Appendix 3. Use of Galois' Field multiplication rule in AES MixColumns step

MixColumn Step can be presented with the following short notation.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \otimes \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

To use the above formula we need to know a) how matrix product is calculated and b) the multiplication rule of Galois' Fields.

Example. Calculate element b_{11} of matrix B, when A is given as below.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \otimes \begin{bmatrix} 95 & 90 & 85 & C3 \\ 65 & FB & 67 & C9 \\ F8 & B1 & A6 & 6E \\ F3 & 97 & 7B & FF \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

1. Matrix Multiplication:

According to the rule of matrix multiplication b_{11} is the dot product of first row of the matrix of the first matrix and the first column of the second matrix of the product. That is

$b_{11} = 2 \otimes 95 + 3 \otimes 65 + 1 \otimes F8 + 1 \otimes F3$

2. Calculation of the products and their sum

Operation $\otimes$ is Galois' field multiplication for which we need polynomial presentations of numbers:

The numbers of the first matrix have short polynomial prestentations $2 = 10_2 = x$, $3 = 11_2 = x + 1$, $1 = 01_2 = \mathbf{1}$
The bytes of the second matrix have following polynomial presentations:
$95 = 1001\ 0101_2 = x^7 + x^4 + x^2 + 1$
$65 = 0110\ 0101_2 = x^6 + x^5 + x^2 + 1$
$F8 = 1111\ 1000_2 = x^7 + x^6 + x^5 + x^4 + x^3$
$F3 = 1111\ 0011_2 = x^7 + x^6 + x^5 + x^4 + x + 1$

$2 \otimes 95 = x\,(x^7 + x^4 + x^2 + 1) = x^8 + x^5 + x^3 + x$
Because the degree of the polynomial > 7, we reduce the polynomial by adding the modulus of Galois' Field $x^8 + x^4 + x^3 + x + 1$
$(\underline{x^8} + x^5 + \underline{x^3 + x}) + (\underline{x^8} + x^4 + \underline{x^3 + x} + 1) = x^5 + x^4 + 1 = 00110001$ (underlined powers appear twice => even coefficient 2 equals 0)

$3 \otimes 65 = (x+1)(x^6 + x^5 + x^2 + 1) = (x^7 + \underline{x^6} + x^3 + x) + (\underline{x^6} + x^5 + x^2 + 1) = x^7 + x^5 + x^3 + x^2 + x + 1 = 1010\ 1111$

The rest are simple:
$1 \otimes F8 = F8 = x^7 + x^6 + x^5 + x^4 + x^3 = 1111\ 1000$
$1 \otimes F3 = F3 = x^7 + x^6 + x^5 + x^4 + x + 1 = 1111\ 0011$

Final step is to add the four products together using XOR addition:

0011 0001
1010 1111
1111 1000
1111 0011
1001 0101 = 95_{16}

Result: Elemenf $b_{11} = 95$

After this appendix there is a (1p) bonus problem, where you are required to calculate byte B22 of the previous example.