CIS 3362 10/4/24

AES Key Schedule

8 x 16 = 128 bits

32 bits (4 bytes)

KeyExp(byte key[16], word w[44])

w[0]..w[3] → Round key 0

w[4]..w[7] → Round key 1

Round 0 key is the original key:

```
word tmp;
for (int i=0; i<4; i++)
    w[i] = (key[4i], key[4i+1], key[4i+2], key[4i+3])
```

(concat the next 4 bytes)

```
for (int i=4; i<44; i++) {
    tmp = w[i-1]
```

Usually skipped:

```
    if (i%4 == 0) // Once a round (i=4,8,12,...)
        tmp = SubWord(RotWord(tmp)) ⊕ (Rcon[i/4],0,0,0)
```

SubWord: S box

RotWord: Left cyclic rotation by 1 byte

```
    w[i] = w[i-4] ⊕ tmp
}
```

w[23] = ab 73 29 cd

w[20] = 65 90 bb a4

Goal w[24]

temp	RotWord	SubWord (→ w1 Sbox)	Rcon	After XOR
ab 73 29 cd	73 29 cd ab	8f a5 bd 62	20 00 00 00	af a5 bd 62

AF A5 BD 62

⊕ 65 90 BB A4

CA 35 06 C6

2nd example

w[i-4] w[31] = 01 23 45 67

w[i-1] w[34] = 89 ab cd ef ①

w[35] = 88 88 88 88