CIS 3362 10/4/24

AES

bytes as polynomials in $GF(2^8)$ $x^8+x^4+x^3+x+1$

coeff 0/1 , + , x

Input: 128 bits (16 bytes) P → state matrix

1. $S = AddRoundKey(P, K_0)$
2. for r = 1 to 9 (10 rounds, last round diff)
   a. $S = SubBytes(S)$
   b. $S = ShiftRows(S)$ ↔ can be interchanged
   c. $S = MixCols(S)$
   d. $S = AddRoundKey(S, K_i)$
3. Round 10
   $S = SubBytes(S)$
   $S = ShiftRows(S)$
   $S = AddRoundKey(S, K_{10})$
4. Return S

Visualize AES State Matrix

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

each box stores a byte

order of filling in boxes is

$S_{00}, S_{10}, S_{20}, S_{30}, S_{01}, S_{11}, S_{21}, S_{31}$

Add Round key

37			
ae			
c4			
d5			

$\oplus$

65			
34			
fa			
7c			

$=$

52			
9a			
3e			
a9			

$37 \oplus 65 = 52$

S

if $X \oplus Y = Z$, then $X = Y \oplus Z$

$Y \oplus Y = 0$

$5 \oplus c$

0101

1100

$1001 = 9$

Code ^

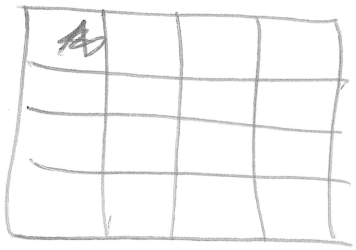
SubBytes

S(00) = 63 (row 0, col 0)

S(27) = cc (row 2, col 7)

S(af) = 79 (row 10, col 15)

Shift Rows



0 ←	S_{00}	S_{01}	S_{02}	S_{03}
1 ←	S_{10}	S_{11}	S_{12}	S_{13}
2 ←	S_{20}	S_{21}	S_{22}	S_{23}
3 ←	S_{30}	S_{31}	S_{32}	S_{33}

→

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

Left Cyclic Shift of i bytes on row i

Mix Cols

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} 01 & 89 & 73 & d5 \\ 23 & ab & 4c & e8 \\ 45 & cd & cb & b2 \\ 67 & ef & f0 & a1 \end{pmatrix}$$

fixed mat

$r1c1 = 02 \times 01 + 03 \times 23 + 01 \times 45 + 01 \times 67$

$r2c4 = 01 \times d5 + 02 \times e8 + 03 \times b2 + 01 \times a1$

$r3c2 = 01 \times 89 + 01 \times ab + 02 \times cd + 03 \times ef$

$03 = (x+1)$ → 00000011

$23 = (x^5 + x + 1)$ → 00100011

$(x+1)(x^5+x+1) = x^6 + x^5 + x^2 + x + x + 1$

$= x^6 + x^5 + x^2 + 1$

0110 0101

65

$23 \times 2 =$ (left shift) 01000110

$23 \times 1 =$ 00100011

01100101

02×01

0000 0001

0000 0010

02

r1c1 :

02×01	0000 0010	02
03×23	0110 0101	~~68~~
01×45	0100 0101	~~48~~
01×67	⊕ 0110 0111	⊕ ~~67~~
	0100 0101	45
	45	

---

r2c4

01×D5 = 1101 0101

02×E8 = 1100 1011

1110 1000 << 1

= 1110 10000 = $x^8+x^7+x^6+x^4 = x^7+x^6+x^4+x^3+x+1$

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

11101 0000 ✓

= 1101 0000 ✓
⊕ 1 1011

11001011 = CB

03×B2 =

B2 = 1011 0010] 01×B2

02×B2 = 0110 0100] 02×B2
⊕ 1 1011

1100 1101 (CD)

$01 \times 91 = 1001\ 0001$

ADD ALL TOGETHER

$01 \times D5 = D5$

$02 \times E8 = EB$

$03 \times B2 = CBD$

$01 \times 91 = \oplus\ 9\ 1$

42

$0D \times F5 = E5$

$1101 \times (1111\ 0101)$

$x1$ 1111 0101

$x100$ 11 1101 0100

$x1000$ 111 1010 1000

1001000 1001

1000 1001

0110 1100

1110 0101

$x^{10} = x^8 \cdot x^2 = (x^4 + x^3 + x + 1)\, x^2$

$x^{10} \bmod = x^6 + x^5 + x^3 + x^2$

110
101
1
010

5
6
1

$$x^8+x^4+x^3+x+1 \;\Big|\; 1$$

$$x^8$$

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

$$-x^4-x^3-x+1$$

$$= x^4+x^3+x+1$$

0001 1011