i<4; i++)
        w[i] = (key[4i], key[4i+1], key[4i+2], key[4i+3])
    for (i=4; i<44; i++) {   // fill in new keys
                             // 1 word at a time
        tmp = w[i-1];  // tmp is previous word
        if (i%4 == 0)
            tmp = SubWord(RotWord(tmp)) ⊕ (Rcon[i/4], 00, 00, 00)   // Rcon stores 1 byte
        w[i] = w[i-4] ⊕ tmp  // if i%4 != 0, tmp = w[i-1]
    }
```

RotWord(23 AF 07 15) — left cyclic shift 1 byte (word = 8 hex)

= AF 07 15 23

SubWord (AF 07 15 23)

↓ ↓ ↓ ↓

i = 16

Sbox(AF), Sbox(07), Sbox(15), Sbox(23)

Output Subword	79	C5	59	26
	08	00	00	00 Rcon(4)
⊕	71	C5	59	26

Example Question

Calculate $w[32]$, $w[31] = F3\ CD\ 01\ 75$

$w[28] = B7\ 94\ 5E\ 22$

i	temp	After RotWord	After SubWord	Rcon[i/4]	After XOR Rcon
32	F3 CD 01 75	CD 01 75 F3	BD 7C 9D 0D	80 00 00 00	3D 7C 9D 0D

w[i-4]	tmp ⊕ w[i-4]
B7 94 5E 22	3D 7C 9D 0D B7 94 5E 22 **8A E8 C3 2F**