AES mix cols

Multiplication in field GF_{2^8} w/ mod polynomial

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

Learn how to multiply by x.

$P(x) \times X = Q(x)$

deg ≤ 7 deg ≤ 8

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

$$\begin{array}{r|l} & 1 \\ \hline x^8+x^4+x^3+x+1 & x^8 \\ & -x^8+x^4+x^3+x+1 \\ \hline & -x^4-x^3-x-1 \end{array}$$

$$x^8 \equiv x^4+x^3+x+1 \pmod{x^8+x^4+x^3+x+1}$$

00000010

$02 \times B6$ [$x \cdot (x^7+x^5+x^4+x^2+x)$]

10110110

$02 \times 10110110 = 101101100$ (bit shift)

$= 00011011 \leftarrow$ ok under mod

01110111 (77)

00000011 ← x+1

$03 \times D5$ [$(x+1) \cdot (x^7+x^6+x^4+x^2+1)$]

11010101

$02 \times D5 = 110101010$ (bit shift)

00011011

10110001

$01 \times D5 = 11010101$

01100100 (64)

row 4 → 3 1 1 2 ↓ col 2

D5
7C
39
B6

Ans R4C2 = 3×D5 + 1×7C + 1×39 + 2×B6

64 + 7C + 39 + 77

64 ^ 7C = 18

39 ^ 77 = 4E

18 ^ 4E = 56

0011 1001
0111 0111

Key Schedule

left cyclic shift 1 byte

RotWord(A6378EF1) = 378EF1A6

SubWord(378EF1A6) = 9A 19 A1 24

↳ from S-box do each byte

Pretend Round 9 (Rcon[9] = 1B

9A 19 A1 24

temp = ⊕ 1B 00 00 00

81 19 A1 24