

shift rows transformation

Row 0: no shift

Row 1: 1-byte left

Row 2: 2-byte left

Row 3: 3-byte left

state

→ Shift Row

63	C9	FE	30
F2	F2	63	26
C9	C9	7D	D4
FA	63	82	D4

63	C9	FE	30
F2	63	26	F2
7D	D4	C9	C9
D4	FA	63	82

max column

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

87	F2	4D	57
6E	4C	90	EC
46	F7	4A	C3
A6	8C	D8	95

$$02 \rightarrow 0000\ 0010 = x^7 + x^3 + x + 1$$

$$87 \rightarrow 1000\ 0111 = x^8 + x^4 + x^3 + x + 1$$

$$02 * 87 = x(x^7 + x^3 + x + 1) \quad | x^8 \rightarrow x^4 + x^3 + x + 1$$

$$= x^8 + x^4 + x^3 + x^2 + x$$

$$= x^4 + x^3 + x^2 + x^2 + x + x + 1$$

irreducible polynomial theorem

$$= x^4 + x^2 + 1 = 0001\ 0101$$

$$03 \rightarrow 0000\ 0011 = (x+1)$$

$$6E \rightarrow 0110\ 1110 = (x^6 + x^5 + x^3 + x^2 + x)$$

$$03 * 6E = (x+1)(x^6 + x^5 + x^3 + x^2 + x)$$

$$= x^7 + x^6 + x^4 + x^3 + x^2 + x + x^6 + x^5 + x^3 + x^2 + x$$

$$= x^7 + x^5 + x^4 + x = 10110010$$

$$01 * 46 = 46 = 0100 \text{ D110}$$

$$01 * A6 = A6 = 1010 \text{ 0110}$$

odd-1 $\rightarrow 1$
even-1 $\rightarrow 0$

$$02 * 87 = 00010101$$

$$03 * 6E = 10110010$$

$$01 * 46 = 01000110$$

$$01 * A6 = 1010 \text{ 0110}$$

$$\underline{01000111}$$

XOR

$$= 01000111$$

For 2nd element

$$000 \\ 01 * 87 = 87 = 10000111$$

$$02 = 000000010 = x^6 + x^5 + x^3 + x^2 + x$$

$$03 = 000000110 = (x^6 + x^5 + x^4 + x^3 + x^2 + x)$$

$$6E = 01101110 = x^7 + x^6 + x^4 + x^3 + x^2$$

$$02 * 6E = x(x^6 + x^5 + x^4 + x^3 + x^2 + x) = 11011100$$

$$03 \rightarrow 00000011 = (x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x)$$

$$46 \rightarrow 01000110 = (x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x)$$

$$03 * 46 = (x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x) = 11001110 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$$

97		
32		
94		
ED		

$$01 * A6 = A6 = 1010 \ 0110$$

Now

$$01 * 87 = 1000 \ 0111$$

$$02 * 6E = 1101 \ 1100$$

$$03 * 46 = 1100 \ 1010$$

$$01 * A6 = 1010 \ 0110$$

} XOR

$$(0011 \ 0111)_2$$

$$= 37$$

For 3rd element

$$01 * 87 = 87 = 1000 \ 0111$$

$$01 * 6E = 6E = 0110 \ 1110$$

$$02 \rightarrow 0000 \ 0010 = x^2$$

$$02 \rightarrow 0000 \ 0010 = x^6 + x^2 + x$$

$$46 \rightarrow 0100 \ 0110 = x^6 + x^3 + x^2 = 10001100$$

$$02 * 46 = x(x^6 + x^2 + x) = x^7 + x^3 + x^2$$

$$03 \rightarrow 0000 \ 0011 = x+1$$

$$03 \rightarrow 0000 \ 0011 = x^7 + x^5 + x^2 + x$$

$$A6 \rightarrow 1010 \ 0110 = x^7 + x^5 + x^2 + x$$

$$03 * A6 = (x+1)(x^7 + x^5 + x^2 + x) = x^8 + x^6 + x^3 + x^2$$

$$= x^4 + x^3 + x^1 + x^6 + x^5 + x^2 +$$

$$x^7 + x^5 + x^2 + x + \emptyset$$

$$\begin{aligned}
 &= x^7 + x^6 + x^5 + x^4 + 1 \\
 &= 11110001
 \end{aligned}$$

Now

$$\begin{array}{l}
 01 * 87 \rightarrow \begin{array}{cc} 1000 & 0111 \\ 0110 & 1110 \end{array} \\
 01 * 6E \rightarrow \begin{array}{cc} 1000 & 1100 \\ 1111 & 0001 \end{array} \\
 02 * 46 \rightarrow \\
 03 * A6 \rightarrow
 \end{array}
 \quad \text{XOR} \quad
 \begin{array}{c}
 (1001 \ 0100)_2 = (94)_{10}
 \end{array}$$

For 4^{nth} element

$$\begin{array}{l}
 x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 0 \\
 0000 \quad 0011 = (x+1) \\
 0111 = x^7 + x^2 + x + 1
 \end{array}$$
~~$$\begin{array}{l}
 03 * 87 = 03 \rightarrow \begin{array}{cc} 0000 & 0011 \\ 1000 & 0111 \end{array} \\
 87 \rightarrow 1000
 \end{array}$$~~

$$\begin{aligned}
 03 * 87 &= (x+1)(x^7 + x^2 + x + 1) \\
 &= x^8 + x^3 + x^2 + x + x^7 + x^2 + x + 1 \\
 &= (x^8 + x^3 + x^2 + x + 1) + (x^7 + x^2 + x + x^7 + x^2 + x + 1) \\
 &= 10010010
 \end{aligned}$$

$$01 * 6E = 6E = 0110\ 1110$$

$$01 * 46 = 46 = 0100\ 0110$$

$$02 \rightarrow 0000 \quad 0010 = x^7 + x^5 + x^2 + x$$

$$A6 \rightarrow 1010 \quad 0110 = (x^7 + x^5 + x^2 + x)$$

$$02 * A6 = x(x^7 + x^5 + x^2 + x)$$

$$= x^8 + x^6 + x^3 + x^2$$

$$= x^4 + x^3 + x + 1 + x^6 + x^3 + x^2$$

$$= x^6 + x^4 + x^2 + x + 1$$

$$= 01010111$$

Now

$$03 * 87 \rightarrow \begin{array}{r} 10010010 \\ 0110\ 1110 \end{array}$$

$$01 * 6E \rightarrow \begin{array}{r} 0100\ 0110 \end{array}$$

$$01 * 46 \rightarrow \begin{array}{r} 0101\ 0111 \end{array}$$

$$02 * A6 \rightarrow \begin{array}{r} (1110\ 1101)_2 \end{array}$$

$$= ED$$

XOR

xOR

* 80

* 10

97		
37		
04		
ED		

$$x^2 + x + x$$

$$6, 1, 4, 2, 3 + x^2$$