FIPS-197 notes

Peter Franušić *

FIPS-197 is the Federal Information Processing Standard Publication 197 (FIPS PUB 197). It is a publication of the National Institute of Science and Technology (NIST). FIPS-197 specifies the Advanced Encryption Standard (AES). New readers of FIPS-197 may find themselves faced with a steep learning curve. These notes address some of the more difficult topics. In order to provide synchronization, the section headings are identical to those in FIPS-197.

4. Mathematical Preliminaries

> All bytes in the AES algorithm are interpreted as finite field elements... Finite field elements can be added and multiplied, but these operations are different from those used for numbers.

A *finite field* is a set with a finite number of elements and two operations. AES uses the finite field $\mathrm{GF}(2^8)$ where the GF stands for "Galois Field" (pronouced "gal WAH") and the 2^8 is the number of elements in the set.

$\mathrm{GF}(2^8)$ has a set P that consists of 256 polynomials. There are two operations in $\mathrm{GF}(2^8)$. The first is the "add" operation (denoted here by $\oplus$). The second is the "multiply" operation (denoted here by $\bullet$).

$$\mathrm{GF}(2^8) = (\mathrm{P}, \oplus, \bullet)$$

A few words about symbols... The "add" operation is denoted above by the symbol $\oplus$. FIPS-197 uses this symbol in some equations, but in most equations it uses the + symbol. Both symbols signify the same operation: the "addition" of polynomial elements in $\mathrm{GF}(2^8)$. In these notes, we'll only use the + symbol.

 Email: pete@sargo.com

The "multiply" operation is denoted above by the symbol $\bullet$. FIPS-197 uses this symbol in some equations. In other equations it simply omits the symbol and the operation is implied. In both cases the operation means "multiplication" of polynomial elements in GF(2^8). In these notes, we'll use the implied form in most equations.

We also note that the symbol $\otimes$ is introduced is section 2.2 as the symbol for modulo $x^4 + 1$ multiplication of polynomials with coefficients in GF(2^8). The symbol is used later in sections 4.3, 5.1.3 and 5.3.3. The $\otimes$ symbol should not be confused with the $\bullet$ symbol.

It is important to understand that the elements in GF(2^8) are *not* integers. Rather, each element is a *polynomial* with binary coefficients. For example, the polynomial $x^5 + x^2$ is an element in GF(2^8). Any GF(2^8) polynomial may be represented using an *integer vector* notation which consists of two hexadecimal digits within curly braces.

Here is a partial list of the GF(2^8) polynomials and the corresponding integer vectors. Note that the "multiply" operation is implied in each term. Also note that the eight binary coefficients in each polynomial are represented as two hexadecimal digits within curly braces.

$$\begin{aligned}
0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 0x^1 + 0x^0 &= \{\texttt{00}\} \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 0x^1 + 1x^0 &= \{\texttt{01}\} \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 0x^0 &= \{\texttt{02}\} \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0 &= \{\texttt{03}\} \\
&\vdots \\
1x^7 + 1x^6 + 1x^5 + 1x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 &= \{\texttt{FD}\} \\
1x^7 + 1x^6 + 1x^5 + 1x^4 + 1x^3 + 1x^2 + 1x^1 + 0x^0 &= \{\texttt{FE}\} \\
1x^7 + 1x^6 + 1x^5 + 1x^4 + 1x^3 + 1x^2 + 1x^1 + 1x^0 &= \{\texttt{FF}\}
\end{aligned}$$

We usually write GF(2^8) polynomials using a short-hand notation. Any term with its coefficient equal to 0 is not written, any term with its coefficient equal to 1 is written without the coefficient, any term x^1 is written simply as x, and any term x^0 is written as 1. For example

$$\begin{aligned}
x &= \{\texttt{02}\} \\
x^2 + 1 &= \{\texttt{05}\} \\
x^7 + x^3 + x + 1 &= \{\texttt{8B}\}
\end{aligned}$$

4.1 Addition

> The addition of two elements in a finite field is achieved by "adding" the coefficients for the corresponding powers in the polynomials for the two elements. The addition is performed with the XOR operation...

The "add" operation in GF(2^8) is *not* integer addition. It is polynomial addition. The following example in FIPS-197 shows the addition of two polynomials.

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) \quad = \quad x^7 + x^6 + x^4 + x^2$$

So what happened to the $x + 1$ in each polynomial? Why didn't they show up in the sum as $2x + 2$? The answer is that we're not doing integer addition. The $+$ operator denotes exclusive-or addition. Here's the exclusive-or truth table:

$$\begin{aligned} 0 + 0 &= 0 \\ 0 + 1 &= 1 \\ 1 + 0 &= 1 \\ 1 + 1 &= 0 \end{aligned}$$

In the example, the two x terms cancel out because the exclusive-or of their coefficients is 0. The distributive property holds for GF(2^8).

$$\begin{aligned} x + x &= 1x + 1x \\ &= (1 + 1)x \\ &= 0x \\ &= 0 \end{aligned}$$

4.2 Multiplication

> In the polynomial representation, multiplication in GF(2^8) (denoted by $\bullet$) corresponds with the multiplication of polynomials modulo an **irreducible polynomial** of degree 8.

The "multiply" operation in GF(2^8) is *not* integer multiplication. It is modular multiplication of polynomials. The modulus is the polynomial $m(x)$. It has an x^8 term, which makes it a polynomial of degree 8.

$$m(x) \quad = \quad x^8 + x^4 + x^3 + x + 1$$

The polynomial $m(x)$ is *irreducible* because it cannot be factored. It's similar to a prime integer. Except for 1 and $m(x)$, there are no two polynomials $p(x)$ and $q(x)$ such that

$$p(x) \bullet q(x) \quad = \quad m(x)$$

The following example in FIPS-197 shows the multiplication of two polynomials. Note that the distribution property holds for GF(2^8).

$$\begin{aligned}
\{57\} \bullet \{83\} &= (x^6 + x^4 + x^2 + x + 1) \bullet (x^7 + x + 1) \\
&= (x^6 + x^4 + x^2 + x + 1) \bullet x^7 + \\
&\quad (x^6 + x^4 + x^2 + x + 1) \bullet x + \\
&\quad (x^6 + x^4 + x^2 + x + 1) \bullet 1 \\
&= x^{13} + x^{11} + x^9 + x^8 + x^7 + \\
&\quad x^7 + x^5 + x^3 + x^2 + x + \\
&\quad x^6 + x^4 + x^2 + x + 1 \\
&= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1
\end{aligned}$$

We have a problem. This is a degree 13 polynomial. GF(2^8) polynomials are no larger that degree 7. So what went wrong? The answer is that "multiplication" in GF(2^8) includes reduction by $m(x)$. We neglected to reduce on each multiply above. But fortunately, because of the distribution property, we can do one humongous reduction at the end, which is what the example in FIPS-197 does.

We can compute the reduction using long division. The dividend is the degree 13 polynomial from above. The divisor is our irreducible degree 8 polynomial $m(x)$. We do the long division, chuck the quotient polynomial $x^5 + x^3$ and keep the remainder polynomial $x^7 + x^6 + 1$. Remember that "subtraction" in GF(2^8) is simply an exclusive-or, just like "addition."

We show the details of the long division as two subtractions. For the first subtraction, we multiply our degree 8 $m(x)$ by x^5 so that we have an x^{13} term that will cancel out.

$$\begin{aligned}
m(x) \bullet x^5 &= (x^8 + x^4 + x^3 + x + 1) \bullet x^5 \\
&= x^{13} + x^9 + x^8 + x^6 + x^5
\end{aligned}$$

Now we "subtract" this from the degree 13 polynomial. To "subtract" we simply do the exclusive-or operation $\oplus$ in GF(2^8). (*E.g.* $x^{13} - x^{13} = x^{13} \oplus x^{13} = 0$). We are left with a polynomial of degree 11.

$$\begin{aligned}
& x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\
- \quad & (x^{13} + x^9 + x^8 + x^6 + x^5) \\
= \quad & x^{11} + x^4 + x^3 + 1
\end{aligned}$$

For the second subtraction, we multiply $m(x)$ by x^3 so that we have an x^{11} term that will cancel out.

$$\begin{aligned}
m(x) \bullet x^3 &= (x^8 + x^4 + x^3 + x + 1) \bullet x^3 \\
&= x^{11} + x^7 + x^6 + x^4 + x^3
\end{aligned}$$

Now we "subtract" this from the degree 11 polynomial. We are left with a polynomial of degree 7, which is in GF(2^8) and is the element {C1}.

$$\begin{aligned} & x^{11} + x^4 + x^3 + 1 \\ - \quad & (x^{11} + x^7 + x^6 + x^4 + x^3) \\ = \quad & x^7 + x^6 + 1 \\ = \quad & \{\texttt{C1}\} \end{aligned}$$

4.3 Polynomials with Coefficients in GF(2^8)

We are given the two polynomials $a(x)$ and $b(x)$. Each has four terms. Each term is the product of a coefficient (*e.g.* a_3) and a power of x (*e.g.* x^3). The coefficients of $a(x)$ and $b(x)$ are not integers. They are polynomials in GF(2^8).

$$\begin{aligned} a(x) &= a_3x^3 + a_2x^2 + a_1x + a_0 \\ b(x) &= b_3x^3 + b_2x^2 + b_1x + b_0 \end{aligned}$$

We wish to compute the modulo $x^4 + 1$ product $a(x) \otimes b(x)$. The example in FIPS-197 does this in two steps. The first step is to do the multiplications without reductions. We save the reduction for the second step.

$$\begin{aligned} a(x) \otimes b(x) &= (a_3x^3 + a_2x^2 + a_1x + a_0) \otimes \\ & \quad (b_3x^3 + b_2x^2 + b_1x + b_0) \\ &= (a_3x^3 + a_2x^2 + a_1x + a_0)b_3x^3 + \\ & \quad (a_3x^3 + a_2x^2 + a_1x + a_0)b_2x^2 + \\ & \quad (a_3x^3 + a_2x^2 + a_1x + a_0)b_1x + \\ & \quad (a_3x^3 + a_2x^2 + a_1x + a_0)b_0 \\ &= a_3b_3x^6 + a_2b_3x^5 + a_1b_3x^4 + a_0b_3x^3 + \\ & \quad a_3b_2x^5 + a_2b_2x^4 + a_1b_2x^3 + a_0b_2x^2 + \\ & \quad a_3b_1x^4 + a_2b_1x^3 + a_1b_1x^2 + a_0b_1x + \\ & \quad a_3b_0x^3 + a_2b_0x^2 + a_1b_0x + a_0b_0 \\ &= (a_3b_3)x^6 + (a_3b_2 + a_2b_3)x^5 + \\ & \quad (a_3b_1 + a_2b_2 + a_1b_3)x^4 + \\ & \quad (a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3)x^3 + \\ & \quad (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \\ & \quad (a_1b_0 + a_0b_1)x + a_0b_0 \end{aligned}$$

We replace each of the seven coefficient expressions with a c_i so that we have a compact set of equations. The result is the same as equation (4.9) in FIPS-197.

$$\begin{aligned}
a(x) \otimes b(x) &= c(x) \\
c(x) &= c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_2x + c_0 \\
c_6 &= a_3b_3 \\
c_5 &= a_3b_2 + a_2b_3 \\
c_4 &= a_3b_1 + a_2b_2 + a_1b_3 \\
c_3 &= a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\
c_2 &= a_2b_0 + a_1b_1 + a_0b_2 \\
c_1 &= a_1b_0 + a_0b_1 \\
c_0 &= a_0b_0
\end{aligned}$$

Now for step two. We have $c(x)$ which is a degree 6 polynomial. It must be reduced to a degree 3 polynomial. Again, we can compute the reduction using long division where the dividend is $c(x)$ and the divisor is x^4+1. The reduction requires three subtractions.

For the first subtraction, we multiply x^4+1 by c_6x^2 so that we have an x^6 term that will cancel out.

$$(x^4+1)c_6x^2 = c_6x^6 + c_6x^2$$

Now we "subtract" this from the $c(x)$ polynomial. Since $(c_6 + c_6) = 0$, we are left with a polynomial of degree 5.

$$\begin{aligned}
& (c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0) \\
- \; & (c_6x^6 + c_6x^2) \\
= \; & (c_6 + c_6)x^6 + c_5x^5 + c_4x^4 + c_3x^3 + (c_2 + c_6)x^2 + c_1x + c_0 \\
= \; & c_5x^5 + c_4x^4 + c_3x^3 + (c_2 + c_6)x^2 + c_1x + c_0
\end{aligned}$$

For the second subtraction, we multiply $x^4 + 1$ by c_5x so that we have an x^5 term that will cancel out.

$$(x^4+1)c_5x = c_5x^5 + c_5x$$

This gets "subtracted" from the degree 5 remainder above. Since $(c_5 + c_5) = 0$, we are left with a polynomial of degree 4.

$$\begin{aligned}
& (c_5x^5 + c_4x^4 + c_3x^3 + (c_2 + c_6)x^2 + c_1x + c_0) \\
- \; & (c_5x^5 + c_5x) \\
= \; & (c_5 + c_5)x^5 + c_4x^4 + c_3x^3 + (c_2 + c_6)x^2 + (c_1 + c_5)x + c_0 \\
= \; & c_4x^4 + c_3x^3 + (c_2 + c_6)x^2 + (c_1 + c_5)x + c_0
\end{aligned}$$

For the last subtraction, we multiply $x^4 + 1$ by c_4 so that we have an x^4 term that will cancel out.

$$(x^4 + 1)c_4 \quad = \quad c_4x^4 + c_4$$

This gets "subtracted" from the degree 4 remainder above. Since $(c_4 + c_4) = 0$, we are left with a polynomial of degree 3, which is what we want.

$$\begin{aligned} & (c_4x^4 + c_3x^3 + (c_2 + c_6)x^2 + (c_1 + c_5)x + c_0) \\ - \quad & (c_4x^4 + c_4) \\ = \quad & (c_4 + c_4)x^4 + c_3x^3 + (c_2 + c_6)x^2 + (c_1 + c_5)x + (c_0 + c_4) \\ = \quad & c_3x^3 + (c_2 + c_6)x^2 + (c_1 + c_5)x + (c_0 + c_4) \end{aligned}$$

We replace the four coefficient expressions with a d_i where each d_i is expressed using the coefficients from $a(x)$ and $b(x)$. The result is the same as equation (4.12) in FIPS-197.

$$\begin{aligned} a(x) \otimes b(x) &= d(x) \\ d(x) &= d_3x^3 + d_2x^2 + d_2x + d_0 \\ d_3 &= c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\ d_2 &= (c_2 + c_6) = a_2b_0 + a_1b_1 + a_0b_2 + a_3b_3 \\ d_1 &= (c_1 + c_5) = a_1b_0 + a_0b_1 + a_3b_2 + a_2b_3 \\ d_0 &= (c_0 + c_4) = a_0b_0 + a_3b_1 + a_2b_2 + a_1b_3 \end{aligned}$$

Equations (4.14) and (4.15) specify two polynomials $a(x)$ and $a^{-1}(x)$. Polynomial $a(x)$ is used in the `MixColumns` transformation (section 5.1.3). Polynomial $a^{-1}(x)$ is used in the `InvMixColumns` transformation (section 5.3.3).

$$\begin{aligned} a(x) &= \{\texttt{03}\}x^3 + \{\texttt{01}\}x^2 + \{\texttt{01}\}x + \{\texttt{02}\} \\ a^{-1}(x) &= \{\texttt{0B}\}x^3 + \{\texttt{0D}\}x^2 + \{\texttt{09}\}x + \{\texttt{0E}\} \end{aligned}$$

What makes `MixColumns` and `InvMixColumns` work together is that $a^{-1}(x)$ is the multiplicative inverse of $a(x)$. In other words, the modulo $x^4 + 1$ product of $a(x)$ and $a^{-1}(x)$ is the multiplicative identity polynomial $\{\texttt{01}\}$.

$$a(x) \otimes a^{-1}(x) \quad = \quad \{\texttt{01}\}$$

The coefficients of $d(x)$ give us an easy way to verify this. First we write the product in terms of $d(x)$. Then we use the formulas in equation (4.12) to compute the four coefficients of $d(x)$.

$$\begin{aligned} a(x) \otimes a^{-1}(x) &= d(x) \\ &= d_3x^3 + d_2x^2 + d_1x + d_0 \end{aligned}$$

$$\begin{aligned} d_3 &= a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\ &= \{03\}\{0E\} + \{01\}\{09\} + \{01\}\{0D\} + \{02\}\{0B\} \\ &= \{03\} + \{09\} + \{0D\} + \{07\} \\ &= \{00\} \end{aligned}$$

$$\begin{aligned} d_2 &= a_2b_0 + a_1b_1 + a_0b_2 + a_3b_3 \\ &= \{01\}\{0E\} + \{01\}\{09\} + \{02\}\{0D\} + \{03\}\{0B\} \\ &= \{0E\} + \{09\} + \{0B\} + \{0C\} \\ &= \{00\} \end{aligned}$$

$$\begin{aligned} d_1 &= a_1b_0 + a_0b_1 + a_3b_2 + a_2b_3 \\ &= \{01\}\{0E\} + \{02\}\{09\} + \{03\}\{0D\} + \{01\}\{0B\} \\ &= \{0E\} + \{03\} + \{06\} + \{0B\} \\ &= \{00\} \end{aligned}$$

$$\begin{aligned} d_0 &= a_0b_0 + a_3b_1 + a_2b_2 + a_1b_3 \\ &= \{02\}\{0E\} + \{03\}\{09\} + \{01\}\{0D\} + \{01\}\{0B\} \\ &= \{0D\} + \{0A\} + \{0D\} + \{0B\} \\ &= \{01\} \end{aligned}$$

We assemble the four coefficients back into the equation for $d(x)$. The first three coefficients are $\{00\}$ so those terms cancel. The coefficient for the x^0 term is $\{01\}$. QED.

$$\begin{aligned} d(x) &= \{00\}x^3 + \{00\}x^2 + \{00\}x + \{01\} \\ &= \{01\} \end{aligned}$$

5.1.1 `SubBytes()` Transformation

The `SubBytes()` transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). This S-box, which is invertible, is constructed by composing two transformations.

The S-box is a non-linear substitution table used in the `SubBytes` and `SubWord` functions to perform one-for-one substitution of byte values. The S-box consists of 256 bytes that are precomputed.

The S-box for AES was not concocted in some dark corner of the National Security Agency. Section 5.1.1 in FIPS-197 specifies a two-step algorithm to compute each byte in the S-box.

1. Compute the GF(256) *multiplicative inverse* using the irreducible polynomial m(x) given in equation (4.1) in FIPS-197.
2. Compute the eight GF(2) *affine transformations* using the formula given in equation (5.1) in FIPS-197.

The following table shows the multiplicative inverse for each polynomial element of GF(256) except {00}. The irreducible polynomial $m(x) = \{011B\}$ is the modulus. The table is organized into 16 rows and 16 columns. Given a polynomial represented by the two hexadecimal digits {RC}, the multiplicative inverse is at the intersection of row R and column C.

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

For example, the multiplicative inverse of {53} may be found at the intersection of row 5 and column 3. Therefore the multiplicative inverse of {53} is {CA}. I.e., {53}{CA} = {01}. Note that element {00} does not have an inverse (it's blank), and no element in the table has the value {00}. Note also that the inverse of {01} is {01}.

Equation (5.1) can be expanded into the eight affine transformations shown here. The plus sign (+) is the exclusive-or operator. Note that the c bits have been replaced by binary constants. Note also that these eight transformations can be computed in parallel by precomputing four additional bytes which provide the required rotations.

$$\begin{aligned}
b'_7 &= b_7 + b_3 + b_4 + b_5 + b_6 + 0 \\
b'_6 &= b_6 + b_2 + b_3 + b_4 + b_5 + 1 \\
b'_5 &= b_5 + b_1 + b_2 + b_3 + b_4 + 1 \\
b'_4 &= b_4 + b_0 + b_1 + b_2 + b_3 + 0 \\
b'_3 &= b_3 + b_7 + b_0 + b_1 + b_2 + 0 \\
b'_2 &= b_2 + b_6 + b_7 + b_0 + b_1 + 0 \\
b'_1 &= b_1 + b_5 + b_6 + b_7 + b_0 + 1 \\
b'_0 &= b_0 + b_4 + b_5 + b_6 + b_7 + 1
\end{aligned}$$

The following table is the S-box shown in FIPS-197 Figure 7. Each polynomial in the table has been computed using the two-step algorithm. The table is organized into 16 rows and 16 columns. Given a polynomial represented by the two hexadecimal digits {RC}, the substitution polynomial is at the intersection of row R and column C.

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

For example, given the polynomial {53}, its substitution may be found at the intersection of row 5 and column 3. Therefore the substitution of {53} is {ED}. Note from the example above that the multiplicative inverse of {53} is {CA}. And the eight affine transformations applied to {CA} produces {ED}.

5.3.2 `InvSubBytes()` Transformation

> `InvSubBytes()` is the inverse of the byte substitution transformation, in which the inverse S-box is applied to each byte of the State. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF(2^8).

The inverse S-box is also non-linear substitution table. It is used in the `InvSubBytes` function to perform one-for-one substitution of byte values. The inverse S-box consists of 256 bytes that are precomputed using a two-step algorithm.

1. Compute the eight *inverse affine transformations* using the formula given below.
2. Compute the GF(256) *multiplicative inverse* using the polynomial m(x).

The inverse affine transformation can be derived from the original eight affine transformations. The first step is to rewrite each equation. For example, in the first equation, we "add" $b'_7 + b_7$ to both sides. The b'_7 on the left drops out, and the b_7 on the right drops out.

$$\begin{aligned}
b_7 &= b'_7 + b_3 + b_4 + b_5 + b_6 + 0 \\
b_6 &= b'_6 + b_2 + b_3 + b_4 + b_5 + 1 \\
b_5 &= b'_5 + b_1 + b_2 + b_3 + b_4 + 1 \\
b_4 &= b'_4 + b_0 + b_1 + b_2 + b_3 + 0 \\
b_3 &= b'_3 + b_7 + b_0 + b_1 + b_2 + 0 \\
b_2 &= b'_2 + b_6 + b_7 + b_0 + b_1 + 0 \\
b_1 &= b'_1 + b_5 + b_6 + b_7 + b_0 + 1 \\
b_0 &= b'_0 + b_4 + b_5 + b_6 + b_7 + 1
\end{aligned}$$

Each equation now has an "old" bit value on the left and a "new" bit value on the right, along with some old ones. The idea is to replace each of the old bit values on the right with the appropriate equations, so that all of the old bit values cancel each other out and we are left with only new bit values on the right. Here's the results:

$$\begin{aligned}
b_7 &= b'_6 + b'_4 + b'_1 + 0 \\
b_6 &= b'_5 + b'_3 + b'_0 + 0 \\
b_5 &= b'_4 + b'_2 + b'_7 + 0 \\
b_4 &= b'_3 + b'_1 + b'_6 + 0 \\
b_3 &= b'_2 + b'_0 + b'_5 + 0 \\
b_2 &= b'_1 + b'_7 + b'_4 + 1 \\
b_1 &= b'_0 + b'_6 + b'_3 + 0 \\
b_0 &= b'_7 + b'_5 + b'_2 + 1
\end{aligned}$$

These eight equations can be condensed into one equation that is similar to equation (5.1) in FIPS-197.

$$b_i \quad = \quad b'_{(i+7) \bmod 8} \oplus b'_{(i+5) \bmod 8} \oplus b'_{(i+2) \bmod 8} \oplus c'_i$$

for $0 \leq i < 8$, where b'_i is the i^{th} bit of the byte, and c'_i is the i^{th} bit of a byte c' with the value {05}. The following table is the inverted S-box shown in FIPS-197 Figure 14.

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