CIS 3362 10/11/25

1. MixCol Program
2. Mix Cols by Hand
3. Key Schedule

a = 17 b = 6 16b + b

r → 0110 a = 10001

res = 000

cur = 0110

when lsb is on res = res ^ cur, add in this many copies of b

cur = leftshift(cur) → multiplies cur by 2 essentially

row 1 col 1

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

D3
7E
B5
29

AES Poly

$x^8 + x^4 + x^3 + x + 1$

02 × D3 = BD

03 × 7E = 82

01 × B5 = B5

01 × 29 = 29

A3

02 × (11010011) = 10100110 ⊕ 11011

10111101

B D

1100
1111
0011

03 × (01111110)

= (02 + 01) × (01111110) = 01×7E: 01111110 → ⊕ 11111100 → 02×7E

10000010

8 2

AES Key Schedule

128 bit key input
creates 10 round keys
initial XOR is w/ the original key.

Notes for key expansion

w[0..3] = orig key
w[4..7] = R1 key
w[8...11] = R2 key
⋮
w[40..43] = R10 key

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

~~temp~~
w[0..3] = key[0..15] // copy key into R0 key

for (i=4; i<44; i++)
temp = w[i-1]
if (i%4 == 0)
temp = SubWord(RotWord(temp) ⊕ (Rcon[i/4] 000000)

w[i] = w[i-4] ⊕ temp

R1 key ends in ... 49 36 B2 E7 (w[7]) w[10]

~~0129~~
R2 key is AF 01 68 74 42 36 B8 89 EF 29 36 24

find w[11] →

  49 36 B2 E7
⊕ EF 29 36 24

  A6 1F 84 C3

Now let's find w[12]

w[11]	ROTWORD	SUBWORD	RCON[i/4]
A6 1F 84 C3	1F 84 C3 A6	C0 5F 2E 24	04 00 00 00

XOR

C4 5F 2E 24

Now to XOR w/ w[i-1]

temp = C4 5F 2E 24

⊕ w[i-1] = A6 1F 84 C3

w[12] = 62 40 AA E7