BAREKENG: Journal of Mathematics and Its Applications
December 2024 Volume 18 Issue 4 Page 2329–2344
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol18iss4pp2329-2344

S-BOX CONSTRUCTION IN THE ADVANCED ENCRYPTION STANDARD (AES) DEVELOPMENT ALGORITHM IN $GF(2^2)$, $GF(2^4)$ & $GF(2^6)$

Adi Setiawan[1*], Faldy Tita[2], Bambang Susanto[3]

[1,3]Department of Data Science, Faculty of Science and Mathematics, Satya Wacana Christian University, Salatiga, Jawa Tengah 50711, Indonesia
[2]Department of Mathematics, Faculty of Science and Mathematics, Satya Wacana Christian University, Salatiga, Jawa Tengah 50711, Indonesia
*Corresponding author's e-mail: ** ***adi.setiawan@uksw.edu***

ABSTRACT

Article History:

Received: 4th, March 2024
Revised: 22nd, May 2024
Accepted: 18th, July 2024
Published:14th, October 2024

This research aims to obtain a method for constructing S-boxes based on $GF(2^2)$, $GF(2^4)$ and $GF(2^6)$. A review of the Galois Field $GF(2^m)$ is presented for $m = 1,2,3,4,5$ and 6. Furthermore, it is used to construct an S-box based on $GF(2^2)$, $GF(2^4)$ and $GF(2^6)$. Based on these results, later it can be developed for S-box construction in the AES algorithm which uses the Galois Field $GF(2^m)$ for $m \geq 10$.

Keywords:

AES Algorithm;
Galois Field;
Irreducible Polynomial;
S-box.

How to cite this article:

A. Setiawan, F. Tita and B. Susanto., "S-BOX CONSTRUCTION IN THE ADVANCED ENCRYPTION STANDARD (AES) DEVELOPMENT ALGORITHM IN *GF* (2^2), *GF* (2^4) & *GF* (2^6)," *BAREKENG: J. Math. & App.*, vol. 18, iss. 4, pp. 2329-2344, December, 2024.

1. INTRODUCTION

In cryptography, a finite field, or Galois field, is used in the Rijndael algorithm (Advanced Encryption Standard - AES) and ECC (Elliptic Curve Cryptography). Various studies on the Galois Field can be seen in Aidoo & Gyam's paper entitled "Construction of Irreducible Polynomial in Galois Field $GF(2^m)$ Using Normal Bases", which proposes how to construct irreducible polynomials in $GF(2^m)$ using normal bases [1]. Furthermore, Chandoul & Sibih in the paper "Note on irreducible polynomial over finite field" proposes how to expand the criteria of irreducibility over finite fields [2]. As well, Nithya & Ramadoss in a paper entitled "Extension fields and Galois Theory", reviews how an expansion field is formed from smaller fields and discusses finite fields in Galois Theory [3]. In addition, Dey & Ghosh in a paper entitled "Search for Monic Irreducible Polynomials with Decimal Equivalents of Polynomials over Galois Field $GF(p^q)$", proposes how to find monic and irreducible polynomials over Galois Field $GF(p^q)$ [4].

Other studies presented how the Galois field is used in cryptography, such as in the Rijndael algorithm and ECC (Elliptic Curve Cryptography). The paper "Hardware Implementation of Galois Field Multiplication for Mix Column and Inverse Mix Column Process in Encryption-decryption Algorithm" [5], proposed a method for implementing Galois Field Multiplication with the help of Matlab and Field Programmable Gate Array (FPGA) devices. Furthermore, a paper entitled "AES S-Box Hardware with Efficiency Improvement Based on Linear Mapping Optimization" [6] proposes how to design a new S-Box in the AES algorithm based on Linear Mapping optimization. Likewise, a paper entitled "Improved Rijndael by Encryption S-Box Using NTRU Algorithm" [7] proposes using the NTRU algorithm to improve the Rijndael Algorithm with S-Box encryption. On the other hand, a paper entitled "Modification of Advanced Encryption Standard (AES) Algorithm with Perfect Strict Avalanche Criterion S-Box" [8] proposes how to modify the AES Algorithm with Perfect SAC (Strict Avalanche Criterion) S-Box.

The AES algorithm uses the Galois Field $GF(2^m)$, where $m = 8$. Likewise, in the papers mentioned above, it appears that there has been no research on how to construct an S-box in the AES algorithm, which uses the Galois Field $GF(2^m)$ for $m = 2, 4$ and 6. In this paper, we will explain how to construct an S-box in the AES algorithm which uses the Galois Field $GF(2^m)$ for $m = 2, 4$ and 6. Based on these results, later it can be developed for S-box construction in the AES algorithm which uses the Galois Field $GF(2^m)$ for $m \geq 10$.

2. RESEARCH METHODS

This section covers the topics of group theory, ring theory, field theory, polynomial rings, and extension fields. Furthermore, the Galois Field $GF(2^m)$ for $m = 1, 2, 3, 4, 5$ and 6 is also presented. The following definitions are taken from Ref [9].

Definition 1. A group G is a set with a binary operation (generally called product) $G \times G \to G$, $(a, b) \to a \cdot b$ for $a, b \in G$ which satisfy the following three axioms.

(G1) The product is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for every $a, b, c \in G$.

(G2) There is an identity element e in G: $a \cdot e = e \cdot a = a$, for every $a \in G$.

(G3) Each element a in G has an inverse $a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$.

We generally denote the above group G as $(G, \cdot, e)$, and $a \cdot b$ is denoted by ab for convenience. A group G is called abelian if $ab = ba$ for all $a, b \in G$.

Example 1. We have the following familiar examples of groups: $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$, $(\mathbb{Q}^*, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$, $(\mathbb{C}^*, \cdot, 1)$.

Definition 2. A ring R is a set with two binary operations, $+$ and $\cdot$, satisfying:

(R1) $(R, +, 0)$ is an abelian group,

(R2) associativity under multiplication: $(ab)c = a(bc)$ for all $a, b, c \in R$,

(R3) distributivities: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$.

The ring R is usually denoted as $(R, +, \cdot)$. From now on, we always assume that R is a ring. A ring R is called commutative if $ab = ba$ for all $a, b \in R$.

Example 2. We can easily see that the following number systems are rings: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$.

Definition 3. A finite field F is a system $(F, +, \cdot)$ where F is a finite set and $+, \cdot$ are binary operations on F such that all of the field axioms hold for both addition and multiplication. The field axioms include associativity, commutativity, distributivity, identity, and inverses. In other words, the finite field must satisfy the following properties:

1. $(F, +)$ is an abelian group where 0 is the identity element.

2. Let $F^* = F - 0$. $(F^*, \cdot)$ is an abelian group where 1 is the identity element.

3. For all elements $a, b, c \in F$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

Example 3. A simple example of a finite field is $\mathbb{Z}_2 = \{0, 1\}$. Addition in this field is like XOR $(0 + 0 = 1 + 1 = 0$ and $1 + 0 = 0 + 1 = 1)$. Multiplication in this field is like AND $(1 \cdot 1 = 1$ and $0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0)$. It can be proved that all the properties of finite fields are satisfied in $\mathbb{Z}_2$.

Lemma 1. *The element of Galois Field $GF\ (2^2)$ is defined as $GF\ (2^2) = \{0, 1\} \cup \{2, 3\}$.*

A polynomial is defined as irreducible if it cannot be factored into nontrivial polynomials over the same field. In the finite field $GF\ (2)$, $x^2 + x + 1$ is irreducible, but $x^2 + 1$ is not, since $(x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1 \pmod 2$. Furthermore, the third-degree polynomial on $GF\ (2)$ which is an irreducible polynomial is $p(x) = x^3 + x + 1$ and $p(x) = x^3 + x^2 + 1$, but $p(x) = x^3 + 1$, $p(x) = x^3 + x^2 + x + 1$ are not irreducible polynomials. The first few numbers of irreducible polynomial (mod 2) for $n = 1, 2, 3, 4, 5$ and 6 are $2, 1, 2, 3, 6$ and 9. The following table (**Table 1**) presents irreducible polynomials of degrees 4, 5, and 6 over $GF\ (2)$. In general, the number of irreducible polynomials of degree n over the finite $GF(q)$ is given by:

$$L_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

where $\mu(n)$ is the Mobius function. For further information, it can be obtained at [10].

Table 1. Table of Irreducible Polynomial degrees 4, 5, and 6 over $\mathbb{Z}_2$.

Regular (Decimal)	Binary Vector	Polynomial Form
19	10011	$x^4 + x + 1$
25	11001	$x^4 + x^3 + 1$
31	11111	$x^4 + x^3 + x^2 + x + 1$
37	100101	$x^5 + x^2 + 1$
41	101001	$x^5 + x^3 + 1$
47	101111	$x^5 + x^3 + x^2 + x + 1$
55	110111	$x^5 + x^4 + x^2 + x + 1$
59	111011	$x^5 + x^4 + x^3 + x + 1$
61	111101	$x^5 + x^4 + x^3 + x^2 + 1$
67	1000011	$x^6 + x + 1$
73	1001001	$x^6 + x^3 + 1$
87	1010111	$x^6 + x^4 + x^2 + x + 1$
91	1011011	$x^6 + x^4 + x^3 + x + 1$
97	1100001	$x^6 + x^5 + 1$
103	1100111	$x^6 + x^5 + x^2 + x + 1$
109	1101101	$x^6 + x^5 + x^3 + x^2 + 1$
115	1110011	$x^6 + x^5 + x^4 + x + 1$
117	1110101	$x^6 + x^5 + x^4 + x^2 + 1$

Example 4. Suppose it is known that the finite field $\mathbb{Z}_2 = \{0, 1\}$. The polynomial of degree 2 over $\mathbb{Z}_2$ namely $p(x) = x^2 + x + 1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots $\mathbb{Z}_2 = GF(2)$. Choose α in the extension field F so that $p(\alpha) = \alpha^2 + \alpha + 1 = 0$ or $\alpha^2 = \alpha + 1$. Consequently, $\alpha^3 = \alpha(\alpha^2) = \alpha(\alpha + 1) = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 1$. That means the extension field has members $0, 1, \alpha$

and α^2 (or $\alpha + 1$) so that the extension field that is formed, namely $F = \{0, 1, \alpha, \alpha^2\}$ contains $\mathbb{Z}_2$. In this case, $p(x) = x^2 + x + 1$ is said to be a primitive polynomial, namely a polynomial that constructs all the elements of an extension field from a base field. The sum of the elements in F can be stated in Table 2 while the multiplication of the elements in F can be stated in Table 3. In addition, $F^* = F - \{0\} = \{1, \alpha, \alpha + 1\} = \{1, \alpha, \alpha^2\}$ can be considered as groups under the multiplication operation. Furthermore, the F^* group is a cyclic group with order 3 which is a prime number so that every element that is not an identity element, namely α and $\alpha + 1$, is a generator element. Based on Theorem 1, F isomorphic with $GF(2^2) = \{0, 1, 2, 3\}$. $GF(2^2)$ can also be expressed in binary system $\{00, 01, 10, 11\}$. Furthermore, Figure 1 presents the relation between $\mathbb{Z}_2 = GF(2) = \{0, 1\}$ and $GF(2^2) = GF(4) = \{0, 1, \alpha, \alpha + 1\}$. Various information about the definition of ring homomorphisms, polynomial rings, expansion fields, ring quotients can be seen in Ref [11].

Table 2. Addition Operation in Extension Field $GF(2^2)$.

$+$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\alpha}$	$\boldsymbol{\alpha + 1}$
$\mathbf{0}$	0	1	α	$\alpha + 1$
$\mathbf{1}$	1	0	$\alpha + 1$	α
$\boldsymbol{\alpha}$	α	$\alpha + 1$	0	1
$\boldsymbol{\alpha + 1}$	$\alpha + 1$	α	1	0

Table 3. The Multiplication Operation in the Extension Field $GF(2^2)$.

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\alpha}$	$\boldsymbol{\alpha + 1}$
$\mathbf{0}$	0	0	0	0
$\mathbf{1}$	0	1	α	$\alpha + 1$
$\boldsymbol{\alpha}$	0	α	$\alpha + 1$	1
$\boldsymbol{\alpha + 1}$	0	$\alpha + 1$	1	α

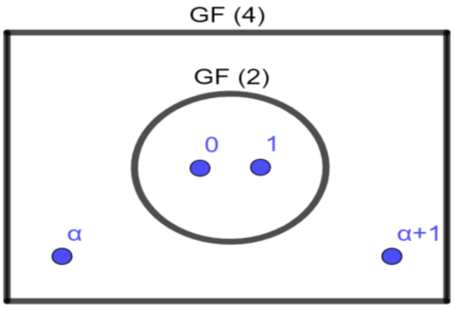

Figure 1. Relationship between $\mathbb{Z}_2 = GF(2)$ and $GF(2^2) = GF(4)$.

Theorem 1. *The element of Galois Field $GF(p^n)$ is defined as*

$$GF(p^n) = \{0, 1, \dots, p - 1\} \cup \{p, p + 1, \dots, p + p - 1\} \cup \dots \cup \{p^{n-1}, p^{n-1} + 1, p^{n-1} + p - 1\}.$$

where p is a prime number and n is a positive integer.

Theorem 1 gives the results obtained about the Galois Field $GF(2^m)$ with $m = 3, 4, 5$ and 6 which are given in the following examples.

Example 5. The polynomial of degree 3 over $\mathbb{Z}_2$, namely $p(x) = x^3 + x + 1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots $\mathbb{Z}_2 = GF(2)$. Choose α in the extension field F from $\mathbb{Z}_2$ so that $p(\alpha) = \alpha^3 + \alpha + 1 = 0$ or $\alpha^3 = \alpha + 1$. Then we get $\alpha^4 = \alpha(\alpha^3) = \alpha(\alpha + 1) = \alpha^2 + \alpha, \alpha^5 = \alpha^2(\alpha^3) = \alpha^2(\alpha + 1) = \alpha^3 + \alpha^2 = (\alpha + 1) + \alpha^2 = \alpha^2 + \alpha + 1$. Likewise,

$$\alpha^6 = \alpha^3(\alpha^3) = \alpha^3(\alpha + 1) = \alpha^4 + \alpha^3 = (\alpha^2 + \alpha) + (\alpha + 1) = \alpha^2 + 1,$$

$$\alpha^7 = \alpha^4(\alpha^3) = \alpha^4(\alpha + 1) = \alpha^5 + \alpha^4 = (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) = 1.$$

It means that the extension field formed is $F = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1\}$ which contains $\mathbb{Z}_2$. In this case, $p(x) = x^3 + x + 1$ is said to be a primitive polynomial. The sum of the elements in the extension field, namely F, can be stated in Table 4, while the multiplication of the elements in F can be stated in Table 5. In addition, $F^* = F - \{0\} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ can be viewed as a group under the multiplication operation. Furthermore, group F^* is a cyclic group with order 7. As a result, every element that is not an identity element, namely $\alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1$ and α^2+1, is a generator element of group F^*.

Table 4. Addition Operation in Extension Field $GF(2^3)$.

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$		1	0

Table 5. The Multiplication Operation in the Extension Field $GF(2^3)$.

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Based on Table 5 it can be determined the inverse of each element in the finite field F. The inverse of element 1 is 1 itself, the inverse of α is α^2+1, the inverse of $\alpha+1$ is $\alpha^2+\alpha$, the inverse of α^2 is $\alpha^2+\alpha+1$, the inverse of α^2+1 is α, the inverse of $\alpha^2+\alpha$ is $\alpha+1$ and the inverse of $\alpha^2+\alpha+1$ is α^2. Galois Field F is isomorphic with Galois Field $GF(2^3)=\{0,1,2,3,4,5,6,7\}$ and can be expressed in Binary System $\{000,001,010,011,100,101,110,111\}$. The relationship among $\mathbb{Z}_2$, $GF(2^2)=GF(4)$, $GF(2^3)=GF(8)$ and $GF(2^4)=GF(16)$ is presented in Figure 2. In this case, $GF(2)=\{0,1\}\subseteq GF(2^2)=\{0,1,\alpha,\alpha+1\}\subseteq GF(2^3)=\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$

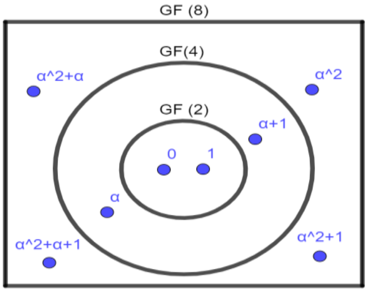

Figure 2. Relationship between Z₂, $GF(2^2)$, and $GF(2^3)$.

Example 6. The polynomial of degree 3 over $\mathbb{Z}_2$, namely $p(x)=x^3+x^2+1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots in $\mathbb{Z}_2=GF(2)$. Results analogous to Example 3 can be obtained. Likewise, the results are presented in Table 6. Based on Table 6, the inverse of each element can be determined. Element 1 has inverse 1, element α has inverse $\alpha^2+\alpha$, element α^2 has inverse $\alpha+1$, element α^2+1 has inverse $\alpha^2+\alpha+1$, element $\alpha^2+\alpha+1$ has inverse α^2+1, element $\alpha+1$ has inverse α^2 and element $\alpha^2+\alpha$ has inverse α. This Galois Field is isomorphic to the Galois Field $GF(2^3)=\{0,1,2,3,4,5,6,7\}$ and can be expressed in the binary system $\{000,001,010,011,100,101,110,111\}$. As a result, the Galois Field formed in Example 5 and Example 6 are mutually isomorphic.

Table 6. Power Form, Polynomials, Vectors, and Regulars in $GF(2^4)$.

Power Form	Polynomial Form	Binary Vector	Regular
0	0	000	0
α^0	1	001	1
α^1	α	010	2
α^2	α^2	100	4
α^3	α^2+1	101	5
α^4	$\alpha^2+\alpha+1$	111	7
α^5	$\alpha+1$	011	3
α^6	$\alpha^2+\alpha$	110	6

Example 7. The polynomial of degree 4 over $\mathbb{Z}_2$, namely $p(x) = x^4 + x + 1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots in $\mathbb{Z}_2 = GF(2)$. Next, choose α in the extension field F of $\mathbb{Z}_2$ so that $p(\alpha) = \alpha^4 + \alpha + 1 = 0$ or $\alpha^4 = \alpha + 1$. Furthermore,

$$\begin{aligned}
\alpha^5 &= \alpha(\alpha^4) = \alpha(\alpha + 1) = \alpha^2 + \alpha,\\
\alpha^6 &= \alpha^2(\alpha^4) = \alpha^2(\alpha + 1) = \alpha^3 + \alpha^2.\\
\alpha^7 &= \alpha^3(\alpha^4) = \alpha^3(\alpha + 1) = \alpha^4 + \alpha^3 = (\alpha + 1) + \alpha^3 = \alpha^3 + \alpha + 1,\\
&\vdots\\
\alpha^{15} &= \alpha^{11}(\alpha^4) = \alpha^{11}(\alpha + 1) = \alpha^{12} + \alpha^{11}\\
&= (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) = 1.
\end{aligned}$$

That means, the field that is formed is $F = \{\, a + b\alpha + c\alpha^2 + d\alpha^3 | a, b, c \text{ and } d \in \mathbb{Z}_2\}$ which contains the field $\mathbb{Z}_2$ and has $2^4 = 16$ elements. In this case, $p(x) = x^4 + x + 1$ is said to be a primitive polynomial. On the other hand, $F^* = F - \{0\}$ can be considered a group under the multiplication operation. The F^* group is a cyclic group with order 15, which is not a prime number, so we can look for elements from F^* that are generator elements and elements that are not builders of F^*. Elements that are generated are $\alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}$ and α^{14} while $\alpha^3, \alpha^5, \alpha^9, \alpha^{10}, \alpha^{12}$ are not generator elements. It means that α^k is a generator if $\gcd(k, 15) = \gcd(k, 2^4 - 1) = 1$ otherwise, it is not a generator. **Table 7** shows how the α elements are the generators of F^*. Based on **Table 7** and the fact that $\alpha^{15} = 1$, it is easy to determine the inverse of each element in a finite field F. For example, the inverse of α is α^{14} $(or\ \alpha^3 + 1)$. Galois Field (2^3) is isomorphic with Galois Field $GF(2^4) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ and can be expressed in the binary system $\{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$. $GF(2^4)$ is isomorphic to the GF formed by the irreducible polynomial $p(x) = x^4 + x^3 + 1$. The relationship among $\mathbb{Z}_2$, $GF(2^2) = GF(4)$, $GF(2^3) = GF(8)$ and $GF(2^4) = GF(16)$ is presented in **Figure 3**. In this case, $GF(2) = Z_2 = \{0, 1\} \subseteq GF(2^2) = \{\, 0, 1, \alpha, \alpha + 1\,\} \subseteq GF(2^3) = \{\, 0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\,\} \subseteq GF(2^4) = \{\, 0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\,\}$.

Table 7. **Power Form, Polynomials, Vectors, and Regulars in $GF(2^4)$.**

Power Form	Polynomial Form	Binary Vector	Regular
0	0	0000	0
α^0	1	0001	1
α^1	α	0010	2
α^2	α^2	0100	4
α^3	α^3	1000	8
α^4	$\alpha + 1$	0011	3
α^5	$\alpha^2 + \alpha$	0110	6
α^6	$\alpha^3 + \alpha^2$	1100	12
α^7	$\alpha^3 + \alpha + 1$	1011	11
α^8	$\alpha^2 + 1$	0101	5
α^9	$\alpha^3 + \alpha$	1010	10
α^{10}	$\alpha^2 + \alpha + 1$	0111	7
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110	14
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	15
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101	13
α^{14}	$\alpha^3 + 1$	1001	9

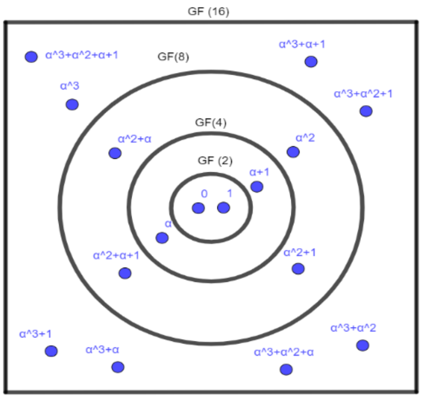

Figure 3. Relationships among $\mathbb{Z}_2$, $GF(2^2)$, $GF(2^3)$, and $GF(2^4)$.

Example 8. The polynomial of degree 4 over $\mathbb{Z}_2$, namely $p(x) = x^4 + x^3 + x^2 + x + 1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots in $\mathbb{Z}_2 = GF(2)$. It is chosen α in the extension field F of $\mathbb{Z}_2$ so that $p(\alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$ or $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$. Furthermore, $\alpha^5 = \alpha(\alpha^4) = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = 1$. It means that α is not a generator of the group $F^* = F - \{0\}$. However,

$$\begin{aligned}
(\alpha + 1)^1 &= \alpha + 1,\\
(\alpha + 1)^2 &= \alpha^2 + 1,\\
(\alpha + 1)^3 &= (\alpha + 1)^2\,(\alpha + 1) = (\alpha^2 + 1)(\alpha + 1)\\
&= \alpha^3 + \alpha + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,\\
&\vdots\\
(\alpha + 1)^{15} &= (\alpha + 1)^{14}\,(\alpha + 1) = (\alpha^3 + \alpha)(\alpha + 1)\\
&= \alpha^4 + \alpha^2 + \alpha^3 + \alpha\\
&= \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha^3 + \alpha = 1.
\end{aligned}$$

Consequently, $F^* = F - \{0\}$ can be considered as a group under multiplication and is constructed by $\alpha + 1$ and has members $\alpha + 1$, $(\alpha + 1)^2$ (or $\alpha^2 + 1$), $(\alpha + 1)^3$ (or $\alpha^3 + \alpha^2 + \alpha + 1$), $(\alpha + 1)^4$ (or $\alpha^3 + \alpha^2 + \alpha$), $(\alpha + 1)^5$ (or $\alpha^3 + \alpha^2 + 1$), $(\alpha + 1)^6$ (or α^3), $(\alpha + 1)^7$ (or $\alpha^2 + \alpha + 1$), $(\alpha + 1)^8$ (or $\alpha^3 + 1$), $(\alpha + 1)^9$ (or α^2), $(\alpha + 1)^{10}$ (or $\alpha^3 + \alpha^2$), $(\alpha + 1)^{11}$ (or $\alpha^3 + \alpha + 1$), $(\alpha + 1)^{12}$ (or α), $(\alpha + 1)^{13}$ (or $\alpha^2 + \alpha$), $(\alpha + 1)^{14}$ (or $\alpha^3 + \alpha$) dan $(\alpha + 1)^{15}$ (or 1).

Table 8. Power Form, Polynomials, Vectors, and Regulars in $GF(2^4)$.

Power Form	Polynomial Form	Binary Vector	Regular
0	0	0000	0
$(\alpha + 1)^0$	1	0001	1
$(\alpha + 1)^1$	$\alpha + 1$	0011	3
$(\alpha + 1)^2$	$\alpha^2 + 1$	0101	5
$(\alpha + 1)^3$	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	15
$(\alpha + 1)^4$	$\alpha^3 + \alpha^2 + \alpha$	1110	14
$(\alpha + 1)^5$	$\alpha^3 + \alpha^2 + 1$	1101	13
$(\alpha + 1)^6$	α^3	1000	8
$(\alpha + 1)^7$	$\alpha^2 + \alpha + 1$	0111	7
$(\alpha + 1)^8$	$\alpha^3 + 1$	1001	9
$(\alpha + 1)^9$	α^2	0100	4
$(\alpha + 1)^{10}$	$\alpha^3 + \alpha^2$	1100	12
$(\alpha + 1)^{11}$	$\alpha^3 + \alpha + 1$	1011	11
$(\alpha + 1)^{12}$	α	0010	2
$(\alpha + 1)^{13}$	$\alpha^2 + \alpha,$	0110	6
$(\alpha + 1)^{14}$	$\alpha^3 + \alpha$	1010	10

The extension fields that are formed are

$$F = \{\, a + b\alpha + c\alpha^2 + d\alpha^3 | a, b, c \text{ and } d \in \mathbb{Z}_2\}$$

which contains the field $\mathbb{Z}_2$ and has $2^4 = 16$ elements. In this case, $p(x) = x^4 + x^3 + x^2 + x + 1$ is said to be an irreducible polynomial but not a primitive polynomial. On the other hand, $F^* = F - \{0\}$ can be considered as a group under the multiplication operation. Furthermore, the F^* group is a cyclic group with order 15, which is not a prime number, so that elements from F^* which are generator elements and elements that are not generators of F^* can be found. The generator elements are $(\alpha+1), (\alpha+1)^2, (\alpha+1)^4, (\alpha+1)^7$, $(\alpha+1)^8, (\alpha+1)^{11}, (\alpha+1)^{13}$, and $(\alpha+1)^{14}$ whereas $(\alpha+1)^3$, $(\alpha+1)^5$, $(\alpha+1)^9$, $(\alpha+1)^{10}$, $(\alpha+1)^{12}$ are not generator elements. It means that $(\alpha+1)^k$ is a generator if $gcd(k,15) = gcd(k, 2^4 - 1) = 1$ otherwise it is not a generator. Based on Table 8 and the fact that $(\alpha + 1)^{15} = 1$, it is easy to determine the inverse of each element in a finite field F. For example, the inverse of $\alpha + 1$ is $(\alpha + 1)^{14}$ or $\alpha^3 + \alpha$ and the inverse of $(\alpha + 1)^2$ or $\alpha^2 + 1$ is $(\alpha + 1)^{13}$ or $\alpha^2 + \alpha$. $GF(2^4)$ is isomorphic to the GF that is formed by the irreducible polynomial $p(x) = x^4 + x^3 + 1$. On the other hand, it is also isomorphic with the GF formed by the irreducible polynomial $p(x) = x^4 + x + 1$.

Example 9. The polynomial of degree 5 over $\mathbb{Z}_2$, namely $p(x) = x^5 + x^3 + 1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots in $\mathbb{Z}_2 = GF(2)$. It is chosen α in the extension field F of $\mathbb{Z}_2$ so that $p(\alpha) = \alpha^5 + \alpha^2 + 1 = 0$ or $\alpha^5 = \alpha^2 + 1$. Furthermore,

$\alpha^6 = \alpha(\alpha^5) = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha$,
$\alpha^7 = \alpha^2(\alpha^5) = \alpha^2(\alpha^2 + 1) = \alpha^4 + \alpha^2$,
$\vdots$
$\alpha^{30} = \alpha^{29}(\alpha) = (\alpha^3 + 1)\ \alpha = \alpha^4 + \alpha$,
$\alpha^{31} = \alpha^{30}(\alpha) = (\alpha^4 + \alpha)\ \alpha = \alpha^5 + \alpha^2 = \alpha^2 + 1 + \alpha^2 = 1$.

In other words, the extension field that is formed is

$$F = \{\, a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 | a, b, c, d \text{ and } e \in \mathbb{Z}_2\}$$

which contains the field $\mathbb{Z}_2$ and has $2^5 = 32$ elements. In this case, $p(x) = x^5 + x^2 + 1$ is said to be a primitive polynomial. Table 9 fully states how the α element as a generator of F^*. Based on the fact that $\alpha^{31} = 1$, it is easy to determine the inverse of each element in a finite field F. For example, the inverse of α is α^{30} or $\alpha^4 + \alpha$, and the inverse of α^2 is α^{29} or $\alpha^3 + 1$.

This study only takes the example of $GF(2^5)$ which is constructed using a degree 5 primitive polynomial, namely $p(x) = x^5 + x^2 + 1$. In the same way, $GF(2^5)$ can be constructed using another primitive polynomial, namely $p(x) = x^5 + x^3 + 1$, $p(x) = x^5 + x^3 + x^2 + 1$, $p(x) = x^5 + x^4 + x^2 + 1$, $p(x) = x^5 + x^4 + x^3 + x + 1$, and $p(x) = x^5 + x^4 + x^3 + x^2 + 1$. Table 9 presents the power, the elements formed, the vector, and the score obtained from the vector. Furthermore, Figure 4 presents the relationship among $\mathbb{Z}_2$, $GF(2^2)$, $GF(2^3)$, $GF(2^4)$, and $GF(2^5)$.

Table 9. Power Form, Polynomials, Vectors, and Regulars in $GF(2^5)$.

Power Form	Polynomial Form	Binary Vector	Regular
0	0	00000	0
α^0	1	00001	1
α^1	α	00010	2
α^2	α^2	00100	4
α^3	α^3	01000	8
α^4	α^4	10000	16
α^5	$\alpha^2 + 1$	00101	5
α^6	$\alpha^3 + \alpha$	01010	10
α^7	$\alpha^4 + \alpha^2$	10100	20
α^8	$\alpha^3 + \alpha^2 + 1$	01101	13
α^9	$\alpha^4 + \alpha^3 + \alpha$	11010	26
α^{10}	$\alpha^4 + 1$	10001	17
α^{11}	$\alpha^2 + \alpha + 1$	00111	7
α^{12}	$\alpha^3 + \alpha^2 + \alpha,$	01110	14
α^{13}	$\alpha^4 + \alpha^3 + \alpha^2$	11100	28
α^{14}	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	11101	29
α^{15}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	11111	31
α^{16}	$\alpha^4 + \alpha^3 + \alpha + 1$	11011	27
α^{17}	$\alpha^4 + \alpha + 1$	10011	19
α^{18}	$\alpha + 1$	00011	3

Power Form	Polynomial Form	Binary Vector	Regular
α^{19}	$\alpha^2 + \alpha$	00110	6
α^{20}	$\alpha^3 + \alpha^2$	01100	12
α^{21}	$\alpha^4 + \alpha^3$	11000	24
α^{22}	$\alpha^4 + \alpha^2 + 1$	10101	21
α^{23}	$\alpha^3 + \alpha^2 + \alpha + 1$	01111	15
α^{24}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$	11110	30
α^{25}	$\alpha^4 + \alpha^3 + 1$	11001	25
α^{26}	$\alpha^4 + \alpha^2 + \alpha + 1$	10111	23
α^{27}	$\alpha^3 + \alpha + 1$	01011	11
α^{28}	$\alpha^4 + \alpha^2 + \alpha$	10110	22
α^{29}	$\alpha^3 + 1$	01001	9
α^{30}	$\alpha^4 + \alpha$	10010	18

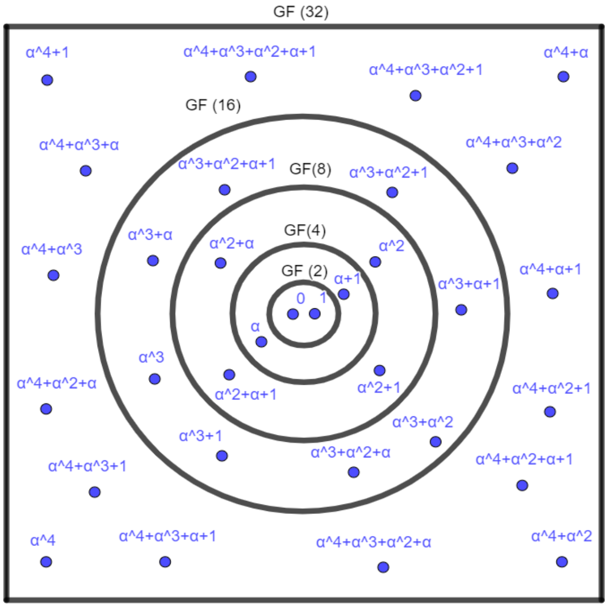

Figure 4. Relationships among Z₂, $GF(2^2) = GF(4)$, $GF(2^3) = GF(8)$, $GF(2^4) = GF(16)$and $GF(2^5) = GF(32)$.

Example 10. The polynomial of degree 6 over $\mathbb{Z}_2$, namely $p(x) = x^6 + x^3 + 1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots in $\mathbb{Z}_2 = GF(2)$. Next, select in the extension field F of Z₂ such that $p(\alpha) = \alpha^6 + \alpha^3 + 1 = 0$ or $\alpha^6 = \alpha^3 + 1$. Furthermore,
$\alpha^7 = \alpha(\alpha^6) = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha,$
$\alpha^8 = \alpha^2(\alpha^6) = \alpha^2(\alpha^3 + 1) = \alpha^5 + \alpha^2,$
$\alpha^9 = \alpha^3(\alpha^5) = \alpha^3(\alpha^3 + 1) = \alpha^6 + \alpha^3 = (\alpha^3 + 1) + \alpha^3 = 1,$
$\vdots$
$\alpha^{18} = \alpha^{27} = \alpha^{36} = \alpha^{45} = \alpha^{54} = \alpha^{63} = \alpha^{72} = 1.$
In other words, the extension field that is formed is

$$F = \{a + b\,\alpha + c\,\alpha^2 + d\,\alpha^3 + e\,\alpha^4 + f\,\alpha^5 \mid a, b, c, d, e \text{ and } f \text{ in } GF(2)\}$$

which contains field $GF(2) = Z_2$ and has 2^6 = 64 elements. However, because it undergoes summarization, field F only has 10 elements so it becomes

$$F = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^3 + 1, \alpha^4 + \alpha, \alpha^5 + \alpha^2\}.$$

In this case, $p(x) = x^6 + x^3 + 1$ is not a primitive polynomial because $\alpha^9 = 1$. Table 10 presents how the elements α^n where $n = 0, 1, 2, 3, 4, 5, 6, 7, 8$ and 9 such that $\alpha^0 = \alpha^9 = 1$. Consequently, the inverse of α is $\alpha^8 = \alpha^5 + \alpha^2$, the inverse of α^2 is $\alpha^7 = \alpha^4 + \alpha$, the inverse of α^3 is $\alpha^6 = \alpha^3 + 1$ and the inverse of α^4 is α^5. Conversely, the inverse of α^5 is α^4, the inverse of $\alpha^6 = \alpha^3 + 1$ is α^3, the inverse of $\alpha^7 = \alpha^4 + \alpha$ is α^2 and finally the inverse of $\alpha^8 = \alpha^5 + \alpha^2$ is α.

Table 10. Power Form, Polynomials, Vectors, and Regulars in $GF(2^6)$.

Power Form	Polynomial Form	Binary Vector	Regular
0	0	000000	0
α^0	1	000001	1
α^1	α	000010	2
α^2	α^2	000100	4
α^3	α^3	001000	8
α^4	α^4	010000	16
α^5	α^5	100000	32
α^6	$\alpha^3 + 1$	001001	9
α^7	$\alpha^4 + \alpha$	010010	18
α^8	$\alpha^5 + \alpha^2$	100100	36
α^9	1	000001	1

Example 11. The polynomial of degree 6 over $\mathbb{Z}_2$, namely $p(x) = x^6 + x^5 + 1$ is an irreducible polynomial over $\mathbb{Z}_2$ such that it has no internal roots $\mathbb{Z}_2 = GF(2)$. Next, choose α in the extension field F of Z_2 so that $p(\alpha) = \alpha^6 + \alpha^5 + 1 = 0$ or $\alpha^6 = \alpha^5 + 1$. Next,

$$\alpha^7 = \alpha(\alpha^6) = \alpha(\alpha^5 + 1) = \alpha^6 + \alpha = \alpha^5 + 1 + \alpha = \alpha^5 + \alpha + 1,$$
$$\alpha^8 = \alpha(\alpha^7) = \alpha(\alpha^6 + \alpha) = \alpha^7 + \alpha^2 = \alpha^5 + \alpha + 1 + \alpha^2 = \alpha^5 + \alpha^2 + \alpha + 1.$$

Furthermore,

$$\alpha^{61} = \alpha^{60}(\alpha) = (\alpha^3 + \alpha^2)\alpha = \alpha^4 + \alpha^3,$$
$$\alpha^{62} = \alpha^{61}(\alpha) = (\alpha^4 + \alpha^3)\alpha = \alpha^5 + \alpha^4,$$
$$\alpha^{63} = \alpha^{62}(\alpha) = (\alpha^5 + \alpha^4)\alpha = \alpha^6 + \alpha^5 = \alpha^5 + 1 + \alpha^5 = 1.$$

In other words, the extension field that is formed is

$$F = \{a + b\,\alpha + c\,\alpha^2 + d\,\alpha^3 + e\,\alpha^4 + f\,\alpha^5 \mid a, b, c, d, e \,\&\, f \ in\ Z_2\}$$

which contains field Z_2 and has $2^6 = 64$ elements. In this case, $p(x) = x^6 + x^5 + 1$ is said to be a primitive polynomial. Table 11 fully presents how the α element is the generator of F^*. Based on the fact that $\alpha^{63} = 1$, it is easy to determine the inverse of each element in a finite field F. For example, the inverse of α is α^{62} or $\alpha^5 + \alpha^4$, and the inverse of α^2 is α^{61} or $\alpha^4 + \alpha^3$. In this case, only the example of $GF(2^6)$ is taken, which is constructed using a primitive polynomial of degree 6, namely $p(x) = x^6 + x^5 + 1$. Table 11 presents the power, elements formed, vectors, and the scores obtained from these vectors. Further information about irreducible polynomials and how to construct expansion fields based on irreducible polynomials can be seen in papers [12], [13], [14].

Table 11. Power Form, Polynomials, Vectors, and Regulars of $GF(2^6)$.

Power	Polynomial	Vector	Regular
0	0	000000	0
α^0	1	000001	1
α^1	α	000010	2
α^2	α^2	000100	4
α^3	α^3	001000	8
α^4	α^4	010000	16
α^5	α^5	100000	32
α^6	$\alpha^5 + 1$	100001	33
α^7	$\alpha^5 + \alpha + 1$	100011	35
α^8	$\alpha^5 + \alpha^2 + \alpha + 1$	100111	39
α^9	$\alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	101111	47
⋮	⋮	⋮	⋮
α^{31}	$\alpha^3 + \alpha^2 + 1$	001101	13
α^{32}	$\alpha^4 + \alpha^3 + \alpha$	011010	26
⋮	⋮	⋮	⋮
α^{59}	$\alpha^2 + \alpha$	000110	6
α^{60}	$\alpha^3 + \alpha^2$	001100	12
α^{61}	$\alpha^4 + \alpha^3$	011000	24
α^{62}	$\alpha^5 + \alpha^4$	110000	48
α^{63}	1	000001	1

In this research, the following steps were used:
1. It is explained how to construct an S-box in developing the AES algorithm on $GF(2^2)$.
2. Next, explain how to construct an S-box in developing the AES algorithm on $GF(2^4)$.
3. Furthermore, it is explained how to construct an S-box in developing the AES algorithm on $GF(2^6)$.

3. RESULTS AND DISCUSSION

In this article, it is explained how to construct an S-box in developing the AES algorithm on $GF(2^2)$, $GF(2^4)$, and $GF(2^6)$.

3.1 Galois Field $GF(2^2) = GF(2^1 \cdot 2^1) = GF(2(2))$

$GF(2^8)$ (which has $2^8 = 256$ elements) can be expressed as $GF(2^4(2^4))$ such that the S-box obtained is 16×16. Analogous to this, $GF(2^2)$ which has 2^2 *or* 4 elements. $GF(2^2) = GF(4) = GF(2(2))$ can be constructed from an irreducible polynomial of degree 2, namely

$$p(x) = x^2 + x + 1$$

Suppose we choose α such that $p(\alpha) = 0$ or $p(\alpha) = \alpha^2 + \alpha + 1 = 0$ or $\alpha^2 = \alpha + 1$. As a result, the elements in $GF(2^2) = GF(4)$ are 0, $\alpha^0 = 1, \alpha^1 = \alpha$ and $\alpha^2 = \alpha + 1$. This means that an S-box table can be created which is presented in **Table 12**.

Table 12. S-box Design in $GF(2^2) = GF(4)$.

$\cdot$	0	1
0	S_{00}	S_{01}
1	S_{10}	S_{11}

To determine S_{00}, S_{01}, S_{10} and S_{11} it can be done as follows:

1. Element 0 is mapped to itself so that $S_{00} = 0$.
2. Element 1 is mapped to itself so that $S_{01} = 1$.
3. In this case $\alpha^3 = \alpha(\alpha^2) = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$. As a result, $p(x)\,q(x) = 1$ where $p(x) = x$ and $q(x) = x + 1$ such that $p(x) = x$ corresponds to a 2-digit binary, namely 10 and $q(x) = x + 1$ related to a 2-digit binary, namely 11 which is equivalent to 3 so that $S_{10} = 3$.
4. Furthermore, $\alpha^3 = (\alpha^2)\alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$. Consequently, $p(x)\,q(x) = 1$ where $p(x) = x + 1$ and $q(x) = x$ so that $p(x) = x + 1$ corresponds to a 2-digit binary, namely 11 and $q(x) = x$ relates to 2-binary digit, namely 10 which is equivalent to 2 so that $S_{11} = 2$. Next, we obtain an S-box table which has 4 cells in **Table 13**.

Table 13. The S-box Result of $GF(2^2) = GF(4)$.

$\cdot$	**0**	**1**
0	$S_{00} = 0$	$S_{01} = 1$
1	$S_{10} = 3$	$S_{11} = 2$

Furthermore, suppose an affine matrix is chosen:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and the constant vector $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ so that $S_{00} = 0$ when expressed as a vector it becomes $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and the result is obtained as

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

That means $S_{00} = 1$. In the same way, $S_{01} = 1$ when expressed in vector becomes $\begin{bmatrix}0\\1\end{bmatrix}$ and the result is obtained

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

i.e., $S_{01} = 3$. Furthermore, $S_{10} = 3$ when expressed as a vector becomes $\begin{bmatrix}1\\1\end{bmatrix}$ and the result is obtained

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

i.e., $S_{10} = 2$. Furthermore, $S_{11} = 2$ when expressed as a vector becomes $\begin{bmatrix}1\\0\end{bmatrix}$ and the result is obtained

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

i.e., $S_{11} = 0$. As a result, an S-box table of transformation results is obtained as stated in Table 14.

Table 14. The S-box results of $GF(2^2) = GF(4)$ after transformation.

·	0	1
0	$S_{00} = 1$	$S_{01} = 3$
1	$S_{10} = 2$	$S_{11} = 0$

3.2 Galois Field $GF(2^4) = GF(2^2 \cdot 2^2) = GF(4\ (4))$.

Analogous to the S-box construction in the case of $GF(2^8)$, $GF(2^4)$ which has 2^4 or 16 elements and $GF(2^6) = GF(2^3(2^3))$ which has $2^6 = 64$ elements. $GF(2^4)$ can be constructed from an irreducible polynomial of degree 4, i.e. $p(x) = x^4 + x^3 + 1$.

In this case, $p(0) = p(1) = 1$. Suppose α is chosen so that $p(\alpha) = 0$ or $\alpha^4 + \alpha^3 + 1 = 0$ or $\alpha^4 = \alpha^3 + 1$. As a result the elements in $GF(2^4)$ are 0, $\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2, \alpha^3, \alpha^4 = \alpha^3 + 1$,

$$\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + 1 + \alpha = \alpha^3 + \alpha + 1,$$
$$\alpha^6 = \alpha\alpha^5 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + 1 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\vdots$$
$$\alpha^{15} = \alpha\alpha^{14} = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha^3 + 1 + \alpha^3 = 1.$$

Furthermore, an S-box table can be formed which is stated in Table 15.

Table 15. S-box of $GF(2^4) = GF(16)$.

·	0 (00)	1 (01)	2 (10)	3 (11)
0 (00)	S_{00}	S_{01}	S_{02}	S_{03}
1 (01)	S_{10}	S_{11}	S_{12}	S_{13}
2 (10)	S_{20}	S_{21}	S_{22}	S_{23}
3 (11)	S_{30}	S_{31}	S_{32}	S_{33}

To determine $S_{00}, S_{01}, \ldots, S_{33}$ can be done as follows:

1. Element 0 is mapped to itself such that $S_{00} = 0$.

2. Element 1 is also mapped to itself such that $S_{01} = 1$.

3. $\alpha^{15} = 1 = \alpha^{14}(\alpha) = (\alpha^3 + \alpha^2)\alpha$ so that the result is $p(x)\,q(x) = 1$ with $p(x) = x^3 + x^2$ and $q(x) = x$. Furthermore, $p(x)$ corresponds to the 4-digit binary 1100 (i.e., equivalent to 30) and $q(x)$ corresponds to the 4-digit binary 0010 (i.e. equivalent to 2) such that $S_{30} = 2$.

4. $\alpha^{15} = 1 = \alpha^{13}(\alpha^2) = (\alpha^2 + \alpha)\alpha^2$ so that the result is $p(x)\,q(x) = 1$ with $p(x) = x^2 + x$ and $q(x) = x^2$. Furthermore, $p(x)$ corresponds to the 4 digits binary 0110 (i.e., equivalent to 12) and $q(x)$ corresponds to the 4-digit binary 0100 (i.e. equivalent to 2) so that $S_{12} = 4$.

5. Furthermore, $\alpha^{15} = 1 = \alpha^3(\alpha^{12}) = \alpha^3(\alpha + 1)$ such that the result is $p(x)q(x) = 1$ where $p(x) = x^3$ and $q(x) = x + 1$. Furthermore, $p(x)$ corresponds to the 4-digit binary 1000 (i.e. equivalent to 20) and $q(x)$ corresponds to the 4-digit binary 0010 (i.e. equivalent to 3) so that $S_{20} = 3$.

6. $\alpha^{15} = 1 = \alpha^2 (\alpha^{13}) = \alpha^2 (\alpha^2 + \alpha)$ such that the result is $p(x)\,q(x) = 1$ where $p(x) = x^2$ and $q(x) = x^2 + 1$. Next, $p(x)$ corresponds to the 4 digits binary 0100 (i.e., equivalent to 10) and $q(x)$ corresponds to the 4-digit binary 0110 (i.e. equivalent to 6) so $S_{10} = 6$.
7. $\alpha^{15} = 1 = \alpha(\alpha^{14}) = (\alpha^3 + \alpha^2)\alpha$ so that the result is $p(x)\,q(x) = 1$ where $p(x) = x$ and $q(x) = x^3 + x^2$. Furthermore, $p(x)$ corresponds to the 4-digit binary 0010 (i.e. equivalent to 02) and $q(x)$ corresponds to the 4-digit binary 1100 (i.e. equivalent to 12) so that $S_{02} = 12$.

In the same way, the S-box results are presented in **Table 16.**

Table 16. The S-box result of $GF(2^4) = GF(16)$.

.	0 (00)	1 (01)	2 (10)	3 (11)
0 (00)	$S_{00} = 0$	$S_{01} = 1$	$S_{02} = 12$	$S_{03} = 8$
1 (01)	$S_{10} = 6$	$S_{11} = 15$	$S_{12} = 4$	$S_{13} = 14$
2 (10)	$S_{20} = 3$	$S_{21} = 13$	$S_{22} = 11$	$S_{23} = 10$
3 (11)	$S_{30} = 2$	$S_{31} = 9$	$S_{32} = 7$	$S_{33} = 5$

Suppose a 4 × 4 affine matrix is chosen, i.e.

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and the vector constant, i.e.

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

so that $S_{12} = 4$ when expressed in vector form will become $S_{12} = 4$

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

and obtained

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

and in other words $S_{12} = 8$. The S-box result after being transformed becomes **Table 17**.

Table 17. The S-box results of $GF(2^4) = GF(16)$ after transformation.

.	0 (00)	1 (01)	2 (10)	3 (11)
0 (00)	$S_{00} = 10$	$S_{01} = 11$	$S_{02} = 12$	$S_{03} = 14$
1 (01)	$S_{10} = 0$	$S_{11} = 5$	$S_{12} = 8$	$S_{13} = 4$
2 (10)	$S_{20} = 3$	$S_{21} = 13$	$S_{22} = 7$	$S_{23} = 6$
3 (11)	$S_{30} = 2$	$S_{31} = 15$	$S_{32} = 1$	$S_{33} = 9$

3.3 Galois Field $GF(2^6) = GF(2^3 \cdot 2^3) = GF(8\,(8))$.

Suppose we take the irreducible polynomial $p(x) = x^6 + x^5 + 1$ so that $p(0) = p(1) = 1$. Choose α so that $p(\alpha) = 0$ or $\alpha^6 + \alpha^5 + 1 = 0$ or $\alpha^6 = \alpha^5 + 1$. In this case, the elements in $GF(2^6)$ are 0, $\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6 = \alpha^5 + 1, \alpha^7 = \alpha\alpha^6 = \alpha(\alpha^5 + 1) = \alpha^6 + \alpha = \alpha^5 + 1 + \alpha = \alpha^5 + \alpha + 1$.

Further, it is obtained

$\alpha^{62} = \alpha^{61}(\alpha) = (\alpha^4 + \alpha^3)\,\alpha = \alpha^5 + \alpha^4$,

$\alpha^{63} = \alpha^{62}(\alpha) = (\alpha^5 + \alpha^4)\,\alpha = \alpha^6 + \alpha^5 = \alpha^5 + 1 + \alpha^5 = 1$.

Next, an S-box table can be formed which can be expressed in **Table 18**. To determine $S_{00}, S_{01}, \dots, S_{77}$ can be done as follows:

1. Element 0 is mapped to itself such that $S_{00} = 0$.
2. Element 1 is also mapped to itself such that $S_{01} = 1$.
3. $\alpha^{63} = 1 = \alpha^{1}(\alpha^{62}) = \alpha(\alpha^{5} + \alpha^{4})$ so that the result is $p(x)\,q(x) = 1$ where $p(x) = x$ and $q(x) = x^5 + x^4$. Furthermore $p(x)$ corresponds to the 6 digit binary 000010 (i.e., equivalent to 02) and $q(x)$ corresponds to the 6 digit binary 110000 (i.e., equivalent to 48) so that $S_{02} = 48$.
4. $\alpha^{63} = 1 = \alpha^{2}(\alpha^{61}) = \alpha^{2}(\alpha^{4} + \alpha^{3})$ so that the result is $p(x)\,q(x) = 1$ where $p(x) = x^2$ and $q(x) = x^4 + x^3$. Furthermore, $p(x)$ corresponds to the 6 digit binary 000100 (i.e., equivalent to 04) and $q(x)$ corresponds to the 6 digit binary 011000 (i.e., equivalent to 24) so that $S_{02} = 24$.

Further, the following steps are obtained:

5. $\alpha^{63} = 1 = \alpha^{61}(\alpha^{2}) = (\alpha^{4} + \alpha^{3})\,\alpha^{2}$ so that the result is $p(x)\,q(x) = 1$ where $p(x) = x^4 + x^3$ and $q(x) = x^2$. Furthermore, $p(x)$ corresponds to the 6 digit binary 011000 (i.e. equivalent to 30) and $q(x)$ corresponds to the 6 digit binary 000100 (i.e. equivalent to 4) so that $S_{30} = 4$.
6. $\alpha^{63} = 1 = \alpha^{62}(\alpha) = (\alpha^{5} + \alpha^{4})\,\alpha$ so that the result is $p(x)\,q(x) = 1$ where $p(x) = x^5 + x^4$ and $q(x) = x$. Furthermore, $p(x)$ corresponds to the 6 digit binary 110000 (i.e. equivalent to 60) and $q(x)$ corresponds to the 6 digit binary 000010 (i.e. equivalent to 48) so that $S_{60} = 2$.

Next, a complete S-box is presented in **Table 19**.

Table 18. S-box of $GF(2^6) = GF(64)$.

.	0 (000)	1 (001)	2 (010)	3 (011)	4 (100)	5 (101)	6 (110)	7 (111)
0 (000)	S_{00}	S_{01}	S_{02}	S_{03}	S_{04}	S_{05}	S_{06}	S_{07}
1 (001)	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}	S_{17}
2 (010)	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{27}
3 (011)	S_{30}	S_{31}	S_{32}	S_{33}	S_{34}	S_{35}	S_{36}	S_{37}
4 (100)	S_{40}	S_{41}	S_{42}	S_{43}	S_{44}	S_{45}	S_{46}	S_{47}
5 (101)	S_{50}	S_{51}	S_{52}	S_{53}	S_{54}	S_{55}	S_{56}	S_{57}
6 (110)	S_{60}	S_{61}	S_{62}	S_{63}	S_{64}	S_{65}	S_{66}	S_{67}
7 (111)	S_{70}	S_{71}	S_{72}	S_{73}	S_{74}	S_{75}	S_{76}	S_{77}

Table 19. The S-box Result of $GF(2^6) = GF(64)$.

.	0 (000)	1 (001)	2 (010)	3 (011)	4 (100)	5 (101)	6 (110)	7 (111)
0 (000)	$S_{00} = 0$	$S_{01} = 1$	$S_{02} = 48$	$S_{03} = 32$	$S_{04} = 24$	$S_{05} = 63$	$S_{06} = 16$	$S_{07} = 46$
1 (001)	$S_{10} = 12$	$S_{11} = 27$	$S_{12} = 47$	$S_{13} = 37$	$S_{14} = 8$	$S_{15} = 26$	$S_{16} = 38$	$S_{17} = 43$
2 (010)	$S_{20} = 6$	$S_{21} = 44$	$S_{22} = 61$	$S_{23} = 28$	$S_{24} = 39$	$S_{25} = 15$	$S_{26} = 34$	$S_{27} = 41$
3 (011)	$S_{30} = 4$	$S_{31} = 62$	$S_{32} = 13$	$S_{33} = 9$	$S_{34} = 19$	$S_{35} = 60$	$S_{36} = 58$	$S_{37} = 42$
4 (100)	$S_{40} = 3$	$S_{41} = 49$	$S_{42} = 22$	$S_{43} = 40$	$S_{44} = 46$	$S_{45} = 21$	$S_{46} = 14$	$S_{47} = 20$
5 (101)	$S_{50} = 35$	$S_{51} = 23$	$S_{52} = 55$	$S_{53} = 53$	$S_{54} = 17$	$S_{55} = 7$	$S_{56} = 36$	$S_{57} = 10$
6 (110)	$S_{60} = 2$	$S_{61} = 33$	$S_{62} = 31$	$S_{63} = 59$	$S_{64} = 54$	$S_{65} = 43$	$S_{66} = 52$	$S_{67} = 42$
7 (111)	$S_{70} = 57$	$S_{71} = 56$	$S_{72} = 30$	$S_{73} = 51$	$S_{74} = 3$	$S_{75} = 18$	$S_{76} = 25$	$S_{77} = 5$

Furthermore, if an affine matrix is used

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

and constant matrix

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

such that $S_{01} = 1$ is transformed into

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

and the result is $S_{01} = 46$. In the same way, the S-box transformation results are obtained as presented in **Table 20**.

Table 20. The S-box Results of $GF(2^6) = GF(64)$ after Transformation.

.	0 (000)	1 (001)	2 (010)	3 (011)	4 (100)	5 (101)	6 (110)	7 (111)
0 (000)	$S_{00} = 45$	$S_{01} = 46$	$S_{02} = 41$	$S_{03} = 29$	$S_{04} = 9$	$S_{05} = 51$	$S_{06} = 21$	$S_{07} = 8$
1 (001)	$S_{10} = 63$	$S_{11} = 13$	$S_{12} = 11$	$S_{13} = 32$	$S_{14} = 49$	$S_{15} = 14$	$S_{16} = 20$	$S_{17} = 52$
2 (010)	$S_{20} = 36$	$S_{21} = 15$	$S_{22} = 63$	$S_{23} = 13$	$S_{24} = 23$	$S_{25} = 59$	$S_{26} = 26$	$S_{27} = 2$
3 (011)	$S_{30} = 35$	$S_{31} = 48$	$S_{32} = 60$	$S_{33} = 50$	$S_{34} = 17$	$S_{35} = 55$	$S_{36} = 62$	$S_{37} = 6$
4 (100)	$S_{40} = 41$	$S_{41} = 38$	$S_{42} = 28$	$S_{43} = 1$	$S_{44} = 8$	$S_{45} = 53$	$S_{46} = 56$	$S_{47} = 27$
5 (101)	$S_{50} = 25$	$S_{51} = 31$	$S_{52} = 47$	$S_{53} = 40$	$S_{54} = 22$	$S_{55} = 39$	$S_{56} = 19$	$S_{57} = 54$
6 (110)	$S_{60} = 42$	$S_{61} = 30$	$S_{62} = 3$	$S_{63} = 61$	$S_{64} = 44$	$S_{65} = 5$	$S_{66} = 43$	$S_{67} = 6$
7 (111)	$S_{70} = 58$	$S_{71} = 48$	$S_{72} = 0$	$S_{73} = 33$	$S_{74} = 41$	$S_{75} = 18$	$S_{76} = 10$	$S_{77} = 32$

In paper [15] Galois Field $GF(2^m)$ for $m = 8$ is used but uses a different affine matrix than that used in the AES algorithm and uses the same S-box as in the AES algorithm. In this research, Galois Field $GF(2^m)$ for $m = 2, 4$ and 6 is used to construct the S-box. Furthermore, in paper [16] the Galois Field $GF(2^m)$ for $m = 8$ is also used but by replacing the irreducible polynomial used in the AES algorithm, namely from $X^8 + X^4 + X^3 + X + 1$ into $X^8 + X^6 + X^5 + X + 1$. In research [17], a modern method is used for the construction of an S-Box by using non-linear transformation but still uses Galois Field $GF(2^m)$ for $m = 8$. In addition, in the paper [18], finite field modification is used in constructing the S-box. In this case, a field with order $2^3 = 8$ is used. Furthermore, in paper [19] an adjacency matrix is used for affine matrix transformation, but in this paper the Galois Field $GF(2^m)$ for $m = 8$ is still used. In the research of [20] it has been conducted on how to measure the goodness of algorithms similar to AES, such as the Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), and Non-linearity (NL), but using the S-box based on another polynomial irreducible of degree 8 over $GF(2^8)$.

4. CONCLUSIONS

In this paper, we have explained how to construct the S-box based on $GF(2^2)$, $GF(2^4)$ and $GF(2^6)$. The AES algorithm uses an S-box based on $GF(2^8)$. Further research can be carried out by constructing an S-box on $GF(2^{10})$. Likewise, further research can be carried out by measuring the goodness of algorithms similar to AES, such as Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), and Non-linearity (NL), but using the S-box proposed above.

ACKNOWLEDGMENT

This research was supported by Satya Wacana Christian University through the internal research scheme in 2023 with Decree No. 039/RIK-RPM/8/2023. We are grateful for their contribution to this research. Additionally, we would like to express our appreciation to the anonymous reviewers for their valuable feedback that significantly enhanced the quality of our paper.

REFERENCES

[1] A. Aidoo and K. B. Gyam, "Construction of Irreducible Polynomials in Galois fields, GF(2m) Using Normal Bases," *Asian Res. J. Math.*, vol. 14, no. 3, pp. 1–15, Jul. 2019, doi: 10.9734/arjom/2019/v14i330131.

[2] A. Chandoul and A. M. Sibih, "Note on irreducible polynomials over finite field," *Eur. J. Pure Appl. Math.*, vol. 14, no. 1,

pp. 265–267, 2021, doi: 10.29020/NYBG.EJPAM.V14I1.3898.

[3] B. Nithya and V. Ramadoss, “Extension fields and Galois Theory,” *Int. J. Math. Trends Technol.*, vol. 65, no. 7, 2019, doi: 10.14445/22315373/ijmtt-v65i7p507.

[4] S. Dey and R. Ghosh, “Mathematical Method to Search for Monic Irreducible Polynomials with Decimal Equivalents of Polynomials over Galois Field GF(pq),” *Circ. Comput. Sci.*, vol. 2, no. 11, 2017, doi: 10.22632/ccs-2017-252-68.

[5] R. H. Prayitno, S. A. Sudiro, S. Madenda, and S. Harmanto, “HARDWARE IMPLEMENTATION OF GALOIS FIELD MULTIPLICATION FOR MIXCOLUMN AND INVERSEMIXCOLUMN PROCESS IN ENCRYPTION-DECRYPTION ALGORITHMS,” *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 14, 2022.

[6] A. Nakashima, R. Ueno, and N. Homma, “AES S-Box Hardware With Efficiency Improvement Based on Linear Mapping Optimization,” *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 69, no. 10, 2022, doi: 10.1109/TCSII.2022.3185632.

[7] H. H. Mahmoud and M. M. Hoobi, “Improved Rijndael by encryption S-Box Using NTRU Algorithm,” *Iraqi J. Sci.*, vol. 56, no. 4, pp. 2984–2995, 2015.

[8] N. Angraini and Y. Suryanto, “MODIFICATION ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM WITH PERFECT STRICT AVALANCHE CRITERION S-BOX,” *J. Tek. Inform.*, vol. 3, no. 4, 2022, doi: 10.20884/1.jutif.2022.3.4.352.

[9] K. Zhao, *Ring and Field Theory*. 2022. doi: 10.1142/12819.

[10] J. Stillwell, *Undergraduate Analysis (Undergraduate Texts in Mathematics)*. 1996.

[11] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*. 1994. doi: 10.1017/cbo9781139172769.

[12] D. Hachenberger and D. Jungnickel, *Topics in Galois Fields*, vol. 29. 2020. [Online]. Available: http://link.springer.com/10.1007/978-3-030-60806-4

[13] S. Chibeti, I. Kyapwanyama, H. M. Phiri, and J. Kalunga, “An Introduction to the Theory of Field Extensions,” *Adv. Pure Math.*, vol. 13, no. 02, pp. 103–132, 2023, doi: 10.4236/apm.2023.132006.

[14] L. Childs, *A Concrete Introduction to Higher Algebra*. 1996. [Online]. Available: http://www.amazon.com/Undergraduate-Analysis-Texts-Mathematics/dp/0387948414

[15] Alamsyah, B. Prasetyo, and Y. Muhammad, “S-box Construction on AES Algorithm using Affine Matrix Modification to Improve Image Encryption Security,” *Sci. J. Informatics*, vol. 10, no. 2, 2023, doi: 10.15294/sji.v10i2.42305.

[16] H. Susanto, Alamsyah, and A. T. Putra, “Security Improvement of the 256-BIT AES Algorithm With Dynamic S-Box Based on Static Parameter as the Key for S-Box Formation,” *J. Adv. Inf. Syst. Technol.*, vol. 4, no. 1, pp. 33–41, 2022, doi: 10.15294/jaist.v4i1.59976.

[17] W. E. Ahmed, “A Modern Method for Constructing the S-Box of Advanced Encryption Standard,” *Appl. Math.*, vol. 10, no. 04, pp. 234–244, 2019, doi: 10.4236/am.2019.104018.

[18] J. K. Kim, “On the Modification of Finite Field Based S-Box,” *East Asian Math. J.*, vol. 37, no. 1, pp. 1–7, 2021.

[19] N. Siddiqui *et al.*, “A Highly Nonlinear Substitution-Box (S-Box) Design Using Action of Modular Group on a Projective Line Over a Finite Field,” *PLoS One*, vol. 15, no. 11 November, pp. 1–16, 2020, doi: 10.1371/journal.pone.0241890.

[20] F. Tita, A. Setiawan, and B. Susanto, “Performance of S-Box Constructed by Irreducible Polynomials on GF(2),” *2024 IEEE Symp. Ind. Electron. Appl.*, 2024.