Scientific Research Publishing

Applied Mathematics, 2019, 10, 234-244
http://www.scirp.org/journal/am
ISSN Online: 2152-7393
ISSN Print: 2152-7385

A Modern Method for Constructing the S-Box of Advanced Encryption Standard

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) A Modern Method for Constructing the S-Box of Advanced Encryption Standard. *Applied Mathematics*, **10**, 234-244.
https://doi.org/10.4236/am.2019.104018

Received: March 22, 2019
Accepted: April 26, 2019
Published: April 29, 2019

Abstract

The substitution table (S-Box) of Advanced Encryption Standard (AES) and its properties are key elements in cryptanalysis ciphering. We aim here to propose a straightforward method for the non-linear transformation of AES S-Box construction. The method reduces the steps needed to compute the multiplicative inverse, and computes the matrices multiplication used in this transformation, without a need to use the characteristic matrix, and the result is a modern method constructing the S-Box.

Keywords

Advanced Encryption Standard, S-Box, Extended Euclidean Algorithm, Greatest Common Divisor, XOR Operation

1. Introduction

The S-Box table of AES is taken as a lookup table to substitute an input byte by another, this table is constructed using a non-linear transformation depends on the usual method taking more calculation steps to give the corresponding byte.

The S-Box plays a fundamental role in encryption and decryption processes, as byte substitution appears in many steps. At the first round of the encryption process, we add the plaintext matrix to the key matrix, then we substitute each byte by another byte according to S-Box, for example, to substitute the byte *xy*(say), we take the byte in the cell that has *x* as the column index and *y* as the row index, we do this substitute byte step in all rounds of the encryption process, and in all round of the decryption process, we do the inverse substitute byte step, to substitute the byte *xy*(say), we take the index of the column, and the index of the row of the cell that contains *xy*, as the left and the right character of the result byte, respectively. The S-Box (Table 1), involves substitution bytes for all

bytes from {00} to {*FF*} in hexdecimal presentation.

The S-Box is constructed using the following operations [1]:

1) Finding the multiplicative inverse of an input byte in the finite field $GF\left(2^8\right)$ based on the irreducible polynomial $P(x)=x^8+x^4+x^3+x+1$.
2) Multiplying this multiplicative inverse by a specific matrix (matrix *M*).
3) Adding the multiplication result to a specific vector $\left(\{63\}=01100011\right)$.

We convert the hexadecimal presentation of the input byte into binary presentation as $\left(a_7a_6a_5a_4a_3a_2a_1a_0\right)$ and write it as a polynomial $A(x)=a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$, let its multiplicative inverse be $T(x)=t_7x^7+t_6x^6+t_5x^5+t_4x^4+t_3x^3+t_2x^2+t_1x+t_0$, we multiply $T(x)$ by the following characteristic matrix:

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

Then, we add the result to (01100011).

We note that, for the input {00} the output is {63}.

Table 1. The AES S-Box.

	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

1.1. Problem Statement

We search for an easier and straightforward method for constructing the AES S-Box.

1.2. Proposed Solution

The multiplicative inverse of an input byte can be computed in clear steps using an iterated formula.

Multiplying the multiplicative inverse matrix by the characteristic matrix can be determined directly from this multiplicative inverse using simple XOR operations, without a need to use the characteristic matrix.

2. Traditional Way

In cryptography, the extended Euclidean algorithm has wide uses especially for finding a multiplicative inverse (modular inverse).

Euclidean algorithm is used to find the greatest common divisor of two integers *a* and *b*, (denoted by $\gcd(a,b)$).

When $b > a$, and

$$b - r = aq \tag{2}$$

for some integers *r* and *q*, we say

$$r = b \pmod a \tag{3}$$

and if $b \pmod a = 0$ then

$$\gcd(a,b) = a \tag{4}$$

With the polynomials $A(x)$ and $P(x)$, we write $\gcd(A(x),P(x))$ [2].

The algorithm below gives $\gcd(A(x),P(x))$, where $A(x) < P(x)$

Algorithm (1): Euclidean algorithm [3]

Input: Polynomials $A(x), P(x)$.

Output: $\gcd(A(x),P(x))$.

1) While $A(x) \neq 0$ do

a) $r(x) = P(x) \bmod A(x)$, $P(x) = A(x)$, $A(x) = r(x)$.

2) Return $P(x)$.

The step (1.(a)) of the algorithm (1) involves the division algorithm:

$$P(x) = A(x)q(x) + r(x) \tag{5}$$

where $0 \le r(x) = P(x) \bmod A(x) < A(x)$.

It implies that [4]

$$\gcd(A(x),P(x)) = \gcd(A(x),r(x)) \tag{6}$$

If $r(x) \neq 0$, the step will be repeated, let us write the repeated application of the division algorithm as:

$$P(x) = q_1(x)A(x) + r_1(x), \quad 0 \le r_1(x) < A(x)$$

$$A(x)=q_2(x)r_1(x)+r_2(x),\quad 0\le r_2(x)<r_1(x)$$
$$r_1(x)=q_3(x)r_2(x)+r_3(x),\quad 0\le r_3(x)<r_2(x)$$
$$\cdots$$
$$r_{i-3}(x)=q_{i-1}(x)r_{i-2}(x)+r_{i-1}(x),\quad 0\le r_{i-1}(x)<r_{i-2}(x)$$
$$r_{i-2}(x)=q_i(x)r_{i-1}(x)+r_i(x),\quad 0\le r_i(x)<r_{i-1}(x) \tag{7}$$

When $r_i(x)=0$, and since

$$\gcd\left(A(x),P(x)\right)=\gcd\left(r_{i-1}(x),r_i(x)\right) \tag{8}$$

we get

$$\gcd\left(A(x),P(x)\right)=r_{i-1}(x) \tag{9}$$

The extended form of the Euclidean algorithm is called Extended Euclidean algorithm, it gives (besides $\gcd\left(A(x),P(x)\right)$, $X(x)$ and $Y(x)$ such that

$$\gcd\left(A(x),P(x)\right)=A(x)X(x)+P(x)Y(x) \tag{10}$$

Rewrite the equations of the system (7) as:

$$r_1(x)=P(x)-q_1(x)A(x)$$
$$r_2(x)=A(x)-q_2(x)r_1(x)$$
$$r_3(x)=r_1(x)-q_3(x)r_2(x)$$
$$\cdots$$
$$r_{i-2}(x)=r_{i-4}(x)-q_{i-2}(x)r_{i-3}(x)$$
$$r_{i-1}(x)=r_{i-3}(x)-q_{i-1}(x)r_{i-2}(x) \tag{11}$$

Then, in the last equation of system (11), $r_{i-1}(x)=r_{i-3}(x)-q_{i-1}(x)r_{i-2}(x)$, replace $r_{i-2}(x)$ with its value from the above equation (it involves $r_{i-3}(x)$), then replace $r_{i-3}(x)$ with its value from the above equation, continue doing this replacement, we obtain

$$\begin{aligned} r_{i-1}(x)=r_{i-3}(x)&-\left(q_{i-1}(x)\right)\left(r_{i-4}(x)-\left(q_{i-2}(x)\right)\left(r_{i-5}(x)-\left(q_{i-3}(x)\right)\right.\right.\\ &\times\left.\left.\left(r_{i-6}(x)-\left(q_{i-4}(x)\right)\left((\cdots)\left(P(x)-q_1(x)A(x)\right)\right)\right)\right)\right) \end{aligned} \tag{12}$$

Equation (12) takes the form

$$r_{i-1}(x)=A(x)X(x)+P(x)Y(x) \tag{13}$$

In our problem $1\le i<8$, and since the multiplicative inverse only exists when the *gcd* is 1 [5].

$$r_{i-1}(x)=1 \tag{14}$$

The multiplicative inverse [2] of $A(x)$ modulo $P(x)$ is $A^{-1}(x)$ such that

$$A(x)A^{-1}(x)=1\left(\bmod P(x)\right) \tag{15}$$

When $\gcd\left(A(x),P(x)\right)=1$,

$$1=A(x)X(x)+P(x)Y(x) \tag{16}$$

$$1\left(\mathrm{mod}\,P(x)\right)=\left(A(x)X(x)+P(x)Y(x)\right)\left(\mathrm{mod}\,P(x)\right) \tag{17}$$

and since

$$P(x)Y(x)=0\left(\mathrm{mod}\,P(x)\right) \tag{18}$$

we get

$$X(x)=A^{-1}(x) \tag{19}$$

So, the procedure of the extended Euclidean algorithm finds the greatest common divisor, also it finds the multiplicative inverse.

Below an algorithm to find $A^{-1}(x)$, we will denote $A^{-1}(x)$ by $T(x)$.

Algorithm (2): Extended Euclidean algorithm [3]

Input: Polynomials $A(x), P(x)$.

Output: The multiplicative inverse of $A(x)$.

1)Set $y_2(x)=0$, $y_1(x)=1$.

2) While $A(x)\neq 1$ do

a) $q(x)=P(x)divA(x)$, $r(x)=P(x)+q(x)A(x)$.

b) $y(x)=y_2(x)+y_1(x)q(x)$

c) $y_2(x)=y_1(x)$, $y_1(x)=y(x)$.

d) $P(x)=A(x)$, $A(x)=r(x)$.

3) Return $y_1(x)$.

Now, we have $T(x)=(t_7t_6t_5t_4t_3t_2t_1t_0)$, we multiply it (from the left) by matrix M

$$M\left(T(x)\right)=\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}\begin{bmatrix}t_0\\t_1\\t_2\\t_3\\t_4\\t_5\\t_6\\t_7\end{bmatrix}=\begin{bmatrix}t_0+t_4+t_5+t_6+t_7\\t_0+t_1+t_5+t_6+t_7\\t_0+t_1+t_2+t_6+t_7\\t_0+t_1+t_2+t_3+t_7\\t_0+t_1+t_2+t_3+t_4\\t_1+t_2+t_3+t_4+t_5\\t_2+t_3+t_4+t_5+t_6\\t_3+t_4+t_5+t_6+t_7\end{bmatrix} \tag{20}$$

Then, we add the result to $(\{63\}=01100011)$ to obtain the output of the input $A(x)=(a_7a_6a_5a_4a_3a_2a_1a_0)$

$$\begin{bmatrix}t_0+t_4+t_5+t_6+t_7\\t_0+t_1+t_5+t_6+t_7\\t_0+t_1+t_2+t_6+t_7\\t_0+t_1+t_2+t_3+t_7\\t_0+t_1+t_2+t_3+t_4\\t_1+t_2+t_3+t_4+t_5\\t_2+t_3+t_4+t_5+t_6\\t_3+t_4+t_5+t_6+t_7\end{bmatrix}+\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix}=\begin{bmatrix}t_0+t_4+t_5+t_6+t_7+1\\t_0+t_1+t_5+t_6+t_7+1\\t_0+t_1+t_2+t_6+t_7\\t_0+t_1+t_2+t_3+t_7\\t_0+t_1+t_2+t_3+t_4\\t_1+t_2+t_3+t_4+t_5+1\\t_2+t_3+t_4+t_5+t_6+1\\t_3+t_4+t_5+t_6+t_7\end{bmatrix} \tag{21}$$

Example

Using the traditional way, we want to find the output byte that corresponding to the input byte {53} (Table 2).

$$\{53\}=01010011,\quad A(x)=x^6+x^4+x+1,\quad P(x)=x^8+x^4+x^3+x+1.$$

Iteration 1

$y_2(x)=0$, $y_1(x)=1$,

$q(x)=x^2+1$, $r(x)=x^2$,

$y(x)=x^2+1$, $y_2(x)=1$, $y_1(x)=x^2+1$,

$P(x)=x^6+x^4+x+1$, $A(x)=x^2$.

Iteration 2

$q(x)=x^4+x^2$, $r(x)=x+1$,

$y(x)=x^6+x^2+1$, $y_2(x)=x^2+1$, $y_1(x)=x^6+x^2+1$,

$P(x)=x^2$, $A(x)=x+1$.

Iteration 3

$q(x)=x+1$, $r(x)=1$,

$y(x)=x^7+x^6+x^3+x$, $y_2(x)=x^6+x^2+1$, $y_1(x)=x^7+x^6+x^3+x$,

$P(x)=x+1$, $A(x)=1$.

$$T(x)=y_1(x)=x^7+x^6+x^3+x=11001010.$$

$$\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}\begin{bmatrix}0\\1\\0\\1\\0\\0\\1\\1\end{bmatrix}=\begin{bmatrix}0\\1\\1\\1\\0\\0\\0\\1\end{bmatrix} \tag{22}$$

$$\begin{bmatrix}0\\1\\1\\1\\0\\0\\0\\1\end{bmatrix}+\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\1\\1\\0\\1\\1\\1\end{bmatrix} \tag{23}$$

The output is $11101101=ED$.

Table 2. To find the output of {53}.

	…	3	…
⋮	…	…	…
5	…	??	…
⋮	…	…	…

3. Modern Way

We use the formula [6] below to find the multiplicative inverse.

3.1. The Iterated Formula

The iterated formula

$$T_i(x)=\left(q_i(x)\right)\left(T_{i-1}(x)\right)+T_i(x),\quad 2\le i<8 \tag{24}$$

where $T_0(x)=1, T_1(x)=q_1(x)$, gives the multiplicative inverse $T=T_i$ when $r_i=1$.

To show that, we use the system (11).

When $i=1$, $r_1(x)=1$,

$$r_1(x)=P(x)-\left(q_1(x)\right)\left(A(x)\right) \tag{25}$$

$$1=P(x)-\left(q_1(x)\right)\left(A(x)\right) \tag{26}$$

We obtain $T(x)=q_1(x)=T_1(x)$. (Equation (24), takes this as given).

When $i=2$, $r_2(x)=1$, $r_1(x)\neq 0$,

$$r_2(x)=A(x)-\left(q_2(x)\right)\left(r_1(x)\right) \tag{27}$$

$$\begin{aligned}1&=A(x)-\left(q_2(x)\right)\left(P(x)-\left(q_1(x)\right)\left(A(x)\right)\right)\\&=\left(1-\left(q_2(x)\right)\left(q_1(x)\right)\right)\left(A(x)\right)-\left(q_2(x)\right)\left(P(x)\right)\\&=\left(1-\left(q_2(x)\right)\left(q_1(x)\right)\right)\left(A(x)\right)-\left(q_2(x)\right)\left(P(x)\right)\end{aligned} \tag{28}$$

We obtain $T(x)=\left(q_2(x)\right)\left(q_1(x)\right)+1$. From Equation (24)

$$T(x)=T_2(x)=q_2(x)T_1(x)+T_0(x)=\left(q_2(x)\right)\left(q_1(x)\right)+1 \tag{29}$$

When $i=3$, $r_3(x)=1$, $r_1(x)\neq 0$, $r_2(x)\neq 0$,

$$r_3(x)=r_1(x)-q_3(x)r_2(x) \tag{30}$$

$$\begin{aligned}1&=P(x)-q_1(x)A(x)-q_3(x)\left(\left(1-q_2(x)q_1(x)\right)A(x)-q_2(x)P(x)\right)\\&=\left(\left(q_3(x)\right)\left(1-q_2(x)q_1(x)\right)-q_1(x)\right)A(x)+K(x)P(x)\end{aligned} \tag{31}$$

We obtain

$$T(x)=\left(q_3(x)\right)\left(1-\left(q_2(x)\right)\left(q_1(x)\right)\right)-q_1(x)=q_3(x)T_2(x)+T_1(x) \tag{32}$$

and from Equation (24)

$$T(x)=T_3(x)=q_3(x)T_2(x)+T_1(x) \tag{33}$$

By this way, we can show that Equation (24) gives $T(x)$ for $2\le i<8$, when $r_i=1$.

Below an algorithm to find $T(x)$ using the modern way.

Algorithm (3): Modern way to find a multiplicative inverse

Input: Polynomials $A(x), P(x)$.

Output: $T(x)$, the multiplicative inverse of $A(x)$.

1) Set $T_0(x)=0$, $T_1(x)=1$.

2) $q(x)=P(x)divA(x)$, $r(x)=P(x)+q(x)A(x)$.

3) $T(x)=q(x)T_1(x)+T_0(x)$

4) If $r_i(x)=1$ then return $T(x)$, stop.

5) Else $P(x)=A(x)$, $A(x)=r(x)$.

$T_0(x)=T_1(x)$, $T_1(x)=T(x)$.

6) Go to 2

Now, we want to multiply $T(x)$ by the matrix *M*.

First, write *M* as [7]

$$M=\begin{bmatrix}\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&0\\1&1&1&1\end{bmatrix} & \begin{bmatrix}1&1&1&1\\0&1&1&1\\0&0&1&1\\0&0&0&1\end{bmatrix}\\ \begin{bmatrix}1&1&1&1\\0&1&1&1\\0&0&1&1\\0&0&0&1\end{bmatrix} & \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&0\\1&1&1&1\end{bmatrix}\end{bmatrix} \tag{34}$$

Let

$$M_1=\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&0\\1&1&1&1\end{bmatrix},\quad M_2=\begin{bmatrix}1&1&1&1\\0&1&1&1\\0&0&1&1\\0&0&0&1\end{bmatrix} \tag{35}$$

And write $T(x)$ as

$$T=\begin{bmatrix}\begin{bmatrix}t_0\\t_1\\t_2\\t_3\end{bmatrix}\\ \begin{bmatrix}t_4\\t_5\\t_6\\t_7\end{bmatrix}\end{bmatrix} \tag{36}$$

Let

$$T_1=\begin{bmatrix}t_0\\t_1\\t_2\\t_3\end{bmatrix},\quad T_2=\begin{bmatrix}t_4\\t_5\\t_6\\t_7\end{bmatrix} \tag{37}$$

Then

$$M_1T_1 = \begin{bmatrix} t_0 \\ t_0 + t_1 \\ t_0 + t_1 + t_2 \\ t_0 + t_1 + t_2 + t_3 \end{bmatrix} \tag{38}$$

$$M_1T_2 = \begin{bmatrix} t_4 \\ t_4 + t_5 \\ t_4 + t_5 + t_6 \\ t_4 + t_5 + t_6 + t_7 \end{bmatrix} \tag{39}$$

$$M_2T_1 = \begin{bmatrix} t_3 + t_2 + t_1 + t_0 \\ t_3 + t_2 + t_1 \\ t_3 + t_2 \\ t_3 \end{bmatrix} \tag{40}$$

$$M_2T_2 = \begin{bmatrix} t_7 + t_6 + t_5 + t_4 \\ t_7 + t_6 + t_5 \\ t_7 + t_6 \\ t_7 \end{bmatrix} \tag{41}$$

So, the multiplication of M and $T(x)$ gives

$$\begin{bmatrix} M_1T_1 + M_2T_2 \\ M_2T_1 + M_1T_2 \end{bmatrix}$$

From Equation (38) and Equation (39), we note that the results of these multiplications give the form

$$\begin{bmatrix} \text{first element} \\ \text{first} + \text{second} \\ \text{first} + \text{second} + \text{third} \\ \text{first} + \text{second} + \text{third} + \text{fourth} \end{bmatrix}$$

of the second matrix, and similarly, Equation (40) and Equation (41), show that the results give the form

$$\begin{bmatrix} \text{fourth} + \text{third} + \text{second} + \text{first} \\ \text{fourth} + \text{third} + \text{second} \\ \text{fourth} + \text{third} \\ \text{fourth} \end{bmatrix}$$

of the second matrix, so we don't need to use matrix M, as the traditional method.

In the last step, we add $M(T(x))$ to $(\{63\} = 01100011)$.

3.2. Example

Using the modern way, we want to find the output of {53}

$$\{53\} = 01010011, \quad A(x) = x^6 + x^4 + x + 1, \quad P(x) = x^8 + x^4 + x^3 + x + 1.$$

First, finding the multiplicative inverse (Table 3).

Table 3. Finding multiplicative inverse of {53}.

i	$A(x)$	$q(x)$	$r(x)$	$P(x)$
1	x^6+x^4+x+1	x^2+1	x^2+1	$x^8+x^4+x^3+x+1$
2	x^2+1	x^4+x^2	$x+1$	x^6+x^4+x+1
3	$x+1$	$x+1$	1	x^2+1

Since $r_3(x)=1$,

$$\begin{aligned} T(x)=T_3(x)&=\left(q_3(x)\right)T_2(x)+T_1(x)\\ &=\left(q_3(x)\right)\left(\left(q_2(x)\right)\left(q_1(x)\right)+1\right)+q_1(x)\\ &=(x+1)\left[\left(x^4+x^2\right)\left(x^2+1\right)+1\right]+x^2+1\\ &=x^7+x^6+x^3+x\\ &=11001010 \end{aligned}$$

Then, computing the matrices multiplication:

$$\begin{bmatrix}0\\1\\0\\1\\0\\0\\1\\1\end{bmatrix}\rightarrow\begin{bmatrix}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}&\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\\\begin{bmatrix}0\\0\\1\\1\end{bmatrix}&\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\end{bmatrix}=\begin{bmatrix}0\\1\\1\\1\\0\\0\\0\\1\end{bmatrix} \tag{42}$$

Last, adding (01100011)

$$\begin{bmatrix}0\\1\\1\\1\\0\\0\\0\\1\end{bmatrix}+\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\1\\1\\0\\1\\1\\1\end{bmatrix} \tag{43}$$

So, the output is $11101101=ED$.

4. Conclusions

In this paper, a straightforward method for obtaining the Advanced Encryption Standard S-Box look-up table without the traditional use of the characteristic Matrix M is proposed. We have demonstrated that the two methods are equivalent. In addition, the multiplicative inverse of $A(x)$ has been found more elegantly.

In future work, we will investigate the properties and the impact of this technique on cipher complexity analysis.

Conflicts of Interest

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

References

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

[2] Burton, D.M. (2007) Elementary Number Theory. 6th Edition, McGraw-Hill, New York.

[3] Menezes, A., van Oorschot, P. and Vanstone, S. (1997) Handbook of Applied Cryptography. CRC Press, New York. https://doi.org/10.1201/9781439821916

[4] Cormen, T.H., Leiserson, C.E., Rivest, R.L. and Stein, C. (2009) Introduction to Algorithms. 3rd Edition, The MIT Press, Cambridge, London.

[5] Ahmed, W.E. (2019) A Way to Compute a Greatest Common Divisor in the Galois Field (GF (2^n)). *Journal of Advances in Mathematics*, **16**, 8317-8321. https://doi.org/10.24297/jam.v16i0.8167

[6] Ahmed, W.E. (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

[7] Ahmed, W.E. (2019) On Rijndael ByteSub Transformation. *Applied Mathematics*, **10**, 113-118. https://doi.org/10.4236/am.2019.103010