

CIS 3362 10/4/23

AES

① Mix Cols

16 bytes

↓↓↓

1 byte

10110100 (represents a poly)

$$x^7 + x^5 + x^4 + x^2$$

This a polynomial in the field GF_8 .

each coeff is either 0 or 1 $(\text{mod } 2)$

8 means mod each poly by a degree 8 polynomial so the result is degree 7 or less.

$$\text{AES poly mod} = x^8 + x^4 + x^3 + x + 1$$

irreducible polynomial

$$(x^3 + x^2 + 1)(x^2 + x + 1) = x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^2 + x + 1$$

$x^5 + x + 1$

All AES calculations are using this polynomial field w/ that given mod polynomial.

How to "mod"

$$x^8 \bmod x^8 + x^4 + x^3 + x + 1 = x^4 + x^3 + x + 1$$

$$x^8 \equiv (x^4 + x^3 + x + 1) \bmod x^8 + x^4 + x^3 + x + 1$$

Mix Col

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 9D & EC \\ 46 & E7 & 4A & C3 \\ AB & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} \quad \quad \quad \quad \end{bmatrix}$$

r1c1 $02 \times 87 + 03 \times 6E + 01 \times 46 + 01 \times AB$

r1c2 $02 \times F2 + 03 \times 4C + 01 \times E7 + 01 \times 8C$

r3c4 $01 \times 97 + 01 \times EC + 02 \times C3 + 03 \times 95$

mean $(x) \times (x^7 + x^2 + x + 1) =$

$$\begin{array}{r} \text{init ans} \\ 00001110 \\ \oplus 11011 \\ \hline 00010101 \quad (15) \end{array}$$

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

$03 \times 6E =$

$$\begin{array}{r} 01101110 \quad 6E \\ \oplus 11011100 \quad 2 \times 6E \\ \hline 10110010 \quad (B2) \end{array}$$

$(x+1)$
 $(02+01) \times 6E$
 $02 \times 6E + 01 \times 6E$

$$15 \oplus B2 \oplus 46 \oplus AB$$

$$A7 \oplus EC = 47$$

$$\boxed{B01} \quad \boxed{502} \quad \boxed{404} \quad \boxed{A0E} \quad \boxed{700}$$

$$r3c4 \quad \boxed{01 \times 97} + \boxed{01 \times EC} + 02 \times C3 + 03 \times 95$$

$$02 \times C3 = 02 \times (11000011) = \begin{array}{r} \text{\$}10000110 \\ \oplus \quad \rightarrow 11011 \\ \hline 10011101 \quad (9D) \end{array}$$

$$03 \times 95 = 03 \times (10010101) =$$

$$\begin{array}{r} 10010101 \quad 95 \\ \text{\$}00101010 \quad 2 \times 95 \\ \oplus \quad 11011 \\ \hline 10100100 \quad (A4) \end{array}$$

$$\begin{aligned} & \boxed{97 \oplus EC} \oplus 9D \oplus A4 = \\ & \boxed{97 \oplus 9D} \oplus \boxed{EC \oplus A4} \\ & 0A \oplus 48 = 42 \end{aligned}$$

full ans

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

So you can practice!

S-box

S-box(A7)
= 5C

go to row A
go to col 7
find the entry

What is $07 \times B6$ in AES field

$$07 = 00000\underline{111} \times 10110110$$

$$\begin{array}{r} 10110110 \\ \oplus 01101100 \\ \hline 11011 \\ \hline 11000001 \end{array} \quad \begin{array}{l} B6 \\ 2 \times B6 \\ (C1) \end{array}$$

$$\begin{array}{r} \downarrow \text{overflow} \\ \boxed{\cancel{10}}11011000 \\ \hline 110110 \\ \hline 11101110 \\ \hline 1100 \end{array} \quad \begin{array}{l} (+) \\ (EE) \end{array}$$

2F

$$x^{38} \equiv x^4 + x^3 + x + 1$$

$$\begin{aligned} x^9 &= x \cdot x^8 = x(x^4 + x^3 + x + 1) \\ &= x^5 + x^4 + x^2 + x \end{aligned}$$