Appendix 3. Mathematics behind AES steps

1) Usage of Galois' Field multiplication rule in AES MixColumns step
2) Calculation of elements of SBOX table in Substitute Bytes using GF(2^8) mathematics

1) 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 $2 = 10_2 = x$, $3 = 11_2 = x + 1$, $1 = 01_2 = 1$
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
<u>1111 0011</u>
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.

2) HOW THE VALUES OF AES SBOX WERE CALCULATED

AES SBOX is usually presented in form of the following table (Chapter2 slide 27)
Table shows the image byte of any byte XY.

X \ Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 3.
AES S-box

The table is based on mathematics, which can be presented with the following matrix formula.

$$\begin{bmatrix} y8 \\ y7 \\ y6 \\ y5 \\ y4 \\ y3 \\ y2 \\ y1 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} b8 \\ b7 \\ b6 \\ b5 \\ b4 \\ b3 \\ b2 \\ b1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Byte $B=b_1 \ldots b_8$ is the multiplicative inverse *) in GF(2^8) of the input byte XY. B is written from bottom to up after the square matrix.

Byte $Y = y_1 \ldots y_8$ is the image of the input byte (also upside down)

The multiplier square matrix is obtained by rotations of first row.
All additions are XOR additions.

Example: Calculation of the image byte of 69_{16}.
Step1: Input 69 is in binary form 0110 1001. We need its multiplicative inverse, which is quite difficult to do manually. (The method is based on ExtendedGCD for polynomials). In WolframAlpha we can calculate the inverse with the following command: PolynomialMod[PolynomialMod[(x^6+x^5+x^3+1)^254, x^8+x^4+x^3+x+1],2] which gives $x^6 + x^2 + x + 1$ which is byte 0100 0111.
Step2 We need calculator which is able to do matrix operations (Excel will do)

$$\begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{which gives} \quad \begin{pmatrix} 3 \\ 4 \\ 4 \\ 3 \\ 3 \\ 3 \\ 3 \\ 1 \end{pmatrix}$$

Step3. Reducing the result to binary numbers using rule even $\rightarrow$ 0 , odd $\rightarrow$ 1
and reading it from bottom to up we get 11111001 = F9.
By checking the answer from the SBOX table we see that the result matches.

It is important to notice, that **AES uses the precalculated SBOX** table (it does no matrix operations)

*) The multiplicative inverse of polynomial p(x) in GF(2^8) is a polynomial $p^{-1}(x)$, for which $p(x)*p^{-1}(x)$ mod q(x) = 1. (q(x) is the modulus used in AES: $x^8 + x^4 + x^3 + x + 1$).
Because GF(2^8) is an Abelian group with 255 elements, we have p(x)^255 mod q(x) = 1, which leads to formula **$p(x)^{-1}$ = p(x)^254 mod q(x)**.

This formula was used in WolframAlpha command
PolynomialMod[PolynomialMod[(x^6+x^5+x^3+1)^254, x^8+x^4+x^3+x+1],2]