AES Mix columns

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

predefine Matrix

$*$

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

$=$

$S'_{0,0}$	$S'_{0,1}$	$S'_{0,2}$	$S'_{0,3}$
$S'_{1,0}$	$S'_{1,1}$	$S'_{1,2}$	$S'_{1,3}$
$S'_{2,0}$	$S'_{2,1}$	$S'_{2,2}$	$S'_{2,3}$
$S'_{3,0}$	$S'_{3,1}$	$S'_{3,2}$	$S'_{3,3}$

For Ex:-

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

State Array.

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

predefine Matrix

$*$

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

State Array

$=$

?	?	?	?
?	?	?	?
?	?	?	?
?	?	?	?

New State Array

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} ? & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}$$

$$\{02\} * \{87\} \oplus \{03\} * \{6E\} \oplus \{01\} * \{46\} \oplus \{01\} * \{A6\}$$

$$02 = \underbrace{00000010}$$

$$\hookrightarrow x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + x^0$$

$$0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 = x$$

$$87 = 10000111$$

$$\hookrightarrow x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + x^0$$

$$1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1$$

$$= x^7 + x^2 + x^1 + x^0$$

$$= x^7 + x^2 + x + 1$$

Now Multiply {02} & {87}.

Both polynomial terms represented to be multiplied and after multiplication the result must also belong to the set of polynomials. If not replace with irreducible polynomial.

$GF(2^3) = GF(8)$ i.e 8 bits are used.

Use irreducible polynomial thm, $GF(2^3)$

$$\underline{x^4 + x^3 + x + 1}$$

So $x^8 = \underline{x^4 + x^3 + x + 1}$

Ihy $GF(2^8) = GF(256)$ i.e. 256 bits are used.

For that irreducible polynomial is $\underline{x^8 + x^4 + x^3 + x + 1}$

Now multiply

$\{02\} * \{87\} = x * (x^7 + x^2 + x + 1)$

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

Now since x^8 does not belong to the finite field bcz set of polynomial contains $x^7 - - - - x^0$.

So replace x^8 with $p(x) = x^4 + x^3 + x + 1$

so $= x^4 + \cancel{x^3} + \cancel{x} + 1 + \cancel{x^3} + x^2 + \cancel{x}$

cancel out similar terms in polynomial addition

$\boxed{\{02\} * \{87\} = x^4 + x^2 + 1}$

Now represent in binary.

$\{02\} * \{87\} = \underline{00010101}$

Ex

$\{03\} * \{6E\}$

$\{03\} = 0000\ 0011 = x+1$

$\{6E\} = 0110\ 1110 = x^6+x^5+x^3+x^2+x$

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

$= x^7 + \cancel{x^6} + x^4 + \cancel{x^3} + \cancel{x^2} + \cancel{x^6}$
$+ x^5 + \cancel{x^3} + \cancel{x^2} + x$

Cancel out similar terms

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

Here no need to replace with irreducible polynomial bcz result fits into the set of $\{x^7 \ldots x^0\}$

$\{03\} * \{6E\} = 1011\ 0010$.

Next,

$\{01\} * \{46\} = 46 = 01000110$

Ily $\{01\} * \{A6\} = A6 = 10100110$

Now perform XOR opn.

$02 * 87 = 00010101$

10110010

01000110

10100110

01000111

4 7

2	8	1	1
1	2	3	1
1	1	2	3
3	1	1	2

$*$

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

$=$

47			

Now find out next value By multiplying second row with 1st column of state & predefine matrix array.

$\{01\} * \{87\} * \{02\} * \{6E\} \oplus \{03\} * \{46\} \oplus \{01\} * \{A6\}$

87

$= \underbrace{10000111}$

$02 = 0000\,0010 = x$

$6E = 0110\,01110 = x^6 + x^5 + x^3 + x^2 + x$

$\{02\} * \{6E\} = x * (x^6 + x^5 + x^3 + x^2 + x)$

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

$= 11011100$

lly

$\{03\} * \{46\} \rightarrow 01000110 = x^6 + x^2 + x$

$\hookrightarrow 00000110 = x + 1$

$\{03\} * \{46\} = (x+1) * (x^6 + x^2 + x)$

$= x^7 + x^3 + \cancel{x^2} + x^6 + \cancel{x^2} + x$

$= x^7 + x^6 + x^3 + x.$

11001010

$\{01 * A6\} = A6 = 10100110$

NOW After XOR opn of all 4 terms we get $= 10110111$

So.

New state Array

47	?	?	?
37	?	?	?
?	?	?	?
?	?	?	?

Ily perform other multiplications. When we encounter the resultant polynomial is not in set then ~~the~~ use Irreducible polynomial

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

So final matrix is:

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