CIS 3362 10/7/26

Field (called) $GF(2^8)$ which is used in AES.

Branch of Math - Group Theory
(note: A field is a special type of Group)

→ Polynomials only coeff allowed 0 and 1

→ Deg Poly < 8

AES mod poly $= x^8 + x^4 + x^3 + x + 1$

↳ Irreducible no 2 poly f, g exist s.t $f(x) \cdot g(x) =$ AES poly and degree$(f) > 0$ and degree$(g) > 0$
essentially similar to a prime #.

Add

$(x^6 + x^4 + x^3) + (x^5 + x^4 + x)$

$x^6 + x^5 + 2x^4 + x^3 + x$ take all coeff mod 2

$\equiv x^6 + x^5 + x^3 + x \implies$ ADD + SUB SAME

MULT

$(x^4+x) \cdot (x^4+x^2+1)$

$= x^8 + x^6 + x^4$
$x^5 + x^3 + x$

$f(x) + g(x) \mod h(x)$
$\equiv f(x) \mod h(x) + g(x) \mod h(x)$

What is $x^8 \mod x^8+x^4+x^3+x+1$?

$$x^8+x^4+x^3+x+1 \;\big|\; x^8$$
$$- \; x^8+x^4+x^3+x+1$$
$$\overline{\qquad\qquad x^4+x^3+x+1}$$

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

$\Rightarrow \equiv (x^4+x^3+x+1) + x^6+x^4+x^5+x^3+x$
$\equiv x^6+x^5+1$

What about
$x^{10} \mod (x^8+x^4+x^3+x+1)$?

$x^{10} \equiv x^8 \cdot x^2 \equiv (x^4+x^3+x+1)x^2 = \boxed{x^6+x^5+x^3+x^2}$

$x^4 + x$ is written as $0001\ 0010_2 = 12_{16}$

$x^6 + x^4 + x^3 \longrightarrow 0101\ 1000_2 = 58_{16}$

AES

128 bit blocks, 192 bit blocks or 256 bit blocks

Plain is 128 bits, key is 128 bits

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Each square is a byte (8 bits)

Order bytes:

$a_{00}, a_{10}, a_{20}, a_{30}, a_{01}, a_{11} \ldots$

10 ROUNDS

1. $S = AddRoundKey(P, K_0)$ → bitwise XOR
2. for $i = 1$ to 9:
   - 2a. $S = SubBytes(S)$ → $a_{00} = S(a_{00})$, $a_{10} = S(a_{10})$, ...
   - 2b. $S = ShiftRows(S)$
   - 2c. $S = MixCols(S)$
   - 2d. $S = AddRoundKey(S, K_i)$
3. 3a. $S = SubBytes(S)$
   - 3b. $S = ShiftRows(S)$
   - 3c. $S = AddRoundKey(S, K_{10})$
4. Return S

S-box

~~Col label~~

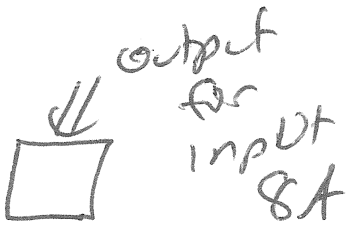
Row labels → 00 01 02 .. 0A 0F

↓

00
10
→ 20
80

1st HEX CHAR of Input

F0



$Sbox(27) = CC$

$Sbox(A1) = 32$

$Sbox(5C) = 4A$

Shift Rows

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

→

a_{00}	a_{01}	a_{02}	a_{03}
a_{11}	a_{12}	a_{13}	a_{10}
a_{22}	a_{23}	a_{20}	a_{21}
a_{33}	a_{30}	a_{31}	a_{32}

i^{th} row cyclic left shift of i byte

Mix Cols

AES Mix Cols Matrix =

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

STATE MATRIX

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} 01 & 89 & AS & 06 \\ 23 & AB & B2 & 44 \\ 45 & CD & 89 & C3 \\ 67 & EF & 73 & 29 \end{bmatrix}$$

Entry in Row I COL J is the Dot Product of Row I is matrix and Column J in second matrix

Entry in Row 4 Col 3 ?

$= 03 \times AS + 01 \times B2 + 01 \times 89 + 02 \times 73$

$(x+1) \times (x^7+x^5+x^2+1)$

01110011

$x \cdot (x^6+x^5+x^4+x+1)$

02 x byte → left shift

11100110

EG

$03 \times A5 = 02 \times A5 + \boxed{01 \times A5}$ (A5)

$02 \times A5 = 1010\ 01010 \equiv 0100\ 1010$

$\oplus\ 1\ 1011$

$0101\ 0001$

$x^8 \equiv (x^4 + x^3 + x + 1) \bmod \text{AESPOLY}$

$01 \times B2 = B2$

$01 \times 89 = 89$

$02 \times 73 = 0111\ 00110 = E6$

$\boxed{51}$

$03 \times A5 = 51 + A5 = F4$

$0101\ 0001$
$1010\ 0101$
$1111\ 0100$

$Ans = (B2 \oplus 89) \oplus (E6 \oplus F4)$

$= (3B) \oplus (12) = \boxed{29}$

(3B: XOR check)

Row 3 Col 2

$01 \times 89 + 01 \times AB + 02 \times C1 + 03 \times EF$

$\boxed{89}$ $\boxed{AB}$

$89 \oplus AB = 22$

$81 \oplus 2A = AB$

$\boxed{89}$

FINAL ANS

1001
1011

$1100\ 11010$

10011010
$\oplus\ 11011$
10000001

$\boxed{81}$

(EF) $01 \times EF = \boxed{1110\ 1111}$

$02 \times EF = 11101\ 1110$

$1101\ 1110$
$\oplus\ 11011$
11000101

$\boxed{C5}$

C5
$\oplus$ EF
$\boxed{2A} \rightarrow 03 \times EF$