Scientific Research Publishing

Applied Mathematics, 2019, 10, 113-118
http://www.scirp.org/journal/am
ISSN Online: 2152-7393
ISSN Print: 2152-7385

On Rijndael ByteSub Transformation

W. Eltayeb Ahmed[1,2]

[1]Mathematics and Statistics Department, Faculty of Science, Imam Mohammad Ibn Saud Islamic University, Riyadh, KSA
[2]Department of Basics and Engineering Sciences, Faculty of Engineering, University of Khartoum, Khartoum, Sudan

Email: waahmed@imamu.edu.sa

How to cite this paper: Ahmed, W.E. (2019) On Rijndael ByteSub Transformation. *Applied Mathematics*, **10**, 113-118.
https://doi.org/10.4236/am.2019.103010

Received: March 2, 2019
Accepted: March 25, 2019
Published: March 28, 2019

Abstract

The first step in converting a plaintext to ciphertext by the famous Advanced Encryption Standard (AES), which is called Rijndael ByteSub Transformation, involves some operations: computing a multiplicative inverse, multiplying this multiplicative inverse by a specific matrix, and adding the result to a specific vector. The purpose of this research is to simplify these operations. This paper gives elegant techniques and presents the matrices multiplication as simple XOR operations, and the result is a simple, straightforward way finding the transformation.

Keywords

Rijndael Cipher, Advanced Encryption Standard, Multiplicative Inverse, XOR Operation

1. Introduction

Rijndael ByteSub transformation (or AES substitution byte) [1] transforms an input byte into another byte by two operations:

1) Finding a multiplicative inverse of an input byte $\left(a_7a_6a_5a_4a_3a_2a_1a_0\right)$ in the finite field GF (2^8).

2) Applying the following affine transform:

$$\begin{aligned} c_i = {} & b_i + b_{(i+4)\bmod(8)} + b_{(i+5)\bmod(8)} + b_{(i+6)\bmod(8)} \\ & + b_{(i+7)\bmod(8)} + d_i,\ 0 \le i \le 7 \end{aligned} \tag{1}$$

where $\left(b_7b_6b_5b_4b_3b_2b_1b_0\right)$ is resulting from the first operation, $\left(d_7d_6d_5d_4d_3d_2d_1d_0\right) = 01100011$.

In general, the multiplicative inverse is found by using the extended Euclidean algorithm [2], instead of using it, we use an elegant technique which finds the multiplicative inverse in clear steps.

The transform of the second operation can be expressed in the matrix form as:

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{2}$$

To solve this system, we use an unusual and more suitable technique which shows this multiplication of matrix (8 × 8) and matrix (8 × 1) as simple XOR operations, and we can find it directly from $(b_7b_6b_5b_4b_3b_2b_1b_0)$.

2. The Methodology

For an input byte $(a_7a_6a_5a_4a_3a_2a_1a_0)$, we find its multiplicative inverse $(b_7b_6b_5b_4b_3b_2b_1b_0)$, and find $(e_7e_6e_5e_4e_3e_2e_1e_0)$ such that:

$$\begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \tag{3}$$

Then, we find the output $(c_7c_6c_5c_4c_3c_2c_1c_0)$ as:

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{4}$$

First, we find a multiplicative inverse of

$a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \bmod\left(x^8 + x^4 + x^3 + x + 1\right)$.

Let $M_1 = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$,

$P = x^8 + x^4 + x^3 + x + 1$, and represent the multiplicative inverse by T.

We seek for q_1 and r_1 satisfying:

$$M_1q_1 + r_1 = Q_1 \tag{5}$$

where $Q_1 = P + 1$ [3], (look at **Table 1**).

If $r_1 = 0$, then $T = q_1$.

If $r_1 \neq 0$, we let $M_2 = r_1 + 1$ and seek for q_i and r_i satisfying:

$$M_i q_i + r_i = Q_i, \quad 2 \leq i \leq 7 \tag{6}$$

where $Q_i = M_{i-1}$, and $M_{i+1} = r_i$ (look at Table 2).

Whenever $r_i = 1$, then

$$T = T_i = q_i T_{i-1} + T_{i-2} \tag{7}$$

where $T_0 = 1$, and $T_1 = q_1$.

Then, to find $(e_7 e_6 e_5 e_4 e_3 e_2 e_1 e_0)$, we write the system (3), as follows:

$$[e] = \begin{bmatrix} X & Y \\ Y & X \end{bmatrix} [b] \tag{8}$$

$$e_i = Xb_i + Yb_j \tag{9}$$

$$e_j = Yb_i + Xb_j \tag{10}$$

where $0 \leq i \leq 3$, $4 \leq j \leq 7$, and

$$X = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \tag{11}$$

$$Y = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{12}$$

$$b_i = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}, \quad b_j = \begin{bmatrix} b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \tag{13}$$

Table 1. First step to find the multiplicative inverse.

i	M	q	r	Q
1	M_1	q_1	r_1	$Q_1 = P + 1$

Table 2. All steps to find the multiplicative inverse.

i	M	q	r	Q
1	M_1	q_1	r_1	$Q_1 = P + 1$
2	$M_2 = r_1 + 1$	q_2	r_2	$Q_2 = M_1$
3	$M_3 = r_2$	q_3	r_3	$Q_3 = M_2$
4	$M_4 = r_3$	q_4	r_4	$Q_4 = M_3$
5	$M_5 = r_4$	q_5	r_5	$Q_5 = M_4$
6	$M_6 = r_5$	q_6	r_6	$Q_6 = M_5$
7	$M_7 = r_6$	q_7	r_7	$Q_7 = M_6$

Then we compute

$$Xb_i = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_0 + b_1 \\ b_0 + b_1 + b_2 \\ b_0 + b_1 + b_2 + b_3 \end{bmatrix} \tag{14}$$

$$Yb_j = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} b_7 + b_6 + b_5 + b_4 \\ b_7 + b_6 + b_5 \\ b_7 + b_6 \\ b_7 \end{bmatrix} \tag{15}$$

$$Yb_i = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_3 + b_2 + b_1 + b_0 \\ b_3 + b_2 + b_1 \\ b_3 + b_2 \\ b_3 \end{bmatrix} \tag{16}$$

$$Xb_j = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} b_4 \\ b_4 + b_5 \\ b_4 + b_5 + b_6 \\ b_4 + b_5 + b_6 + b_7 \end{bmatrix} \tag{17}$$

$$Xb_i + Yb_j = \begin{bmatrix} b_0 \\ b_0 + b_1 \\ b_0 + b_1 + b_2 \\ b_0 + b_1 + b_2 + b_3 \end{bmatrix} + \begin{bmatrix} b_7 + b_6 + b_5 + b_4 \\ b_7 + b_6 + b_5 \\ b_7 + b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} b_0 + b_7 + b_6 + b_5 + b_4 \\ b_0 + b_1 + b_7 + b_6 + b_5 \\ b_0 + b_1 + b_2 + b_7 + b_6 \\ b_0 + b_1 + b_2 + b_3 + b_7 \end{bmatrix} \tag{18}$$

$$Yb_i + Xb_j = \begin{bmatrix} b_3 + b_2 + b_1 + b_0 \\ b_3 + b_2 + b_1 \\ b_3 + b_2 \\ b_3 \end{bmatrix} + \begin{bmatrix} b_4 \\ b_4 + b_5 \\ b_4 + b_5 + b_6 \\ b_4 + b_5 + b_6 + b_7 \end{bmatrix} = \begin{bmatrix} b_3 + b_2 + b_1 + b_0 + b_4 \\ b_3 + b_2 + b_1 + b_4 + b_5 \\ b_3 + b_2 + b_4 + b_5 + b_6 \\ b_3 + b_4 + b_5 + b_6 + b_7 \end{bmatrix} \tag{19}$$

The result is

$$\begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \end{bmatrix} = \begin{bmatrix} b_0 + b_7 + b_6 + b_5 + b_4 \\ b_0 + b_1 + b_7 + b_6 + b_5 \\ b_0 + b_1 + b_2 + b_7 + b_6 \\ b_0 + b_1 + b_2 + b_3 + b_7 \\ b_3 + b_2 + b_1 + b_0 + b_4 \\ b_3 + b_2 + b_1 + b_4 + b_5 \\ b_3 + b_2 + b_4 + b_5 + b_6 \\ b_3 + b_4 + b_5 + b_6 + b_7 \end{bmatrix} \tag{20}$$

and this satisfies:

$$e_i = b_i + b_{(i+4) \bmod (8)} + b_{(i+5) \bmod (8)} + b_{(i+6) \bmod (8)} + b_{(i+7) \bmod (8)}, \quad 0 \le i \le 7 \tag{21}$$

At the last, to find $(c_7c_6c_5c_4c_3c_2c_1c_0)$, we add $(e_7e_6e_5e_4e_3e_2e_1e_0)$ to 01100011.

3. Results

The matrices: Xb_i, Yb_j, Yb_i and Xb_j are just $(b_7b_6b_5b_4b_3b_2b_1b_0)$ with some

XOR operations. When multiplying X by b_i or b_j, the result will be:

(first element, first + second, first + second + third, first + second + third+ fourth) of b_i or b_j, and when multiplying Y by b_i or b_j, starting from the fourth element, the result will be:

(First + second + third + fourth, second + third + fourth, third + fourth, fourth) of b_i or b_j.

So, we can find $(e_7e_6e_5e_4e_3e_2e_1e_0)$ from $(b_7b_6b_5b_4b_3b_2b_1b_0)$ directly.

4. Example

To encrypt:

Input:

32 43 *F*6 *A*8 88 5*A* 30 8*D* 31 31 98 *A*2 *E*0 37 07 34

Key:

2*B* 7*E* 15 16 28 *AE* *D*2 *A*6 *AB* *F*7 15 88 09 *CF* 4*F* 3*C*

using AES [1].

Let us do the first step (Rijndael ByteSub transformation).

$$\begin{bmatrix} 32 & 88 & 31 & E0 \\ 43 & 5A & 31 & 37 \\ F6 & 30 & 98 & 07 \\ A8 & 8D & A2 & 34 \end{bmatrix} + \begin{bmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & A6 & 88 & 3C \end{bmatrix} = \begin{bmatrix} 19 & .. & .. & .. \\ .. & .. & .. & .. \\ .. & .. & .. & .. \\ .. & .. & .. & .. \end{bmatrix}$$

We just transform the element {19},

$$19 = 00011001 = x^4 + x^3 + 1$$

Computing the multiplicative inverse, (look at **Table 3**).

Since $r_2 = 1$,

$$\begin{aligned} T &= T_2 \\ &= q_2 T_1 + T_0 \\ &= x\left(x^4 + x^3 + x^2 + x + 1\right) + 1 \\ &= x^5 + x^4 + x^3 + x^2 + x + 1 \\ &= 00111111 \end{aligned}$$

Now, we take (00111111), to do the second operation.

$$\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Then we add the result to (01100011)

Table 3. Steps finish when $r_2 = 1$.

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

$$\begin{bmatrix}1\\1\\1\\0\\1\\1\\0\\1\end{bmatrix} + \begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\\1\\0\\1\\1\end{bmatrix}$$

So,

$$19 \to 11010100 = D4$$

5. Conclusion

The modern technique proposed in this work equivalently finds the Rijndael byte substitute transformation without a need to compute multiplicative inverses and matrices multiplication by traditional methods.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology (NIST), November 26, 2001.

[2] Menezes, A., van Oorschot, P. and Vanstone, S. (1997) Handbook of Applied Cryptography. CRC Press, New York.

[3] Ahmed, W. (2019) Some Techniques to Compute Multiplicative Inverses for Advanced Encryption Standard. *Journal of Advances in Mathematics*, **16**, 8208-8212. https://doi.org/10.24297/jam.v16i0.8016