# APPENDIX I
# MORE ON SIMPLIFIED AES

**William Stallings**




Supplement to
*Cryptography and Network Security, Fifth Edition*
William Stallings
Prentice Hall 2010
ISBN-10: 0136097049
http://williamstallings.com/Crypto/Crypto5e.html

## I.1 ARITHMETIC IN GF($2^4$)

Table I.1 shows the addition and multiplication tables in GF($2^4$) modulo $x^4 + x + 1$. For example, consider the product (4 • C) = (0100 • 1100). In terms of polynomials, this is the product [$x^2 \times (x^3 + x^2)$] mod ($x^4 + x + 1$) = ($x^5 + x^4$) mod ($x^4 + x + 1$). Because the degree of the polynomial to the right of the mod operator is greater than or equal to the modulus, a division is required to determine the remainder:

$$
\begin{array}{r|l}
x^4 + x + 1 & x + 1 \\
\cline{2-2}
 & x^5 + x^4 \\
 & x^5 + \quad x^2 + x \\
\cline{2-2}
 & \quad x^4 + x^2 + x \\
 & x^4 + \quad x + 1 \\
\cline{2-2}
 & \quad x^2 + 1
\end{array}
$$

In binary, the remainder is expressed as 0101, or 5 in hexadecimal. Thus (4 • C) = 5, which agrees with the multiplication table in Table I.1.

## Table I.1 Arithmetic in GF($2^4$) modulo $x^4 + x + 1$

### (a) Addition

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 1 | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 | 9 | 8 | B | A | D | C | F | E |
| 2 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 | A | B | 8 | 9 | E | F | C | D |
| 3 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | B | A | 9 | 8 | F | E | D | C |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | C | D | E | F | 8 | 9 | A | B |
| 5 | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 | D | C | F | E | 9 | 8 | B | A |
| 6 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 | E | F | C | D | A | B | 8 | 9 |
| 7 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | F | E | D | C | B | A | 9 | 8 |
| 8 | 8 | 9 | A | B | C | D | E | F | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 9 | 8 | B | A | D | C | F | E | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| A | A | B | 8 | 9 | E | F | C | D | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| B | B | A | 9 | 8 | F | E | D | C | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| C | C | D | E | F | 8 | 9 | A | B | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| D | D | C | F | E | 9 | 8 | B | A | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| E | E | F | C | D | A | B | 8 | 9 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| F | F | E | D | C | B | A | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

### (b) Multiplication

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 2 | 0 | 2 | 4 | 6 | 8 | A | C | E | 3 | 1 | 7 | 5 | B | 9 | F | D |
| 3 | 0 | 3 | 6 | 5 | C | F | A | 9 | B | 8 | D | E | 7 | 4 | 1 | 2 |
| 4 | 0 | 4 | 8 | C | 3 | 7 | B | F | 6 | 2 | E | A | 5 | 1 | D | 9 |
| 5 | 0 | 5 | A | F | 7 | 2 | D | 8 | E | B | 4 | 1 | 9 | C | 3 | 6 |
| 6 | 0 | 6 | C | A | B | D | 7 | 1 | 5 | 3 | 9 | F | E | 8 | 2 | 4 |
| 7 | 0 | 7 | E | 9 | F | 8 | 1 | 6 | D | A | 3 | 4 | 2 | 5 | C | B |
| 8 | 0 | 8 | 3 | B | 6 | E | 5 | D | C | 4 | F | 7 | A | 2 | 9 | 1 |
| 9 | 0 | 9 | 1 | 8 | 2 | B | 3 | A | 4 | D | 5 | C | 6 | F | 7 | E |
| A | 0 | A | 7 | D | E | 4 | 9 | 3 | F | 5 | 8 | 2 | 1 | B | 6 | C |
| B | 0 | B | 5 | E | A | 1 | F | 4 | 7 | C | 2 | 9 | D | 6 | 8 | 3 |
| C | 0 | C | B | 7 | 5 | 9 | E | 2 | A | 6 | 1 | D | F | 3 | 4 | 8 |
| D | 0 | D | 9 | 4 | 1 | C | 8 | 5 | 2 | F | B | 6 | 3 | E | A | 7 |
| E | 0 | E | F | 1 | D | 3 | 2 | C | 9 | 7 | 6 | 8 | 4 | A | B | 5 |
| F | 0 | F | D | 2 | 9 | 6 | 4 | B | 1 | E | C | 3 | 8 | 7 | 5 | A |

## I.2 THE MIX COLUMN FUNCTION

The mix column function operates on each column individually. Each nibble of a column is mapped into a new value that is a function of both nibbles in that column. The transformation was defined in Appendix 5B as follows:

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} \\ s_{1,0} & s_{1,1} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} \\ s'_{1,0} & s'_{1,1} \end{bmatrix}$$

We can recast this in terms of polynomials as follows. The value 1 corresponds to the polynomial 1 and the value 4 (binary 100) corresponds to the polynomial $x^2$. Thus, we have:

$$\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} \\ s_{1,0} & s_{1,1} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} \\ s'_{1,0} & s'_{1,1} \end{bmatrix}$$

Remember that multiplication is performed modulo $x^4 + x + 1$. Using the polynomial formulation allows us to develop a simple explanation of the arithmetic involved. Referring back to the representation of the state matrix in Figure 5.12a, we can recast the mix column multiplications as follows:

$$\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} b_0x^3 + b_1x^2 + b_2x + b_3 & b_8x^3 + b_9x^2 + b_{10}x + b_{11} \\ b_4x^3 + b_5x^2 + b_6x + b_7 & b_{12}x^3 + b_{13}x^2 + b_{14}x + b_{15} \end{bmatrix}$$

Let's perform the multiplication of the first row of the left-hand matrix with the first column of the right-hand matrix to get the entry in the upper left-hand corner of the target matrix; that is, the polynomial value for $S'_{0,0}$. We have

$$S'_{0,0} = (b_0x^3 + b_1x^2 + b_2x + b_3) + (x^2)\,(b_4x^3 + b_5x^2 + b_6x + b_7)$$

$$= b_4x^5 + b_5x^4 + (b_0 \oplus b_6)x^3 + (b_1 \oplus b_7)x^2 + b_2x + b_3$$

It can easily be shown that:

$$x^5 \bmod (x^4 + x + 1) = (x^2 + x)$$
$$x^4 \bmod (x^4 + x + 1) = (x + 1)$$

The reader is invited to do the polynomial division to demonstrate these equalities. Using these results, we have:

$$S'_{0,0} = b_4(x^2 + x) + b_5(x + 1) + (b_0 \oplus b_6)x^3 + (b_1 \oplus b_7)x^2 + b_2x + b_3$$
$$= (b_0 \oplus b_6)x^3 + (b_1 \oplus b_4 \oplus b_7)x^2 + (b_2 \oplus b_4 \oplus b_5)x + (b_3 \oplus b_5)$$

Expressed in terms of bits, the four bits of $S'_{0,0}$ are

$$S'_{0,0} = [(b_0 \oplus b_6), (b_1 \oplus b_4 \oplus b_7), (b_2 \oplus b_4 \oplus b_5), (b_3 \oplus b_5)]$$

Similarly, we can show that:

$$S'_{1,0} = [(b_2 \oplus b_4), (b_0 \oplus b_3 \oplus b_5), (b_0 \oplus b_1 \oplus b_6), (b_1 \oplus b_7)]$$
$$S'_{0,1} = [(b_8 \oplus b_{14}), (b_9 \oplus b_{12} \oplus b_{15}), (b_{10} \oplus b_{12} \oplus b_{13}), (b_{11} \oplus b_{13})]$$
$$S'_{1,1} = [(b_{10} \oplus b_{12}), (b_8 \oplus b_{11} \oplus b_{13}), (b_8 \oplus b_9 \oplus b_{14}), (b_9 \oplus b_{15})]$$