ISSN 2986-8041
Noumerico Journal of Technology in Mathematics Education
Volume 2 Issue 1, 2024
https://ejournal.uit-lirboyo.ac.id/index.php/noumerico
https://doi.org/10.33367/jtme.v2i1.5187

Analysis of Fundamental Algebraic Concepts and Information Security System

S M Nazmuz Sakib[*1, 2, 3, 4]
[1]Graduate of BSc in Business Studies School of Business and Trade Pilatusstrasse 6003, 6003 Luzern, Switzerland
[2]Graduate of LLB(Hon's) Faculty of Law Dhaka International University, Satarkul Rd, Dhaka 1212.
[3]Graduate of MBA (Human Resources), International MBA Institute, Samstagernstrasse 57, 8832 Wollerau Switzerland. Phone: +41 78 946 88 86.
[4]Student of LLM (Professional), Department of Law, Bangladesh University of Professionals, Mirpur, Dhaka.
[1]**sakibpedia@gmail.com**
*Correspondence

Article Information:
Received February 21, 2024
Revised March 30, 2024
Accepted March 30, 2024

Keyword:
Algebra, Cryptography, Information Security Systems, Fundamental Algebraic Concepts, Crypto-Algebra, Analysis of Algebra

Abstract

Cryptography plays a crucial role in protecting the data from unauthorized access. Nowadays, various cryptographic algorithms are used. It is not meant for information technology to secure the proposed work's primary target to achieve these tasks and goals. Using a literature review, we study security information systems using S-Boxes. In the research, we discuss two different techniques to generate the new S-boxes and then discuss their other properties to improve the strength of encryption. This chapter is further divided into sections that comprehensively explain the various concepts.

INTRODUCTION

1.1 Fundamental Algebraic concepts

This section is further divided into many subsections which explain the fundamental algebraic concepts, including group, ring, field, vector space, affine space, symmetric group, etc. Further, the Galois field, substitution boxes, and group action are also explained in detail, which is most important for our dissertation.

Binary operation

Definition 1: Let a set $M \neq \phi$ and 'g' be a mapping such that $g: M \times M \longrightarrow M$ then 'g' is called a binary operation if M is closed under the operation 'g.' In mathematical notation,

$g(p, q) = pgq \forall$, p ,$q \in M$

.

Example 1: "+" addition is a binary operation for the non-empty sets $\mathbb{Z}$**,** $\mathbb{R}$**,** $\mathbb{Q}$**,** and $\mathbb{C}$. These sets are closed under addition.

Remark 1: If we divide one integer by another integer, then the result would not necessarily be an integer, so the division is not a binary operation.

Algebraic Structure

Definition 2: A set $B \neq \phi$ is called an Algebraic structure if it has at least one binary operation.

Groupoid

Definition 3: If closed under that binary operation, a set $A \neq \phi$ with a binary operation is called groupoid.

Example 2: i. ($\mathbb{R}$, +) under addition set of real numbers
ii. ($\mathbb{Q}$, +) under addition set of rational numbers
iii. ($\mathbb{C}$, +) under an addition set of complex numbers

Semigroup

Definition 4: A groupoid $A \neq \phi$ is called a semigroup if it satisfies the associative property under the same binary operation. Mathematically,

$a*(b*c) = (a*b)*c \quad \forall\ a, b, c \in$ A

Example 3:$\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$ are semigroup under the binary operation multiplication and addition.

Remark 2: $\mathbb{Z}$ The set of integers is not semigroup under the binary operation division.

Monoid

Definition 5: A semigroup**(**S,*) is called a monoid if it has the identity under the same binary operation. Mathematically,

s*e = s =e*s $\quad \forall$ s $\in S$

Example 4: The set of rational, real, and complex integers are monoid under the binary operation "+" and "."

Remark 3: The set of natural number is not monoid under "+".

1.1.1 Group

Definition 6: If each element in the monoid (G,*) has the inverse, then the set is known as a group. It means for

Mathematically,

$s \varepsilon$ G $\ni\ s' \in$ G such that

$s*s' = s'*s$ = e $\quad \forall$ s $\in$ G where e is identity.

Example 5: $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ are groups under multiplication and additionwith identity 1 and 0 respectively.

Remark 4: In the set of integer$\mathbb{Z}$ each element is not invertible under the binary operation multiplication so$\mathbb{Z}$ is not a group.

Similarly under the binary operation "." and "+" respectively {1} and {0} are trivial group.

Remark 5: In a group, the identity and inverse of each element are always unique.

Subgroup

Definition 7: A subset$S \neq \phi$of group G with binary operation "*" is known as subgroup if S is also subgroup under the binary operation "*" which has the set G.

Example 6: The set of integer $\mathbb{Z}$ is a subgroup under the binary operation "+" $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$**.**

Remark 6: Every group G has two trivial subgroups {e} and **{**G} itself.

Abelian group

Definition 8: A group G is called an abelian group with binary operation "*" if "*" is commutative. Mathematically, $g_1 * g_2 = g_2 * g_1$, $\forall \quad g_1, g_2 \in$ G

Example 7: i. $\mathbb{Q}$, the rational numbers
ii. $\mathbb{R}$, the real numbers
iii. $\mathbb{C}$, the complex numbers
are the abelian group under multiplication

Remark 22: M_n**(**$\mathbb{R}$**)** Matrices having entries from the set of real numbers called the real matrices. It forms the non abelian group under the binary operation multiplication.

Cyclic group

Definition 9: If a group G is generated by a single element of G, then G is known as cyclic. If G is cyclic under addition, we represent it mathematically,

G = ‹g› = {ng: n ∈$\mathbb{Z}$}

And if G is a cyclic group under multiplication, then we write it as,

G = ‹g› ={g^n: n ∈$\mathbb{Z}$}

Example 8: let G be the set of nth root of unity, then G is called a cyclic group and denoted by

G = ‹w› = {1, w, w^2,…, w^{n-1}} where w^n=1

Remark 7: The order of the cyclic group and its generator are equal, and the subgroup's order and the element's order divide the order of the group.

Remark 8: The set of integer$\mathbb{Z}$ has two generators under addition 1 and -1.So $\mathbb{Z}$ is an infinite cyclic group under addition and the group of prime order is always cyclic.

1.1.2 Ring

Definition 10: A set R ≠ ϕ with two binary operations "+" and "." is known as a ring if it satisfies the following properties which are given below.

i- R is an abelian group under the operation "+"
ii- R is semigroup under the operation "."
iii- "+" is distributive over "."

Example 9: The set of integer $\mathbb{Z}$ is a ring under the binary operation which is mentioned above.

Example 10: The set of rational numbers $\mathbb{Q}$ is a ring under the binary operation which is mentioned above.

Example 11: The set of real numbers $\mathbb{R}$ is a ring under the binary operation, which is discussed above.

Example 12: The set of complex numbers $\mathbb{C}$ is a ring under the above mentioned binary operation.
Example 13: Similarly, $M_n(\mathbb{R})$, $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, and $M_n(\mathbb{C})$ are the example of rings.
Example 14: $\mathbb{Z}_n$and n$\mathbb{Z}$are also the example of a ring.
Commutative Ring
Definition 11: A ring R is said to be a commutative ring if "." is commutative.
Example 15: The set of integers forms a commutative ring.
Example 16: $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$ are examples of commutative rings.
Remark 9: $M_n(\mathbb{R})$, $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, and $M_n(\mathbb{C})$ are the examples of non–commutative ring.
Ring having identity
Definition 12: A ring R is known as a ring with identity if R contains the multiplicative identity.
Mathematically, a.1 =1.a = a, ∀ a∈ R
Example 17: ($\mathbb{Z}$, +, **.)**is a ring with identity.
Example 18: ($\mathbb{Q}$**, +, .)** is a ring with identity.
Example 19: ($\mathbb{R}$**, +, .)** is a ring with identity.
Example 20: ($\mathbb{C}$**, +, .)** is a ring with identity.
Remarks 10: n$\mathbb{Z}$ where n>1 is a ring without identity.
Subring
Definition 13: A subset S ≠ ϕ of a commutative ring Ris called a subring of Rif it fulfills the following conditions.

i- If $r, t\in$ S then $r - t \in$ S
ii- If $r, t\in$ S then $rt\in$ S
iii- 1 ∈ S

Example 21: $\mathbb{Z}$is a subring of $\mathbb{Q}$ **.**
Example 22: $\mathbb{Q}$is a subring of $\mathbb{R}$**.**
Example 23: $\mathbb{R}$ is a subring of $\mathbb{C}$**.**
Example 24: n$\mathbb{Z}$is a subring of $\mathbb{Z}$**.**

1.1.3 Field

Definition 14: A set F which is non emptyis known as a field if it satisfies the properties which are given below.

i- **(**F**,**+) is abelian group .
ii- F - {0} form a multiplicative group.
iii- Distributive law holds multiplication over addition, i.e
$p(q + r) = pq + pr$ ∀ $p, q, r\in F$

Example 25: $\mathbb{R}$ is a field.
Example 26: $\mathbb{Q}$ is a field.
Example 27: $\mathbb{C}$ is a field.
Remark 11: The set $\mathbb{Z}_n$ = **{**0, 1, 2, … , p −1**}** is a field where p is any prime number.

In cryptography, we always prefer to choose field having finite elements called finite field or Galois field. The total number of elements in the field is known as order of the field.

Finite field or Galois Field

Definition 15: A field in which the number of elements is finite, is called finite field or sometimes called Galois field in which we can subtract, add, multiply and invest. If this finite field has p elements then we write it as $GF(p)$.

Example 28: $\mathbb{Z}_5$ = {0, 1, 2, 3, 4} is a finite field having five elements.

Remark 12: A real field is an infinite field.

Theorem 1: A finite field having order m occurs if m is a power of a prime. i.e m =p^n for some positive integers n and prime number p and p is known as characteristic of the finite field. There does not exist finite field of order 24 since 24 = 2^3.3 so 24 is not the power of a prime.

Prime field

Definition 16: The prime order's fields are the most important and vital in the algebraic system. The field's elements $GF(p)$ can be shown by integers 0, 1, 2, 3, ... $p-1$.

Theorem 2: Let p be a prime number and the integers ring Z_p is represented by $GF(p)$. This is said to be a prime field or Galois field having a prime number of elements. Also the elements other than zero of the field have their inverses.

1.1.4 Vector Space

Definition 17: Let V be set which is non empty and F is a field then V is known as Vector Space if the below mentioned conditions are satisfied.

i- V is abelian group under addition.

ii- $1(m+n) = 1m + 1n \quad \forall\ 1 \in F$ and $m, n \in$

iii- $(s+t)m = sm + tm \quad \forall\ s, t \in F\ ,\ m \in V$

iv- $s(tm) = (st)m \quad \forall\ s, t \in F$, m $\in V$

v- 1.m = m.1 = m $\quad \forall$ 1 $\in$ F, m $\in$ V, 1 is identity under multiplication.

Example 29: The set M_n of all matrices of ordern is known as vector space over F.

Example 30: For a field the set F^n = $\{(x_1, x_2, x_3, \ldots, x_n)\}/x_i \varepsilon$ F, $1 \leq I \leq n\}$ is a vector space.

Subspace

Definition 18: The non empty subset W is called subspace of a vector space V if W is also a vector space under the same operation defined in V.

Theorem 3: A non empty subset $W \neq \phi$ of a vector space V is called subspace if and only if

i- $w_1, w_2 \in W$ then $w_1 + w_2 \in W$

ii- $If\ p \in F$ and $w \in$ W then $pw \in$ W

Remark 13: Vitself and {0} are subspaces of V, called the trivial or improper subspaces of V.

Example 31: $N = \begin{Bmatrix} 0 \\ x \\ y \end{Bmatrix}$ Where$x, y \in \mathbb{R}$**,** is a subspace of $\mathbb{R}^3$.

Linear Transformation

Definition 19: Let W and V over the same field $F$are two vector spaces then $s$from $W$to $V$is called linear transformation if it satisfies the properties which are mentioned below.

i- $s(u+v) = s(u) + s(v)$

ii- $s(pu) = ps(u)$where$p$ is a scalar.

Example 32: The transformation $s(x, y) = (2x, y - x)$ is linear transformation.

Affine Transformation

Definition 20: A set Ehaving vector space properties and mapping f such that

$$f: E \times E \longrightarrow E$$
$$f(A, B) = \overrightarrow{AB}$$

Remark 14: Chasless relation explain direction

$\overrightarrow{AA}$=0 and $\overrightarrow{AB} = -\overrightarrow{BA}$

Remark 15: Every vector space is affine space.

Permutation

Definition 21: Let Y = {1, 2, 3,…,n} and then $f: Y \longrightarrow Y$ be the collections of all bijective mappings are called permutation.

Symmetry

Definition 22: It is a transformation which acts upon the objects and leaves it apparently unchanged.

Symmetric Group

Definition 23: If X= {1, 2, 3, … n} then the collection of all permutation of this set X is known as the symmetric group and denoted by S_n

Remark 16: $S_n$contains the n!

Remark 17: $S_3$is the symmetry of equilateral triangle.

Group Action

Definition 24: Let G be a group and Y be a set along with rule which associates every element $p \in G$ and $y \in Y$to an element$py \in Y$ such that the following conditions are satisfied.

i- $1.y = y$ $\forall\ y \in$ Y

ii- $s, t \in G$ and y ∈ Y such that
$(st).y = s.(t.y)$

If such an association exists we say that G is acting on Y and this association is called group action.

Example 33: The group of permutation of n objects if $p \in G$and $y \in$ Y such that
p.y = p(y)

Example 34: Gis any group Y = G, define action such that g.y = gyg^{-1} then G is acting by conjugation onto itself.

Stabilizer

Definition 25: Let G be a group which is acting on the Ythen stabilizer of y ∈ Y is defined as

$G_y = \{ \ g \in G : \ g.y = y \ \}$

1.2 Fundamental cryptographic concepts

Now we shall discuss basic terms related to cryptography which are useful and important for understanding the main idea of cryptography and also very important for the proposed work in the coming chapter. Now we shall explain some basic definitions related to cryptography.

Plaintext

Definition 26: The original text or message through which one person wants to communicate with the other person is termed as plaintext. It may be a word file, numerical data, audio file or video file and denoted by M.

Example 35: "please give me a glass of water" is a word file which is a plaintext.

Ciphertext

Definition 27: The text or message which cannot understand by any one or meaningless is known as ciphertext. The original message is transformed into a message which cannot be readable in cryptography. It is denoted by C**.**

Plaintext Alphabets

Definition 28: The alphabets or characters are used in plaintext is known as plaintext alphabets. These may be numerical data, English alphabets or symbols etc.

Ciphertext Alphabets

Definition 29: The alphabets or characters which are used to convert the message from plaintext to ciphertext are known as ciphertext alphabets. These may be different from original alphabets.

Cipher

Definition 30: The process through which a readable message can be converted into unreadable text or meaningless form is known as cipher. It may be substitution or transformation and known as cipher substitution or cipher transformation.

Key

Definition 31: When the sender sends a text, he also sends some extra information so that receiver used this information or code to read the ciphertext which is known as the key. In other words, the key is some rules which are used during the encryption and decryption by sender and receiver. It is denoted by K.

Encryption

Definition 32: The process through which the plaintext is converted into ciphertext is known as encryption. In cryptography, there are used some encryption techniques to send the confidential message from an insecure system. For encryption there are two main requirements;

- An algorithm
- Key

A sender uses it to encrypt the plaintext.

Encryption Algorithm

Definition 33: The process or mathematical process through which we convert the plaintext into unreadable and meaningless form is called encryption algorithm. It is used by a sender to encrypt the plaintext into ciphertext.

Decryption

Definition 34: The process through which the unreadable and meaningless ciphertext convert into plaintext is said to be decryption. Decryption is the alter process of encryption. This process is used on the receiver side to decrypt the meaningless message to plaintext. The process of decryption has two requirements;

- Secure algorithm
- Key

Decryption Algorithm

Definition 35: The process or mathematical process that converts the unreadable or meaningless message into readable text (plaintext) is known as decryption algorithm. In other words, these are techniques which are used in decryption.

It will be cleared from the below image:

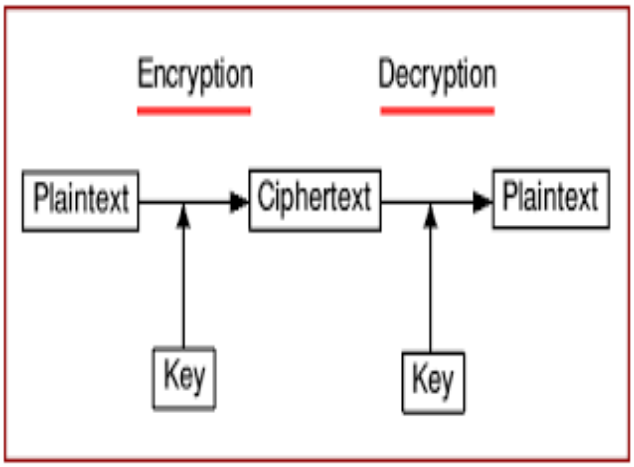


Figure 1. A complete cipher

1.2.1 Cryptology and its classification

Cryptology

Definition 36: Cryptology is the branch of science related to information security. This word is derived from the Greek word kryptos, means hidden so Cryptology is the study of secret message.

Classification of Cryptology

Cryptology is further divided into two main branches;

- Cryptography
- Cryptanalysis

Cryptography

Definition 37: It is the study of the method of transforming a secret message such a way that only the authorized person can understand it.

Cryptanalysis

Definition 38: It is the branch which deals to break the cryptosystem. It is referred to as "breaking the code".

1.2.2 Purpose of Cryptography

Cryptography plays a vital role to achieve the security goals to make sure the privacy of the secret data from the unauthorized channel. It has wide use in daily life now a day due to high security advantages.

The various goals of cryptography are given below.

Confidentiality

To make sure that the secret data in the computer is disseminated and can be accessed only the unapproved party or channel and not by the unauthorized party.

Authentication

The information or data which is accepted by any system or party to be checked whether the data received from an authorized party or a wrong party.

Integrity

Only the certified person or channel is allowed to change the given text or message, no one can alter the message between the sender and receiver.

Non Repudiation

It will ensure that neither the receiver nor the consigner (sender) of a message can deny the transmission.

Access Control

Only the authorized party can access the confidential data or secret information.

1.2.3 Classification of Cryptography

Cryptography is further divided into two main categories;

- Symmetric key cryptography
- Asymmetric key cryptography

Symmetric Key Cryptography

In such type of cryptography, encryption and decryption both have the same key, as shown in the following Fig.

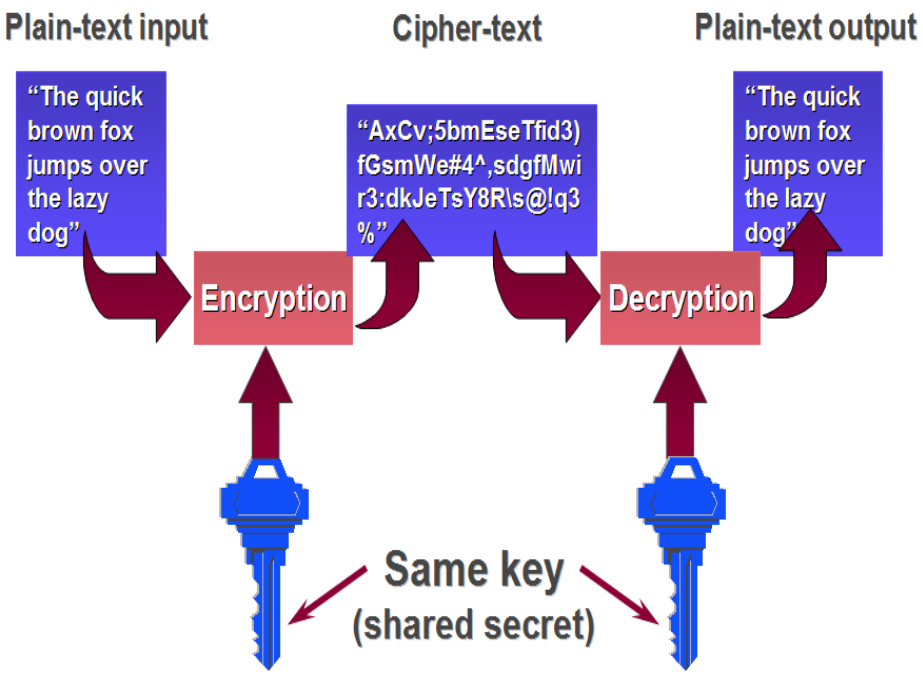


Figure 2. Symmetric Key Cryptography

In such a type of cryptography, the key plays a vital role in the data's security depending on the key's nature and length. There are various symmetric algorithms: DES, TRIPLE DES, and AES. It is further divided into two subclasses;

- Block Cipher
- Stream Cipher

Block Cipher

It is a symmetric key algorithm which is used for encryption. It is mapping which maps n bits of plaintext to n bits of cipher text where n is known as block length or key length. It is usually known as a simple substitution cipher with a large block size.

Stream Cipher

This cipher is also a symmetric key encryption system. It is an essential kind of encryption algorithm. It usually works on a smaller part of the information as compared to the block cipher, which works on a large block of information. It is normally faster than the block cipher in hardware and has less complex hardware circuitry. It may also be advantageous in such situations where transmission errors are primarily probable.

1.2.4 Asymmetric key cryptography

Asymmetric key cryptography or public key cryptography is cryptography which has a pair of keys which are used to decrypt and encrypt the data to make the algorithm more secure. In this type of cryptography, there are two disparate keys that are used to encrypt and decrypt the given data, as shown in Fig. 3

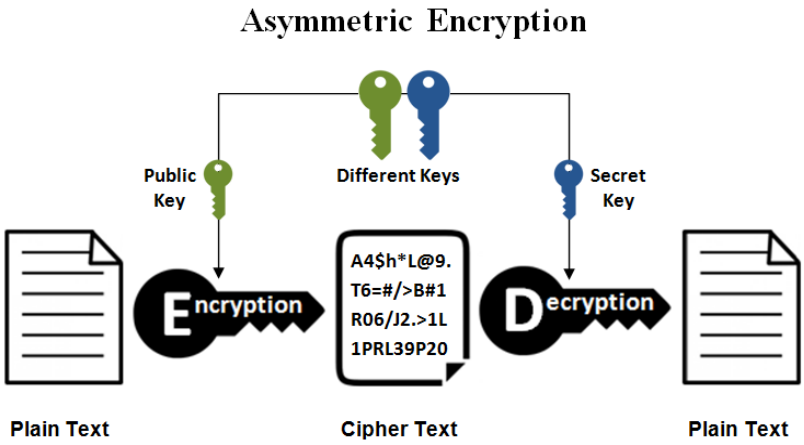


Figure 3. Asymmetric key cryptography

The symmetric key does not replace it. An example of such type cryptography is elliptic curve cryptography.

1.2.5 Theory of S-Box

In the following section, we will discuss the substitution boxes(s-boxes). The main task of S-box theory is to help in the research work to achieve the goals and dissertations.

Substitution Box (S-box)

In cryptography, an S-box is the important and basic component of the symmetric key process through which substitutions are made. Such block ciphers are used to develop the correspondence between the cipher text and key.

What is an S-box?

The S-Boxes are basically Boolean functions from $\{0,1\}^m \longrightarrow \{0,1\}^n$ m×n mappings. Thus, this can be explained as there are n components mapping, each being connected from m bits to 1 bit; in another sense, each component mapping is a Boolean mapping in m Boolean variable.

1.2.6 Balanced Function

A Boolean mapping is considered balanced if the number of zeros and ones are the same in the truth table in counting. The Hamming weight of this binary sequence is how many ones in number.

Properties of good S-box:

- Balanced Component mapping
- The non-linearity of the Component should be very high.
- The Non-zero linear combinations of Component mapping should be highly non-linear and balanced.
- The s-boxes should be highly algebraic degree.

1.2.7 Substitution –Permutation Network (SPN)

Product Cipher

Definition 94: Two or more transformation get together in a cipher to make new cipher which is analogously (comparatively) more secure than the separate ciphers is known as product cipher.

Definition 95: Permutation is the substitution of the sequence of the element of the text by the sequence of these elements which are permuted. There are no addition and subtraction of the elements. We just reshuffle the elements.

Substitution Network

Definition 96: The substitution network or SP network is the product of two or more ciphers. There are used a chain of functions related to mathematics are used in this algorithm. In these algorithms, there are used S-boxes and P boxes for substitution and permutation.

1.2.8 Block cipher and advanced encryption standard

Many cryptographic algorithms have been proposed, but AES is the latest and most secure crypto algorithm. This cryptographic algorithm used permutation operations to make information more secure. We now briefly describe the cryptosystem approved for general standards and technology (NIST). The Advance Encryption Standard (AES) was adopted and effective on May 26, 2002. The Advance Encryption Standard (AES) is also known as the Rijndael Algorithm. It was offered by two cryptographers from Belgium, Joan Daemen and Vincent Rijmen, who submitted this proposal to NIST while selecting AES. The AES was developed to replace two currently existing standards, DES (Data Encryption Standard) and Triple DES because these two standards were no longer secure cryptosystems. Therefore, it was necessary to phase out the DES and adopt a more secure encryption standard. For this algorithm, NIST selected three members of the Rijndael family, each with a block size of 128 bits but with different key lengths of 128, 192, and 256 bits. The key space size in AES is 2^{128}, or approximately 3.4×10^{38}. This number is so large that the fastest "Cracker Machine" available would take trillions of years to crack the AES code by doing an exhaustive key search.

Therefore, AES is expected to remain a secure cryptosystem for many years to come. The enciphering algorithm in AES was developed by two cryptographers, Dr. Joan Daeman and Dr. Vincent Rijmen from Belgium, and was given the name Rijndael. The basic structure of this algorithm is that of an iterated block cipher but with some additional steps. We now discuss briefly the Rijndael algorithm in AES. There are several versions of the Rijndael algorithm in AES; there is a difference in the block/key length and the rounds in numbers. The possible values for the key length are 256, 192, and 128 bits. Similarly, the number of rounds can be 8, 10 or 12. There are a few steps:

- Round key addition
- S-bit substitution
- Permutations
- Row shift operation

- Column mix

AES algorithm can be understood by the following diagram:

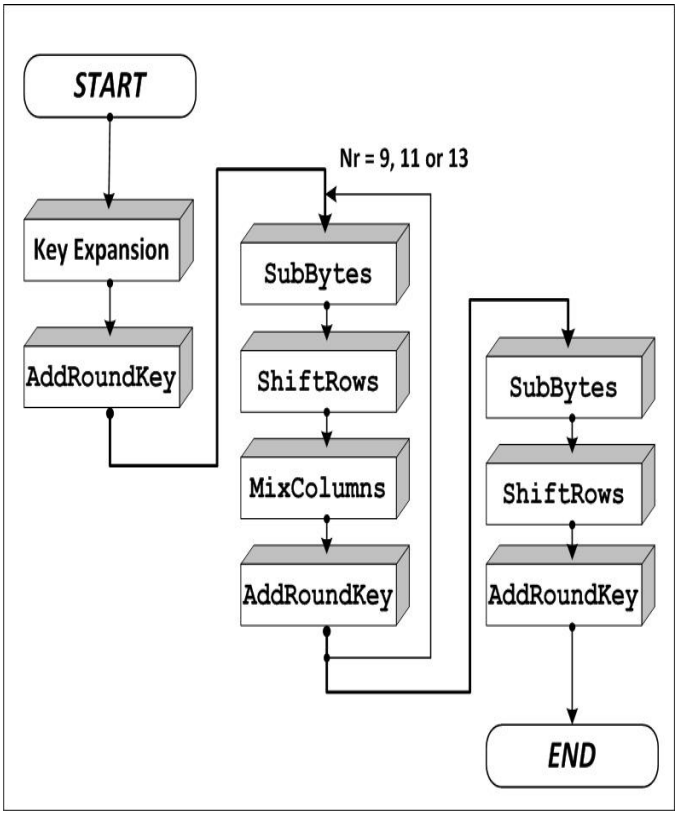


Figure 4. AES Algorithm

1.3 Some Historical Ciphers

Ciphers play a vital role in the field of cryptography. There are different ciphers which are used in cryptography depend on different algebraic structures like groups, rings and fields. Here we discuss some historical ciphers in detail with examples.

1.3.1 Process of Transforming a Message

Basically, there are two ways to transform the message in cryptography. One is called transposition and other is called substitution. Here we shall discuss those substitution methods especially those that employ algebraic techniques and make use of the algebraic system like fields and rings. The general principle involved in the substitution method is to select a permutation f of the set of letters in the alphabets and replace each letter x in the message by $f(x)$.

Suppose we want to send a message to a friend that

ALGEBRA IS GREAT FUN; Plaintext

Since we don't want that an unauthorized recipient can know this message, we decide to send the message in secret form. Let us take f to be the permutation given by table 2.1; for each letter x in the top of the row, $f(x)$ is the letter directly below x.

Table 1. Fixed Table for Cipher

A	B	C	D	E	F	G	H	I
N	F	P	R	K	S	C	E	L
J	K	L	M	N	O	P	Q	R
A	J	Q	G	T	B	I	M	D
S	T	U	V	W	X	Y	Z	
H	O	X	Z	V	Y	U	W	

Replacing each letter in the message by $f(x)$ without blank spaces we transform the original message to

NQCKFDNLHCDKNOSXT ; Cipher-text

We send this message to our friend who has been already provided the secret key in advance. Our friend can recover the message by replacing the letter y in the received message by $f^{-1}(y)$. But the unauthorized person who does not aware the secret key, he can't find out the original message. It looks that one can try all the possible permutations to find out the meaning full message and such a process to breaking the code is known as exhaustive key search. But the number of permutation in the set of 26 English alphabets is equal to

$26! = 403291461126605635584000000 \approx 4\times10^{26}$

This number is so large that it is very hard to find out all possible permutations. If our enemy can take one second for one permutation it will take 10^{19} years to go through all the permutations. So it is not an easy task to find the exhaustive key. It is clear from the above discussion that it is computationally infeasible to break the code by selecting all the permutation but still there are available such type of computers which find out the original message in the short interval of time from the ciphertext. It is required that build up such algebraic system like rings and fields to make the system more secure. Before discussing the algebraic methods in which simple algorithm is used which needs no abstract.

1.3.2 Caesar Cipher

This is a mono alphabetic cipher. It works by arranging the alphabet around a circle as shown in figure 2.2. If we shift each letter forward by k places in the circle we get the resulting permutations called the k length cycle shift and such type of enciphering in which cycle shifting is used called the Caesar cipher. The actual cipher which was used by Caesar with cyclic shift k = 3. In such type of cyclic shifting letter, we shift A to D, B to E and so on. It is shown in the figure below completely,

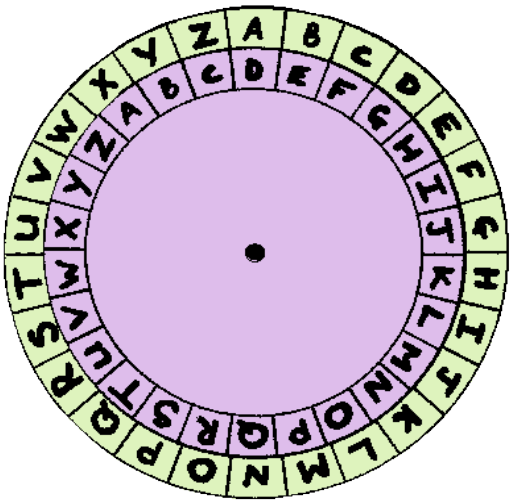


Figure 5. Caesar cipher with k = 3

In the form of table, we can make the arrangement of alphabets as

Table 2. Caesar cipher with k = 3

A	B	C	D	E	F	G	H	I
D	E	F	G	H	I	J	K	L
J	K	L	M	N	O	P	Q	R
M	N	O	P	Q	R	S	T	U
S	T	U	V	W	X	Y	Z	
V	W	X	Y	Z	A	B	C	

Example 36: Encipher the plaintext "HARD WORK IS KEY TO SUCCESS"
Using Caesar cipher with k = 3

Solution: We use the key k = 3 for enciphering as shown in above table 2.3, by substituting each alphabet in the plaintext by the alphabet below it. By converting all the alphabets of the plaintext we obtain the ciphertext

KDUG ZRUN LV NHB WR VXFFHVV

As a result, we obtain the text which is meaningless. We can decipher this meaningless text by replacing each letter in the text by the letter above each one. As a result, we obtain the original plaintext

HARD WORK IS KEY TO SUCCESS.

1.3.3 Vigenere Cipher

We now explain a periodic substitution cipher composed of shifts ciphers. This cipher is called Vigenere cipher named after Claise de Vigenere, a cryptologist of the 16th century. This cipher with period p and key sequence $(k_1, k_2, k_3, \ldots, k_p)$. It is simple to identify the shift cipher by the letter which moves to A. For example, the letter A for key cipher

with k = 3 is D. The word formed by this cipher is called Vigenere cipher. Each letter in the key word, the table contains the each row with one alphabet. The letter below the A forms the cipher. It is given below the table 2.4 with key word TASK.

Table 3. Vigenere cipher with key word Task

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K

Example 37: Encipher the given plaintext using the Vigenere cipher with key word TASK.

I MISS YOU

Solution: To encrypt the plaintext we follow the following procedure, we see the each word in the sentence, and for example the first word I in the message is replaced with the letter c and similarly M the second letter in the second word is replaced by G and I is replaced by J, and continuing this procedure we get the cipher text

C GJLD SPN

We obtain a text which is meaningless. Similarly, we can decipher the message by taking key word in reverse direction and in this way obtain the original message which is

I MISS YOU

1.3.4 Modular Enciphering and Affine Cipher

Let n be the number of characters in the message alphabet A. Let S = $\mathbb{Z}_n$ be the ring of integers modulo n. The enciphering in which algebraic operations of $\mathbb{Z}_n$ are used is called modular enciphering. An affine cipher is the simplest example of modular ciphering.

Let a, b $\in \mathbb{Z}_n$ and suppose a is co prime to n. Then a has inverse in $\mathbb{Z}_n$. Hence the mapping $\phi: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$$\phi(x) = ax + b \qquad (2.2)$$

It is a bijective mapping. The mapping in the can be express as the operations of multiplication and addition in $\mathbb{Z}_n$ is given by

$$\phi(x) = ax + b \quad \text{mod n} \qquad (2.3)$$

Where x mod n represent the remainder left by dividing by n. For deciphering, we use the inverse mapping which is given by

$$\phi^{-1}(y) = a^{-1}(y - b) = a^{-1}y - a^{-1}b \qquad (2.4)$$

For every $y \in \mathbb{Z}_n$ If the plaintext alphabets A is the set of alphabets A, B, C, …, Z then n = 26. We take the mapping ϕ: A $\longrightarrow$ B as shown in table 4

Table 4. Affine cipher

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9
J	K	L	M	N	O	P	Q	R
10	11	12	13	14	15	16	17	18
S	T	U	V	W	X	Y	Z	
19	20	21	22	23	24	25	0	

Example 38: Use the mapping ϕ given above and the affine cipher

$\phi(x) = (5x + 5) \mod 26$ (2.5)

and for deciphering the mapping

$\phi(x) = (7x + 4) \mod 26$ (2.6)

1. To encipher ALGEBRA.
2. To decipher AMEQMNZW.

Solution: As 5 is co-prime to 26 therefore, ϕ is bijective.

1. Replace each letter in the plaintext by a number which is shown above in the table and then applying the mapping ϕ. We write the alphabet relate to ϕ(x). It is completely described in table 5.

Table 5. Enciphering process

Plaintext	A	L	G	E	B	R	A
x	1	12	7	5	2	18	7
$5x+5$	10	65	40	30	15	95	40
$5x+5 \bmod 26$	10	13	14	4	15	17	14
~~Cipher-text~~	J	M	N	D	O	Q	N

2. To decipher the text we use the inverse mapping ϕ^{-1}.If 7x + 4 = y then x $=7^{-1}(y-4)$. In $\mathbb{Z}_{26}$, = $7^{-1} = 15$ as 15 × 7 = 105 = 1 (mod 26) so for deciphering the mapping is d(y) = 15y – 60 = 15y + 18. The deciphering process is given below in table 2.6

Table 6. Deciphering procedure

Ciphertext	A	M	E	Q	M	N	Z	W
y	1	13	5	17	13	14	0	23
15y + 18	33	213	93	273	213	228	18	25
15y+ 18 mod 26	7	5	15	13	5	20	18	25
Plaintext	G	E	O	M	E	T	R	Y

1.3.5 Hill Cipher

We now discuss the importance of the affine cipher which is called as Hill Cipher. Let n be the number of alphabetic letters and r be any positive integer such that $r \geq 1$. Then the mapping f: A $\longrightarrow \mathbb{Z}_n$ which can be extended to $f: A^r \longrightarrow (\mathbb{Z}_n)^r$ by defining the mapping

$$\phi\,(b_1, b_2, b_3, \ldots b_r) = (\phi(b_1), \phi((b_2), \phi((b_3), \ldots, \phi((b_r)) \quad (2.7)$$

Let us denote the elements of $(\mathbb{Z}_n)^r$ as columns and let $(\mathbb{Z}_n)^{r\times r}$ denote the set of $r \times r$ matrices having entries from $\mathbb{Z}_n$. If M is invertible then

$$(\det M)\,(detM^{-1}) = \det(M\,M^{-1}) = \det I = I \quad (2.8)$$

Therefore $\det M$ is an invertible element in $\mathbb{Z}_n$. In the other direction if $\det M$ is invertible in $\mathbb{Z}_n$ then M^{-1} is given by $M^{-1} = (\det M)^{-1} adjM$

Therefore we can say that a square matrix M over $\mathbb{Z}_n$ is an invertible if $\det M$ is co-prime to n.

If M be a matrix whose inverse exist in $\mathbb{Z}_n$ and D $\in (\mathbb{Z}_n)^r$. Then the mapping

$$\phi(X) = KX + D \quad ; \quad \forall \in (\mathbb{Z}_n)^r \quad (2.9)$$

This is called Hill Cipher. To decipher we use the inverse direction

$$\phi^{-1}(Y) = M^{-1}(Y - D) \quad (2.10)$$

Example 39: Use the Hill cipher with n = 26 and r = 2

$$\phi\begin{bmatrix}x_1\\x_2\end{bmatrix} = \begin{bmatrix}8 & 5\\5 & 6\end{bmatrix}\begin{bmatrix}x_1\\x_2\end{bmatrix} + \begin{bmatrix}7\\9\end{bmatrix} \pmod{26} \quad (2.11)$$

1. Encipher the word MOUNTAIN
2. Decipher the word AJGLLRKE

Solution: We firstly verify that $\det\begin{bmatrix}8 & 5\\5 & 6\end{bmatrix} = 23$ is co-prime to 26. We divide the word into blocks of two letters. We represent each block by the number of columns given by the mapping f and then apply the mapping ϕ. This enciphering process is given by.

Table 7. Deciphering Algorithm

Plaintext	MO	UN	TA	IN
			$\begin{bmatrix}x_1\\x_2\end{bmatrix}$ $\begin{bmatrix}13\\15\end{bmatrix}$	$\begin{bmatrix}21\\14\end{bmatrix}$ $\begin{bmatrix}20\\1\end{bmatrix}$ $\begin{bmatrix}9\\14\end{bmatrix}$
$\phi\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$\begin{bmatrix}4\\8\end{bmatrix}$ $\begin{bmatrix}11\\16\end{bmatrix}$	$\begin{bmatrix}16\\11\end{bmatrix}$	$\begin{bmatrix}19\\8\end{bmatrix}$	
Ciphertext	DH	KP	PK	S

In $\mathbb{Z}_{26}(detM)^{-1} = 23^{-1} = 17$. Therefore $M^{-1} = 17\begin{bmatrix} 6 & -5 \\ -5 & 8 \end{bmatrix} = \begin{bmatrix} 24 & 19 \\ 19 & 6 \end{bmatrix}$.

To decipher the message the following mapping is used.

$$\phi^{-1}\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 24 & 19 \\ 19 & 6 \end{bmatrix}\left(\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} - \begin{bmatrix} 7 \\ 9 \end{bmatrix}\right) \quad (2.12)$$

METHOD

The literature review is very important and vital not only to connect the conceptual ideas with handy examples and applications. It provides the light for the role of a research study and this study is linked to secure communication. So in this chapter fundamental background is lighted by stating important results in numbers. Therefore literature review plays a vital role in the field of a research study.

RESULT AND DISCUSSION

A. REVIEW OF S-BOX THEORY

2.1 Rijndael Algorithm

Belgian cryptographers Daemen & Rijmen, (1999) designed a new algorithm for enciphering. It is known as Rijndael algorithm. There are several versions of Rijndael in AES; they differ in key length, block, and number of rounds. The possible values for this block length and the key length are 256, 192, and 128 bits. It is a substitution-permutation network (SPN) with 14, 12, and 10 rounds, depending on the size of the key. As mentioned earlier, the general scheme of Rijndael is like an iterated block cipher.

There are several operations that are used in Rijndael;

- Round key addition
- Byte substitution
- Row shift
- Column mix

The detailed discussion is presented in Daemen & Rijmen, (1999).

2.2 Polynomial Description of AES

Rosenthal (2003) explained the complete Rijndael Advance Encryption Standard in the sense of a complete polynomial description, which was taken for selection by the National Institute of Standard and Technology (NIST), and it described the structure of S-boxes. It also shows how the whole algorithm can be described in a finite ring through a sequence of algebraic manipulation. In Rosenthal (2003), it was explored that description relates to the Algebra of substitution box, so-called 'S-Box' and the most important non-linear part of the AES system. The sparse polynomial explained the S-box.

2.3 Action of Symmetric Group S_8 on AES S-box

Hussain et al., (2010) described a new S_8 S-box which is made by acting symmetric group S_8 on AES S-box and these obtained S-boxes are used to

construct40320^{40320} secret key. Thus in this way, we obtain the encryption keys with the permutations of these existing S-boxes which give 40320 new S-boxes which improve the security and system become more reliable and safe. In Hussain et al., (2010) it is explained that how we construct the new S-boxes, there are several steps which are used to construct the S_8 S-box;

- Conversion hexadecimal to decimal
- Conversion decimal to binary
- Acting S_8on the elements of AES S-box
- Conversion to decimal

There are 40320 elements in symmetric group S_8, acting all the elements on AES S-box we get newly S_8 AES S-boxes whose nonlinearity is same as the original one.

Actually, on the elements of the AES S-box we act the symmetric group S_8 and we reshuffle the elements of the S-box. Here the elements of S_8 are permutations which are acting on the binary digits and permute the original elements.

Here is the example of S_8 AES S-box whose nonlinearity is same as the original one.

Table 8. S_8 AES S-box

209	118	215	243	91	241	243	204	18	128	213	177	127	207	185	87
105	9	232	246	123	226	197	90	188	78	25	189	46	28	83	72
159	254	139	21	23	183	223	108	22	156	220	218	210	106	146	134
4	205	145	201	34	15	132	43	133	3	8	89	249	149	27	214
160	137	52	35	163	117	99	24	67	179	79	155	176	217	181	12
195	202	0	252	16	126	154	227	113	233	63	178	97	100	98	237
74	253	57	251	193	228	147	140	196	250	1	247	66	54	175	56
194	153	64	173	11	174	50	222	62	31	107	144	2	255	219	75
236	36	131	124	231	143	68	135	76	157	119	182	84	230	162	211
80	136	229	110	17	49	10	40	69	125	58	6	111	103	161	235
88	19	51	33	224	5	20	102	73	203	60	81	138	142	92	242
221	104	151	244	172	206	101	184	116	71	94	121	212	115	61	32
59	114	148	53	38	29	30	77	120	238	86	167	225	190	169	41
82	55	158	85	96	129	95	37	208	150	199	186	13	200	166	47
216	122	42	130	240	234	45	14	171	39	141	248	109	198	48	239
44	152	168	164	191	93	65	112	192	170	180	165	26	70	187	7

2.4 Image Encryption

(Hussain et al., 2012) described with the help of two basic and key concepts image encryption: one is the theory of replacement or substitution, permutation network and the other is called Chaos theory. Furthermore, it is analyzed the proposed algorithm's strength by applying it on a color image and derive that the color image can be encrypted through the algorithm successfully and it makes secure and safe against many classic attacks. In Hussain et al., (2012) he demonstrates that chaotic

encryption system is not secured and it can attack easily, So in order to improve the security he offered to adopt the non-linear functions, limited in time and space to alter the key continuously

2.5 Permutation properties

Beth & Ding, (1994) explained the vital permutation's properties which one can use in secure key block cipher as a round function to secure it from different attacks. Good nonlinearity and high order of several classes of almost complete nonlinear permutations and other permutations in $\mathrm{GF}(2)^n$ are presented. In Beth & Ding, (1994) key and basic properties of APN permutation network are highlighted, in this way we obtained highly nonlinear S-boxes.

2.6 Analysis of S-box

Hussain et al., (2011) divided the work into two sections, 1st section represents the analysis of S-box and bit independent criterion, their nonlinearity etc. whereas 2nd section represents conclusion. It is also analyzed against different criterions such as bit independent criterions, differential approximation probability and linear approximation probability; in the view of this work by linear fractional transformation we can construct new s-boxes.

2.7 Analysis of residue prime S-box

Hussain et al., (2011) made some useful efforts to analyze the S-box which is based on the residue of a prime number, which includes differential approximation probability (DP), bit independent criterion (BIC), linear approximation probability (LP) and non-linearity. With the help of these results, we derive the result which is linked with the algebraic encryption strength and weakness of this S-box. In Hussain et al., (2011) they analyzed S-box for different criteria and derived that the residue prime S-box is not satisfied all criteria absolutely.

2.8 Construction of S-boxes using projective general linear group

Altaleb et al., (2017) have developed new techniques to construct highly non-linear S-boxes. Firstly, they used the action of $PGL(2, GF(2^8))$ on the Galois field of 256 elements and then use permutations to construct new kind S-boxes. They computed the strength of these S-boxes and made some useful analysis. They compared these S-boxes with the well known existing S-boxes and show that the analysis of these S-boxes is comparatively better. By the action of the projective general linear group, they constructed 16776960 numbers of S-boxes.

2.9 Cryptographic criteria of Boolean functions

It was studied the mathematical and practical cryptographic criteria of Boolean functions in Elhosary et al., (2013) introduced the algorithm that fulfills the criteria and introduced the Boolean functions that satisfy the better cryptographic criteria. The

Boolean function representation and cryptographic assessment were presented in Elhosary et al., (2013). It was beginning of cryptographic algorithms and opened the new door for the analysis and further, studied the Hash function.

2.10 Matrix manipulation of cryptographic functions

Some efforts were made to investigate the matrix manipulation of cryptographic functions in Meletious et al., (2015). Firstly, considered the cryptographic repeated applications of orbit and found difficult to derive the cryptographic functions which are related to the orbit's length. They investigated the behavior of matrix's power which is made from the generator of the multiplicative group of several primes $p$in $\mathbb{Z}_p$. It was studied matrix factorization approach at the end in (Meletious et al., 2015)

2.11 A method to construct S-boxes based on permutations

In a block cipher, S-boxes are very important nonlinear components. The nonlinearity makes the system more safe against the differential and linear cryptanalysis. These S-boxes are key dependent. In Kazlauskas et al., (2016) simple four algorithms are presented to construct the S-boxes which are based on the key dependent. Kazlauskas et al., (2016) presented eight distance metrics for the analysis of these key dependent S-boxes. In the last section of K. (Kazlauskas et al., 2016), they experimentally investigated the quality analysis of these key dependent S-boxes. These S-boxes can be used in block cipher like AES cipher. It was studied that by changing the secret key, the order of the elements of the S-boxes based on key dependent are also changed.

2.12 Construction of S_{16} AES S-boxes

As earlier some efforts are made to construct the S_8 S-boxes by the action of symmetric group S_8 and constructed 40320 newly S_8 S-boxes as the order of the symmetric group in Hussain et al. (2010). In Siddiqui et al., (2016) used the action of S_{16} instead of S_8 to construct the new S_{16} S-boxes and generate new 16!(20922789888000) S-boxes as the order of the symmetric group S_{16}. At the end finally, they analyzed the strength of the proposed S-boxes by different properties like balance properties, nonlinearity, bijection, bit independent criterion and linear approximation probability etc. These S-boxes are used to develop $m^{16!}$ secret keys which are used to make the system more reliable and secure. One of the advantages of AES algorithm using S_{16} S-boxes gives more reliable keys as compared to the algorithm using in S_8S-boxes.

2.13 Construction of large cryptographic S-boxes

It is clear that large S-boxes have better cryptographic properties than the smaller S-boxes. The main target is to achieve the large S-boxes with bent functions. In Detombe & Tavares, (1992) constructed 5×5 S-boxes with the required bent function. Whenever, these variables are odd in numbers then they have desired cryptographic properties and can be constructed easily. These newly constructed S-boxes fulfill the criterion of good S-boxes. Bent function plays key role to achieve the maximum nonlinearity.

2.14 Improvement in cryptographic properties of AES S-box by multiplication

Many cryptographic algorithms have been proposed but AES is the latest and secure crypto-algorithm. This cryptographic algorithm used permutations operations to make information more secure. We now give a brief description of the cryptosystem approved for general standards and technology (NIST). It is called the Advance Encryption Standard (AES) and was adopted and effective on May 26, 2002. Florin Medeleanu, CiprianRacuciu and Marius Rogobete studied the chances to improve the cryptographic properties of AES algorithm in Medeleanu et al., (2015) and effect of these improvements. It is also described that all the cryptographic properties could not improve at the same time.

2.15 Construction of S-boxes for lightweight block cipher

During the study of different techniques for the construction of S-boxes, it is derived that there is some space for the improvement in the cryptographic properties. H. Mhajloska & Gligoroski (2011) made some useful efforts by using Quasigroup of order 4 to construct new cryptographic S-boxes in (Mhajloska & Gligoroski, 2011). Further, it has opened new door to construct new S-boxes which are satisfied the criterion for the good S-box. They also compare the properties of these constructed S-boxes with the well known existing S-boxes.

2.16 Affine-power Affine S-box

Cui & Cao (2007) studied the algebraic and polynomial structure of the AES S-box and derive that only 9 terms are involved for algebraic expression, while 255 terms for the inverse S-box. They presented new affine-power-affine S-box to improve the algebraic complexity. The algebraic complexity improves of AES S-box from 9 to 253 while for the inverse 255 remain same. They compare the properties of this affine-power-affine S-box with the well known S-boxes and derived that this S-box fulfills the criterion for the good S-box.

2.17 Linear cryptanalysis method for DES cipher

M. Matsui derived a new technique for cryptanalysis of DES cipher, which is a well known plaintext attack. It is possible to break 8 rounds with 2^{22} and 16 rounds with 2^{47} plaintext. We can apply this method on any situation as described in Matsui (1994). It was studied that these attacks for the ciphertext can deal with any non-random situation at any stage

The deciphering process is given below in the table completely

Table 9. Hill Deciphering procedure.

Ciphertext	AJ	GL	LR	KE
		$\begin{bmatrix}y_1\\y_2\end{bmatrix}\begin{bmatrix}1\\10\end{bmatrix}\begin{bmatrix}7\\12\end{bmatrix}\begin{bmatrix}12\\18\end{bmatrix}\begin{bmatrix}11\\5\end{bmatrix}$		
$\Phi^{-1}\begin{bmatrix}y_1\\y_2\end{bmatrix}\begin{bmatrix}5\\22\end{bmatrix}\begin{bmatrix}5\\18\end{bmatrix}\begin{bmatrix}5\\19\end{bmatrix}\begin{bmatrix}20\\0\end{bmatrix}$				
Plaintext	EV	ER	ES	TZ

B. CONSTRUCTION OF S_8 RESIDUE PRIME AND AFFINE AES S-BOXES

Rijndael Block Cipher is based on 128 bits and developed by two cryptographers, Joan Daemen and Vincent Rijmen, was taken on Advanced Encryption Standard (AES) by (NIST) on October 2, 2000. AES is one of the most reliable algorithms which are used in cryptography of symmetric key. The S-box has a vital role in AES, therefore most of the work is focused on the battlement of the S-boxes. In this section, we represent new S_8 S-boxes by using action of S_8 on residue prime S-box as earlier some efforts were made (Hussain et al., 2010). Furthermore, we utilize these S-boxes to construct 40320^{40320} secret keys from S_8 S-boxes and then we utilize these keys and propose a new algorithm which is more reliable when two channels or persons communicate each other. S-box is the only non-linear component which provides confusion capability for AES.

3.1 Algebraic Expression of Residue Prime S-box

The expression for residue prime s-box is obtained from the function in GF(2^8) . As GF(2^8) is a finite field, therefore inverse with respect to multiplication of every element exists and 0 $\longrightarrow$ 0. This inversion of multiplication for the function is as follows

$$F(x) = \begin{cases} x^{-1} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

This affine transformation which can be decomposed into two steps: 1. The linear transformation $L(x)$

$$y = L(x)$$

And the proposed implementation depends on the residue of a prime number and the complete entries in S-box are 256. These entries are the residue of 257, there is logic behind the choice of the number 257 because the residues from 1 to 255 have unique inverses. Furthermore, these residues can be utilized in all block size of AES.

3.2 S_8 residue prime S-boxes

Firstly, we perform the action of S_8 on the original residue prime S-box as the new S-boxes was developed on similar action on AES S-box (Cui & Cao, 2007) and sequentially construct 40320 new residues prime S-boxes. This process is preceded with the conversion of the elements into bytes and the elements in bytes are permuted by the action of the symmetric group S_8 which gives 40320 new S-boxes. For the formation of new S-boxes, the resulting algebraic expression is

f: $S_8\times$ residue prime S-box $\longrightarrow S_8$ S-boxes

In this way, the number of total new S-boxes is 40320 due to an order of the symmetric group because we are acting the elements of symmetric group S_8 on the elements of S-box.

Table 10. Action of S_8 on residue prime S-box

$\pi_{1((Sbox\ residue\ prime)}$	=	$Sbox_1$
$\pi_{2((Sbox\ residue\ prime)}$	=	$Sbox_2$
…	…	…
…	…	…
…	…	…
$\pi_{40320((Sbox\ residue\ prime)}$	=	$Sbox_{40320}$

Where π_1, π_2, π_3,…, π_{40320} are the elements in S_8. In this algorithm, the elements of original residue prime S-box is converted into binary form and then applying the action of symmetric group S_8 we get the 40320 new S_8 residue prime S-boxes. This process can be presented as follows

Table 11. Algorithm for S_8 S-boxes

Residue prime S-box ↓
Convert elements of residue prime S-boxes into bytes ↓
Acting S_8on these elements ↓
We get 40320 new S_8 S-boxes

An example to construct new S_8 residue prime S-boxes from the main S-box is shown in table 2.12

Table 12. An example of bijective S_8 S-boxes

0	2	130	105	194	91	23	163	210	196	184	183	169	177	197	116
242	118	88	217	101	50	237	189	71	68	102	221	90	195	60	203
246	168	190	215	49	136	179	162	46	147	166	9	95	20	111	159
153	42	24	125	158	82	123	243	179	244	209	62	45	55	216	89
254	107	69	213	239	170	249	186	38	150	65	36	181	251	198	248
171	154	225	80	206	127	3	66	180	37	40	226	176	164	228	29
99	58	135	139	33	44	63	10	235	152	178	250	188	208	245	28
229	120	124	25	114	137	175	57	15	34	173	140	113	236	51	106
255	1	156	205	26	143	122	83	240	241	199	81	119	160	231	138
142	27	234	11	18	74	12	96	110	21	252	193	218	223	117	121
204	157	227	22	86	98	48	222	219	70	192	253	129	56	146	31
108	85	14	52	5	75	214	191	100	212	76	7	92	17	43	187
149	8	167	46	201	211	200	47	6	77	13	133	144	104	131	238
220	103	97	145	230	161	247	84	253	232	112	141	126	207	41	72
94	4	53	202	61	172	35	148	182	185	67	19	224	155	39	174
132	32	134	59	79	87	73	78	54	16	93	233	165	64	151	128

3.3 Generating Affine AES S-box through affine mapping

We introduce the affine mapping between byte and the AES S-box. In this case, we firstly convert the elements of the S-box into binary digits and then develop a relation between byte and all the elements of residue prime S-box. So we define a mapping between two bytes such as

$f: (10101010) \longrightarrow (11111111)$

We define an affine mapping between the each binary pairs of the bytes, in the above case we get the result (01010101). After converting all the elements through such type of affine mapping we convert all these bytes into decimal. Here we generate new S-box through affine mapping of the byte (10101010) and the elements of AES S-box and by changing the byte we can generate finite many S-boxes. Also we develop an algorithm to construct all possible 256 AES S-boxes having pseudo code is given below.

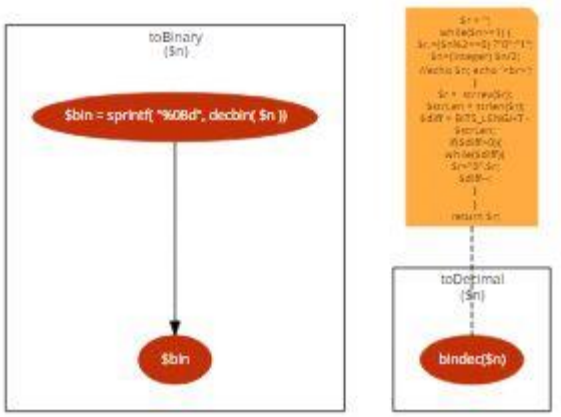
➢ Pseudo Code

1-fetch data from AESSbox.txt to work on and store in an array
2- loop on this array
  2.1 convert each element to binary
3- Get a random value r from converted binary elements
4-Permenute each element of array with r
  4.1 Loop on each array element
    4.1.1 Split each element to array
    4.1.2 Loop on this sub_array
    4.1.3 Perform permute step that is subtract each subvalue of sub_array with every value of random number (r) binary
    4.1.4 save result in permute variable
  4.2 Save permute variable in permuted_array
5- Convert permuted_array back to decimal
6- Write permuted_array on file(data.txt) using file operations

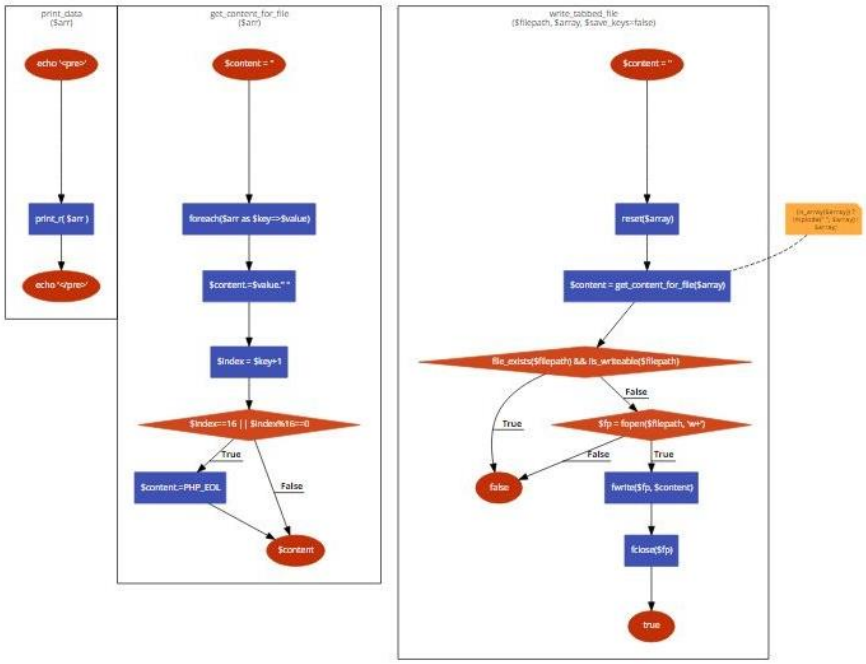
➢ Flow Chart

The flow chart of the above Pseudo is given below which elaborate the complete algorithm which consist of the following three steps.

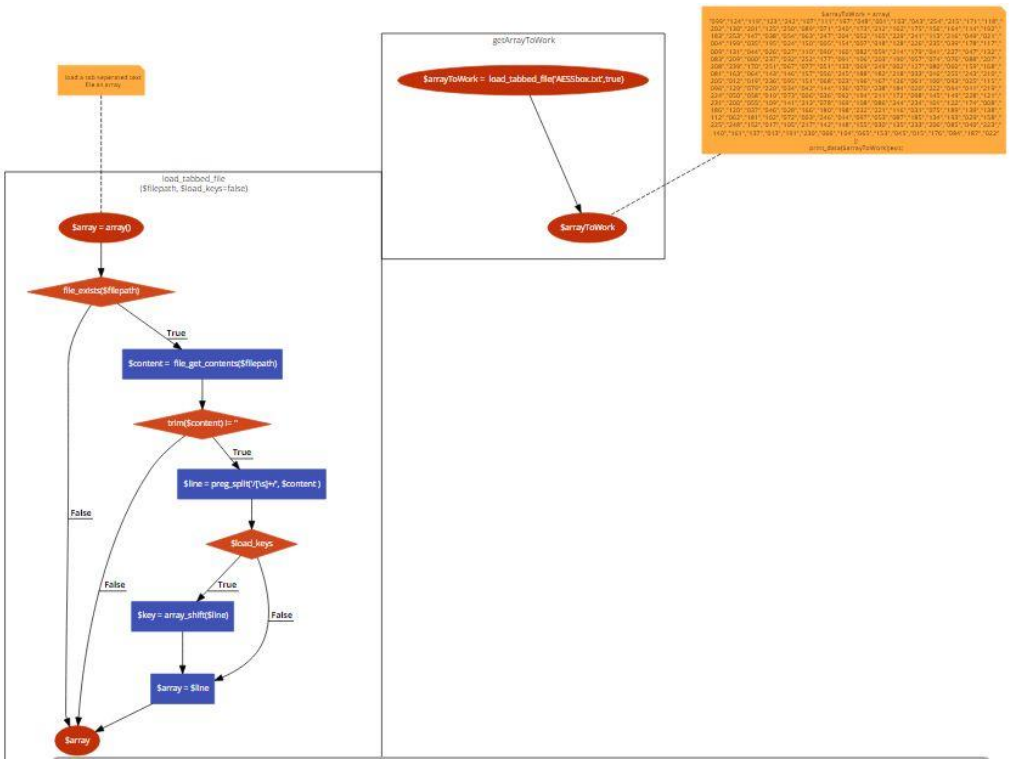
➢ Step 1



- Step 2


print_data
($arr)
echo '<pre>'
print_r($arr)
echo '</pre>'
get_content_for_file
($arr)
$content = ''
foreach($arr as $key=>$value)
$content.=$value." "
$index = $key+1
$index==16 || $index%16==0
True
$content.=PHP_EOL
False
$content
write_tabbed_file
($filepath, $array, $save_keys=false)
$content = ''
reset($array)
$content = get_content_for_file($array)
file_exists($filepath) && is_writeable($filepath)
False
True
$fp = fopen($filepath, 'w+')
False
True
false
fwrite($fp, $content)
fclose($fp)
true

- Step 3


getArrayToWork
$arrayToWork = load_tabbed_file('AESSbox.txt',true)
$arrayToWork
load_tabbed_file
($filepath, $load_keys=false)
$array = array()
file_exists($filepath)
True
$content = file_get_contents($filepath)
trim($content) != ''
True
$line = preg_split('/[\s]+/', $content)
$load_keys
True
$key = array_shift($line)
False
$array = $line
False
False
$array

3.4 Analysis of S_8 residue prime S-boxes and affine S-boxes

We discuss most important ordinary properties which are founded in disparate S-boxes to improve the strength of this recommended algorithm.

3.4.1 Algebraic complexity

The algebraic complexity of S_8 residue prime S-boxes is the same as the AES in T. Beth and C. Ding (1994). We are acting S_8on the original S-box where the elements of $S_8$are permutations and these permutations do not affect the S-box's algebraic complexity. In the case of affine S-boxes we are developing the affine mapping between the fixed byte and the original S-box where this fixed byte reshuffle the elements of S-box just like permutations. These bytes do not affect the algebraic complexity of S-box.

3.4.2 S_8 S-boxes and affine S-boxes are Bijective

In the Galois field GF(2^8) if we consider the input to all the elements of S-box, then the output takes the unique values in GF(2^8). The example of bijective affine S-box is given in table 2.13 below.

Table 12. Affine AES S-box

156	131	136	132	13	148	144	58	207	254	152	212	1	40	84	9
72	125	54	130	5	166	184	15	62	43	93	80	99	91	141	63
72	2	108	217	201	192	8	51	203	90	26	14	142	39	206	234
251	56	220	60	231	105	250	101	248	237	127	29	20	216	77	138
246	124	211	229	228	145	165	95	173	196	41	76	214	28	208	123
172	46	255	18	223	3	78	164	149	52	65	198	181	179	167	48
47	16	85	4	188	178	204	122	186	6	253	128	175	195	96	87
174	92	191	112	109	98	199	10	67	73	37	222	239	0	12	45
50	243	36	19	160	104	187	232	58	88	129	194	155	162	230	140
159	126	176	35	221	213	111	119	185	17	71	235	33	161	244	36
31	205	197	245	182	249	219	163	61	44	83	157	110	106	27	134
24	55	200	146	114	42	177	86	147	169	11	21	154	133	81	247
69	135	218	209	227	89	75	57	23	34	139	224	180	66	116	117
143	193	74	153	183	252	9	241	158	202	168	70	121	62	226	97
30	7	103	238	150	38	113	107	100	225	120	22	49	170	215	32
115	94	118	242	64	25	189	151	190	102	210	240	79	171	68	233

3.4.3 Nonlinearity

Nonlinearity's upper bound is $N(f) = 2^{n-I} - 2^{\frac{n}{2}-I}$ for S-box in GF(2^8).As the elements of S-box are in GF(2^8), 120 is the optimal value of N. Through Walsh Hamamard transform of Boolean function we calculate the nonlinearity. The S_8 residue prime S-box is not entirely a non linear function and its nonlinearity is remained same 99.5 as the original residue prime S-box whereas the nonlinearity of affine AES S-box is decreased by 110.875 as the original AES S-box has 112.

3.4.4 Balance Property

A Boolean functionf_n:$Z_2^n \longrightarrow Z_2$ is known as balance function if

$\#\{x|(x) = 0\} = \#\{x|f(x) = 1\}$ or $HW(f) = 2^{n-1}$. The main feather of this property is that with higher the magnitude imbalance of a function, moreover due to this property we obtained a high probability linear approximation. Thus, due to imbalance property Boolean function becomes weak for linear cryptanalysis. Like AES and S_8AES S-boxes, all the Boolean functions $f_i i$ = 1,2,3,…,8 used in the structure of the Affine and S_8residue prime S-boxes fulfill the criteria of balance property. Hence, our S-boxes are balanced.

3.4.5 Bit independence criterion

In cryptographic output bits independence criterion plays very vital role. It needs pair wise all the avalanche variables however given set's independent of avalanche vectors. The avalanche vectors are constructed by the complementing of a single plaintext bit. The main results of BIC analysis of proposed affine S-box are presented in Table 2.15. The BIC of this affine S-box is acceptable as compare with the other S-boxes in the regard of encryption strength. So our S-box is comparable by analysis. It satisfies bit independent criterion as presented.

Table 13. Performance Indexes for S-box based on action of S_8 on residue Prime

Analysis	Max.	Min.	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	104	94	99.5			
SAC	0.671875	0.34375	0.516846	0.0331112		
BIC		94	102	3.5051		
BIC- SAC		0.46875	0.502511	0.0180058		
DP					0.273438	
LP	162					0.136719

3.4.6 Linear approximation probability

We examine the variation of an event in the LP. This amount play key role in determining the maximum imbalance value for the output in an event. The two masks Γx and Γy which are used to link of the input bits and output bits. The LP is also expressed as

$$LP = \max \left| \left\{ \frac{\#\{x|x.\Gamma x = S(x).\Gamma y}{2^n} \right\} - \frac{1}{2} \right|$$

Where all inputs contains in set X and total elements are 2^n. The LP result of this affine S-box is presented in table 15.

3.4.7 Differential approximation probability

The nonlinear transformation should be unique and lies in their differential uniformity which is essential quality. The output differential Dy_i maps by an input differential Dx_iwhich assure that uniformity in function probability for each. The DAP of affine S-box is measured and expressed as:

$$DP^s\ (\Delta x \rightarrow \Delta y) = \left[\frac{\#\ \{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m} \right]$$

The differential approximation probability's maximum value for proposed affine S-box is 0.0234.Table 2.14 and Table 2.15 shows the comparison of differential approximation probability of proposed S-boxes with AES, APA, Gray, S_8 AES, Skipjack, residue of prime and Xyi S-box.

The differential approximation probability is shown below in the table 14

Table 14. Performance Indexes for affine AES S-box

Analysis	Max.	Min.	Average	Square Deviation	The differential approximation probability	The linear approximation probability
Nonlinearity	113	109	110.875			
SAC	0.5625	0.429688	0.505859	0.0160466		
BIC		108	110.607	1.01204		
BIC- SAC		0.486328	0.505162	0.011663		
DP					0.0234375	
LP	149					0.0820313

3.4.8 Strict avalanche criterion analytically

The SAC depends on the changing of input bit results and output bits. When a single bit varies on input, it levels half of output bits and an S-box is satisfied SAC. The avalanche of changes causes by a single variation in the input of network while Substitution Permutation (S-P) network is used in S-box. The comparison of affine S-box is shown in the table 15 below

Table 15. Comparison of Performance indexes of proposed Affine AES S-box and other S-boxes

S-boxes	Nonlinearity	SAC	BIC–SAC	BIC	DP	LP
AES S-box	112	0.5058	0.504	112.0	0.0156	0.062
APA S-box	112	0.4987	0.499	112.0	0.0156	0.062
Gray S-box	112	0.5058	0.502	112.0	0.0156	0.062
Skipjack S-box	105.7	0.4980	0.499	104.1	0.0468	0.109
Xyi S-box	105	0.5048	0.503	103.7	0.0468	0.156
Residue Prime	99.5	0.5012	0.502	101.7	0.2810	0.132
Affine AES S-box	110.875	0.505859	0.505162	110.607	0.0234375	0.0820313

3.5 Image encryption applications

It turn to a major issue that how can we make secure and reliable confidentiality, authenticity and probity of image. The encryption of the image is to mediate the image reliably over the channel or network so that any unofficial user can free to decrypt the image. The encryption of the image and video encryption have vast applications and usage in the area including the communication through internet, mediation, armed communications etc. The progression of encryption is moving toward a future of endless possibilities. Here we encrypt the Lena's image through affine AES and residue prime S_8 S-box. We do some statistical analysis and compare them with other S-boxes.

3.6 Statistical Analysis

Here, we evaluate the plain and encrypted image by some statistical analyses namely; energy, homogeneity, contrast, correlation and entropy. Instead of algebraic analysis we implement this newly proposed balanced 8×8 S-box in image encryption through these statistical analyses.

3.6.1 Energy

The energy of encrypted image is assessed by energy analysis. The Gray-Level Co-occurrence Matrix (GLCM) is used for this resolve. Energy is defined as the sum of squared components in GLCM. That is

$E = \sum_u \sum_v p^2(u,v)$, where u and v show the pixels in the image and $p(u,v)$ provides the number of GLCM. For constant image the value of energy is 1.

3.6.2 Homogeneity

The substances of an image are surely distributed. In homogeneity analysis, the nearness of distributed elements of GLCM to GLCM diagonal is calculated. It is also famous as gray tone spatial dependency matrix. The GLCM exemplifies the statistics of arrangement of pixel gray levels in tabular form. The analysis can be lengthy further by treating entries from GLCM table. The precise form of Homogeneity is

$$H = \sum_u \sum_v \frac{p(u,v)}{1-|u-v|}.$$

3.6.3 Contrast

The value of contrast supports the observer to detect the objects of an image. A balanced contrast value in the image soaks the objects which permits the more accurate image ID. By way of the value of randomness upsurges in encrypted image, it also increases the contrast to very high level. Due to nonlinearity of mapping, the objects of the image are slanted entirely. That is the high value of contrast in the encrypted image displays the strong encryption since it is reliably related to the confusion produced by the S-box. That is

$C = \sum_u \sum_v (u-v)^2 p(u,v)$. In the case of constant image, the value of contrast is zero.

3.6.4 Correlation

Correlation analysis is done in three diverse ways. The vertical, horizontal and diagonal formats are designated for this purpose. By allowing for the texture of entire image, the correlation of pixel to its neighbors is examined. For the resolution, the

complete image is also analyzed together with partial regions. The correlation is considered as

$$K = \sum_{u,v} \frac{(u - \mu u)(v - \mu v)\, p(u,v)}{\sigma_u \sigma_v}.$$

For a faultlessly positive or perfectly negative images, the value of correlation is 1 or -1 respectively. And for constant image, the correlation is zero, which means that it is not a number, it is just a data type for demonstrating the redefined value.

3.6.5 Entropy

The quantity of randomness is measured by entropy. The degree of entropy is related with the organization of the objects in an image. The randomness of an image is enlarged by substituting nonlinear components in the system. The top level of randomness styles the image hard to detect. Nevertheless, due to lacking in randomness, the encrypted image is just recognized. Hereafter, the encryption strength of an encrypted image is straight measured with entropy and its mathematical form is

$$H = -\sum_{k=0}^{n} p(x_k) \log_b p(x_k),$$

where x_k represents the histogram calculations. The results of newly proposed 8×8 S-box for this analysis are shown in Table 17 and Table 18 which are closed to the standard values.

Table 16. Contrast, Correlation, Energy, Homogeneity and entropy of plain image and cipher image of Lena (512x512, png) by affine AES S-box and residue prime S_8 S-box.

Images	**Entropy**	**Contrast**	**Correlation**	**Energy**	**Homogeneity**
Plain image	7.4451	0.2100	0.9444	0.1455	0.9084
Affine AES S-box	7.5710	9.6320	0.1341	0.0182	0.4669
Residue prime S_8 S-box	7.5647	9.5568	0.1363	0.0184	0.4625

Table 17. Comparison of P Contrast, Correlation, Energy, Homogeneity and entropy of plain image and cipher image of Lena (512x512, png) of affine AES S-box and residue prime S_8S-box with different S-boxes

Images	**Entropy**	**Contrast**	**Correlation**	**Energy**	**Homogeneity**
Plain image	7.4451	0.2100	0.9444	0.1455	0.9084
Affine AES S-box	7.5710	9.6320	0.1341	0.0182	0.4669
residue prime S_8 S-box	7.5647	9.5568	0.1363	0.0184	0.4625
AES S-box	7.2531	7.5509	0.0554	0.0202	0.4662
APA S-box	7.2531	8.1195	0.1473	0.0183	0.4676

Residue prime S-box	7.2531	7.6236	0.0855	0.0202	0.4640
S_8AES S-box	7.2357	7.4852	0.1235	0.0208	0.4707
Gray S-box	7.2531	7.5283	0.0586	0.0203	0.4623
Xyi S-box	7.2531	8.3108	0.0417	0.0196	0.4533
Skipjack S-box	7.2531	7.7058	0.1025	0.0193	0.4689

Figure 6. Lena image

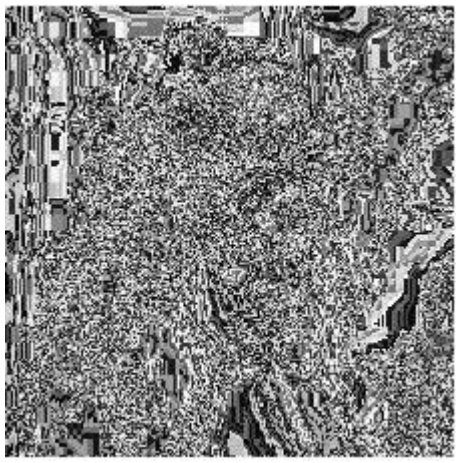


Figure 7. Lena encrypted image by affine AES S-box

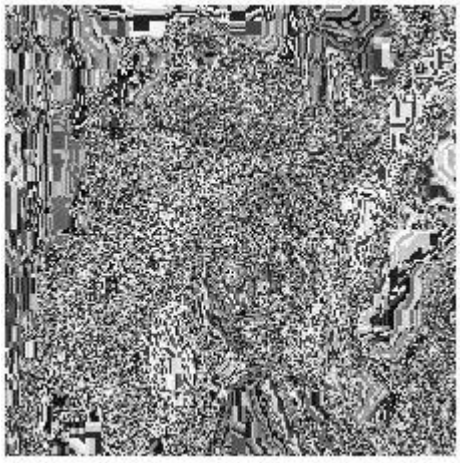


Figure 8. Lena encrypted image by residue prime S_8S-box

CONCLUSION

In this proposed work we have developed two different techniques to generate the new S-boxes and then discussed their different properties like nonlinearity, BIC, DAP, and LAP etc. We compare the strength and properties with other well known S-boxes and the comparison is given in tables. The nonlinearity of the S_8 residue prime S-box do not change whereas in the case of affine AES S-boxes are decreased. In the second technique we can generate finite many S-boxes with different nonlinearity. In this technique, we can get different 256 S-boxes by changing the fixed byte with different nonlinearity whereas by the action of symmetric group S_8 we get 40320 S-boxes with same nonlinearity. Although for the nonlinearity point of view it has deficiency but an improvement in the strength for image encryption as shown in statistical analysis. There are still lot of works for analysis point of view of these newly constructed S-boxes and further we can apply this newly develop technique on different S-boxes to construct new S-boxes.

REFERENCES

Altaleb, A., Saeed, M. S., Hussain, I., & Aslam, M. (2017). An algorithm for the construction of substitution box for block ciphers based on projective general linear group. *AIP Advances*, *7*(3), 035116. https://doi.org/10.1063/1.4978264

Beth, T., & Ding, C. (1994). On Almost Perfect Nonlinear Permutations. In T. Helleseth (Ed.), *Advances in Cryptology—EUROCRYPT '93* (Vol. 765, pp. 65–76). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-48285-7_7

Cui, L., & Cao, Y. (2007). A new S-box structure named Affine-Power-Affine. *International Journal of Innovative Computing, Information and Control*, 751–759.

Daemen, J., & Rijmen, V. (1999). *Rijndael AES algorihm submission*. AES proposal.

Detombe, J., & Tavares, S. (1992). Constructing large cryptographically strong S-boxes. *Advances in Cryptology, Proc. Of CRYPTO92, LNCS*, 165–181.

Elhosary, A. M., Hamdy, N., & Rohiem, A. E. (2013). State of the ART in Boolean function Cryptographic assessment. *International Journal of Computer Network and Computer Security*, *1*(3), 88–94.

Hussain, I., Shah, T., & Asif, M. (2012). Efficient image encryption algorithm based onS_8 S-box transformation and NCA map. *Elsevier*, *285*, 4887–4890.

Hussain, I., Shah, T., & Mahmood, H. (2010). A new algorithm to construct secure keys for AES. *International Journal of Contemporary Mathematical Sciences, 5*(26), 1263–1270.

Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, V. Y. (2011). Some analysis of S-box based on residue of Prime Number. *Proceeding of the Pakistan Academy of Science, 48*(11), 111–115.

Kazlauskas, K., Smaliukas, R., & Vaicekauskas, G. (2016). A novel method to design S-boxes based on key-dependent permutation schemes and its quality analysis. *IJACSA, 7*(4).

Matsui, M. (1994). Linear cryptanalysis method for DES cipher. *EUPOCRYPT93, LNCS, 765*, 386–397.

Medeleanu, F., Racucia, C., & Rogobete, M. (2015). Considerations about the possibilities to improve AES S-box cryptographic properties by Multiplication. *Proceedings of the Romanian Academy, 16*, 339–344.

Meletious, G. C., Triantafyllou, D. S., & Vrahatis, M. N. (2015). Handling problems in cryptography with matrix factorization. *Journal of Applied Mathematics and Bioinformatics, 5*(3), 37–48.

Mhajloska, H., & Gligoroski, D. (2011). A new approach into constructing S-boxes for lightweight block ciphers. *CIIT*.

Rosenthal, J. (2003). A polynomial description of Rijndael Advanced Encryption Standard. *Journal of Algebra and Its Applications, 2*(11), 223–236.

Siddiqui, N. S., Afsar, U., Shah, T., & Qureshi, A. (2016). A novel construction of S_16 AES S- boxes. *International Journal of Computer Science and Information Security, 14*(8).