Some Techniques to Compute Multiplicative Inverses for Advanced Encryption Standard

W. Eltayeb Ahmed

Mathematics and Statistics Department, Faculty of Science, Al-Imam Mohammad Ibn Saud Islamic University, Saudi Arabia

waahmed@imamu.edu.sa

Abstract

This paper gives some techniques to compute the set of multiplicative inverses, which uses in the Advanced Encryption Standard (AES).

Keywords: Multiplicative Inverse, Extended Euclidean Algorithm, AES.

1 Introduction

Sometimes, we want to create another form to a specific mapping seeking for simplicity. In AES, the substitution table is made for substituting a byte by another for all byte values from 0 to 255. The first operation in constructing this table is computing [1] the multiplicative inverse of an input byte in Galois field (GF (2^8)), based on the irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$. To do this, we can use the extended Euclidean algorithm [2].

Although it is straightforward, some people think it is a complicated way.

Here, are some techniques to compute these multiplicative inverses.

2 The methodology

The multiplicative inverse of $M(x)$ modulo $P(x)$ is $M^{-1}(x)$ such that

$$M(x)M^{-1}(x) = 1\ \big(mod\ P(x)\big) \quad \rightarrow (1)$$

and this implies

$$P(x) \mid [M(x)M^{-1}(x) - 1] \quad \rightarrow (2)$$

we can take

$$P(x) = M(x)M^{-1}(x) - 1 \quad \rightarrow (3)$$

Let $T[M(x)]$ represents the multiplicative inverse of $M(x)$ modulo $P(x)$, and $Q(x) = P(x) + 1$, then

$$M(x)T[M(x)] = Q(x) \quad \rightarrow (4)$$

There is one of two possible equations:

$$M(x)A(x) = Q(x) \quad \rightarrow (5)$$

or

$$M(x)[A(x) + B(x)] = Q(x) \quad \rightarrow (6)$$

In case 1,

Date of Submission: 2018-12-23
Date of Publication: 2019-01-30

$$T[M(x)] = A(x) \quad \rightarrow (7)$$

The multiplicative inverse is $\frac{Q(x)}{M(x)}$.

In case 2,

$$T[M(x)] = A(x) + \mathrm{B}(x) \quad \rightarrow (8)$$

Write Eq (6) as

$$M(x)A(x) + M(x)B(x) = Q(x) \quad \rightarrow (9)$$

let

$$M(x)A(x) = Q(x) - r(x) \quad \rightarrow (10)$$

where

$$r(x) = M(x)B(x) \quad \rightarrow (11)$$

rewrite Eq (11) as

$$r(x)C(x) = M(x) \quad \rightarrow (12)$$

then

$$B(x) = \frac{1}{C(x)} \quad \rightarrow (13)$$

and since

$$1 = Q(x)\,(mod\ P(x)) \quad \rightarrow (14)$$

we get

$$B(x) = \frac{Q(x)}{C(x)} = T[C(x)] \quad \rightarrow (15)$$

and Eq (8) becomes

$$T[M(x)] = A(x) + T[C(x)] \quad \rightarrow (16)$$

To compute $T[M(x)]$, we need to compute $T[C(x)] = T\left[\frac{M(x)}{r(x)}\right]$.

So, the multiplicative inverse of $M(x)$ modulo $P(x)$ equals $q(x) = \frac{Q(x)}{M(x)}$, if there is no a remainder $r(x)$, and equals $q(x)$ plus the multiplicative inverse of $\frac{M(x)}{r(x)}$, if there is a remainder $r(x)$.

3 Results and Discussion

Let us take some examples:

Example (1): Computing $T(x)$

i	$M(x)$	$q(x)$	$r(x)$	$Q(x)$
1	x	$x^7+x^3+x^2+1$	0	$x^8+x^4+x^3+x$

so,

$$T(x)=x^7+x^3+x^2+1$$

Example (2): Computing $T(x^2)$

i	$M(x)$	$q(x)$	$r(x)$	$Q(x)$
1	x^2	x^6+x^2+x	x	$x^8+x^4+x^3+x$

then

$$T(x^2)=x^6+x^2+x+T(x)$$

$$=x^7+x^6+x^3+x+1$$

Example (3): Computing $T(x^4)$

i	$M(x)$	$q(x)$	$r(x)$	$Q(x)$
1	x^4	x^4+1	x^3+x	$x^8+x^4+x^3+x$
2	x^3+x	x	x^2	x^4
3	x^2	x	x	x^3+x
4	x	x	0	x^3+x

then

$$T(x^4)=q_1+T\{q_2+\mathrm{T}[q_3+T(q_4)]\}$$

$$=x^4+1+T\{x+\mathrm{T}[x+T(x)]\}$$

We note that this technique iterates computing multiplicative inverse when $r_i(x)\neq 0$, and we maybe face computing a multiplicative inverse many times, in the example (3), we need to compute $T(x)$, $T[x+T(x)]$, and $T\{x+\mathrm{T}[x+T(x)]\}$.

Instead of doing this, we put

$$M_2(x)=r_1(x)+1 \quad \rightarrow (17)$$

and starting from the step $(i=2)$, we repeat the solution til $r_i(x)=1$.

If $r_i(x)=1$, $i\geq 2$, then

$$T[M(x)]=T_i[M(x)]=q_i(x)T_{i-1}[M(x)]+T_{i-2}[M(x)] \quad \rightarrow (18)$$

where

$$T_0[M(x)]=1 \quad \rightarrow (19)$$

and

$$T_1[M(x)] = q_1(x)T_0[M(x)] = q_1(x) \quad \rightarrow (20)$$

$M_2(x)$ becomes $r_1(x) + 1$ so, $Q(x)$ must be $Q(x) + 1$, we prove the Eq (18) by the mathematical induction, (let us just take the first step).

When $i = 2$

$$T_2[M(x)] = q_2(x)T_1[M(x)]+T_0[M(x)]$$

$$= \frac{M(x)}{r_1(x)+1}\left[\frac{Q(x)-r_1(x)}{M(x)}\right]+1$$

$$= \frac{Q(x)+1}{r_1(x)+1}$$

$$= \frac{Q(x)}{M_2(x)}$$

Example (4): Repeating compute $T(x^4)$ using this second technique.

i	$M(x)$	$q(x)$	$r(x)$	$Q(x)$
1	x^4	x^4+1	x^3+x	$x^8+x^4+x^3+x$
2	x^3+x	x	x^2	x^4
$2'$	x^3+x+1	x	x^2+x	x^4
3	x^2+x	$x+1$	1	x^3+x+1

$r_3(x) = 1$, so, from Eq (18)

$$T[M(x)] = q_3(x)T_2[M(x)]+T_1[M(x)]$$

$$= q_3(x)[q_2(x)q_1(x)+1]+q_1(x)$$

$$= (x+1)[x(x^4+1)+1]+x^4+1$$

$$= x^6+x^5+x^4+x^2$$

To avoid repeating step $(i = 2)$, we use this technique when $r_1(x) \neq 0$ immediately.

Example (5): Computing $T(x^6+x^5+x^4+x^2)$

We found $T(x^4) = x^6+x^5+x^4+x^2$, let us compute $T(x^6+x^5+x^4+x^2)$

i	$M(x)$	$q(x)$	$r(x)$	$Q(x)$
1	$x^6+x^5+x^4+x^2$	x^2+x	x^5+x	$x^8+x^4+x^3+x$
2	x^5+x+1	$x+1$	x^4+1	$x^6+x^5+x^4+x^2$
3	x^4+1	x	1	x^5+x+1

$r_3(x) = 1$, so, from Eq (18)

$$T[M(x)] = q_3(x)T_2[M(x)]+T_1[M(x)]$$

$$= q_3(x)[q_2(x)q_1(x) + 1]+q_1(x)$$

$$= x[(x + 1)(x^2 + x) + 1] + x^2 + x$$

$$= x^4$$

Conclusions

These techniques compute a multiplicative inverse of $M(x)$ modulo $P(x)$ by easy and clear steps, and when $r_1(x) \neq 0$, we can use the formula Eq (18), after using Eq (17).

References

1. Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology (NIST), November 26, 2001.
2. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997.