بسم الله الرحمن الرحيم

In the name Of Allah, the most beneficent, the eternally merciful

Construction of S-boxes over Finite Commutative Rings

By

Wahid Ullah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2016

Construction of S-boxes over Finite Commutative Rings

By

Wahid Ullah

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2016

Construction of S-boxes over Finite Commutative Rings

By

Wahid Ullah

A thesis submitted in the partial fulfillment of the requirement for the degree of

MASTER OF PHILOSOPHY

in

Mathematics

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2016

Dedicated to

My Beloved

Parents

(Late)

Acknowledgement

All praises to Almighty Allah, the most Merciful and the more Beneficent, who created this universe and gave us the idea to discover it. First of all I am highly grateful to Allah Almighty who helped and blessed me more than I deserve.

I deem it a great honor to express my deepest sense of gratitude to my honorable supervisor **Prof Dr. Tariq Shah** for his kind and able guidance, valuable comments and encouraging altitude throughout my research work.

Special thanks to **Dr. Majid Khan (**Assistant Prof at FAST**)** for his helps in this work.

I would like to express my appreciation to the faculty members and the administration of Mathematics department, Quaid-i-Azam University, Islamabad.

This acknowledgment would be incomplete unless I offer my humble veneration to my family especially to my brothers Rehman Ullah, Shahid Ullah and Sisters for their endless love, care and supporting spiritually throughout my life and academic career.

Sincere thanks to all my friends and class mate's especially Abid Ullah Khan, Arif Ullah Khan, Shahid Niaz, Fahim Nawaz, Tanveer ul Haq, Asad Shah, Jawad Ali, Akhter Abbas, Muhammad Asif, Yasir Naseer and Irfan Ullah for their necessary cooperation in the accomplishment of my dissertation

Last but not the least, I would like to thank to one of my best teacher and friend **Muhammad Zahid Khan** (Lecturer in GDC#2, Bannu), who have been a source of encouragement and motivation to complete the degree of Philosophy.

Wahid Ullah

August 2016

Preface

Cryptography is used for protection and transmitting information in such a way that only specified persons can read and process on it. The basic cryptographic techniques were used for thousands of years in different areas. In history, many governments or organized groups mostly used cryptography to conceal secret messages from enemies. About 100 BC Julius Caesar made use of certain encryptions so that he may sent secret messages to his army. This type of encryption is known as Caesar cipher, which is a type of substitution cipher (A cipher is an encryption or decryption algorithm and substitution means that each character of a message is replaced by another character to form the message unreadable).

Even though over the last 40 years, Modern cryptography is considered as a mature branch of science but it is still relatively new field of study compared to other subjects and every new day brings so many developments. But now a days, millions of secure and encoded transmissions occur online every day. Cryptographic standards are used to protect data, banking data, images, videos, health information and much more. In all these, the online security threats evolve so quickly, so there is a need of network security, which is the study of methods for protecting data in communication systems and computers from unauthorized authorities. Network security or data security progressed rapidly since 1975. Modern cryptography and Network security techniques are mostly based on mathematical theory and computer science practices.

For few years, finite Galois rings have great importance in cryptography and coding theory. In 1979, Priti Shankar established a relationship between BCH- codes over Galois ring $GR(p^k, m)$ and Galois field $GF(p^m)$ through a p-reduction map. In the construction of these BCH-codes, the maximal cyclic subgroup G_{p^m-1} of group of units of Galois ring $GR(p^k, m)$ plays a pivotal role. The maximal cyclic subgroup G_{p^m-1} is isomorphic to Galois group $GF(p^k)^*$ and this provides a way to use it in cryptography. The Galois rings were firstly used in cryptography by Shah et al.

In cryptography, the substitution box (S-box) is the vital component of almost all symmetric cryptosystem. The process of encryption creates confusion and diffusion in data and the S-box plays a key role to make confusion in data because it is the only non-linear and invertible part in the encryption process. The strength of encryption technique depends on the ability of S-box in twisting the data hence, the process of finding new and powerful S-boxes are of great importance in the field of cryptography. Firstly, S-boxes are constructed only by using Galois fields. But Shah et al. gives method of construction of S-boxes by using elements of Galois rings $GR(4,2)$ and $GR(4,4)$. Here Shah et al. used the maximal cyclic subgroup of the group of units of Galois ring $GR(4,4)$, which has 16 elements and so that 4×4 S-box is formed. The maximal cyclic subgroup of group of units of commutative chain ring is also used to construct healthier S-box.

The purpose of the research is to develop a good understanding of some basic concepts of cryptography but mainly focused on the construction of S-boxes on local rings $\mathbb{Z}_{p^k}$ and on maximal cyclic subgroup G_s of Galois rings. The newly constructed S-boxes are then analyzed by some algebraic analyses to determine the strength of the proposed S-boxes and by statistical analyses of their application in image encryption algorithms.

The details of the dissertation are here under:

- The first chapter consists of three section. In the first section, we discussed some basic algebraic concepts, which are necessary to understand cryptography. In the second section, we discussed some basic components of cryptography and lastly we discussed some examples of classical and modern cryptography.
- In the second chapter, the concept of S-box is discussed. In addition, the construction techniques of S-box on maximal cyclic subgroup of group of Galois ring $GR(4,4)$.
- In the third chapter, a novel technique to construct S-boxes on maximal cyclic subgroup of order 256 of group of units of Galois ring $GR(8,8)$ is discussed. Some algebraic analysis to determine the strength of these S-boxes are also given in this chapter. The statistical analysis of the plain image and encrypted image are also given in this chapter. The application of these S-boxes in image encryption is also discussed.
- In the fourth chapter, the construction method of S-box over finite local ring $\mathbb{Z}_{2^9}$ is given. Also this S-box is analyzed by algebraic and statistical analysis.
- The last chapter consists the conclusion of these works.

Contents

Chapter 1

Algebraic Preliminaries

This chapter serves as a pillar in the base of modern cryptography. Before we begin our discussion, we review some basic concepts, which are required to understand the discussion in the upcoming chapters [8]. This chapter consists of three section. In the first section, we discussed some basic algebraic concepts that are essential to understand cryptography. In the second section, we discussed some basic components of cryptography and lastly we discussed some example of classical and modern cryptography.

1.1.1. Binary Operation

Let M be a non-void set, then the function $* : M \times M \to M$ is said to be a binary operation on M.

1.1.2. Groupoid

Let M be a non-void set and $*\colon M \times M \to M$ is a binary operation defined on M then $(M,*)$ is said to be a Groupoid, i.e. if $\forall\ x, y \in M,\ *(x, y) = x * y \in M$.

1.1.3. Semigroup

Let M be a non-void set and $*$ be a binary operation, then $(M,*)$ is said to be a semigroup if the following axioms holds:

(i) For every pair $(m_1, m_2) \in M \times M,\ *(m_1, m_2) \in M$.

(ii) Associative law holds in M with respect to the binary operation $*$. i.e.

$$*(m_1,*(m_1, m_2) = *(*(m_1, m_2), m_3)\ for\ all\ m_1, m_2, m_3, \in M.$$

1.1.4. Monoid

A non-void set M together with binary operation $*$ is said to be Monoid, if $(M,*)$ is a semigroup and there is an identity element e in M such that

$$for\ all\ m\ \in M,\ *(e, m) = e = *(m, e).$$

1.1.5. Group

A monoid $(M,*)$ is said to be form a group if for every element $m \in M$, there exists a unique element n in M such that $*\,(m,n) = e = *\,(n,m)$ where e is identity element in M.

Example 1: The sets $(\mathbb{Z},+),(Q,+),(R,+),(R\backslash\{0\},.)$ and $(Q\backslash\{0\},.)$ are all groups. The set of integers $\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$ and the operation is addition modulo n form a group with the identity element 0. Every element x has an inverse$-x$ such that $x + (= x) \equiv 0\ mod(n)$. Note that this set does not form a group with the operation of multiplication modulo n because most elements x do not have an inverse y such that $x \odot y \equiv 1\ mod(n)$.

Remark 1: The sets $N\ and\ \mathbb{Z}$ w.r.t the binary operation **.** (i.e.w.r.t usual multiplication) are not groups but these sets are only monoid. Similarly the set $(N,+)$ is only semigroup, $(\mathbb{Z},-)$ is only groupoid. Moreover, this is due to the fact that inverse of each elements w.r.t the usual multiplication in $N\ and\ \mathbb{Z}$ does not exists i.e. for instance inverse of 2 is $\frac{1}{2}$, which doesn't belong to $N\ and\ \mathbb{Z}$. Similarly, identity w.r.t binary operation $+$ is 0 which doesn't belong to N and so that's why we say that $(N,+)$ is only semigroup.

Abelian group

A group $(M,\circ)$ is said to be abelian if commutative law holds is M with respect to the binary operation $\circ$ i.e. for every $m_1, m_2 \in M$, $\circ\,(m_1, m_2) = \circ\,(m_2, m_1)$

Example 2: The sets $(Z,+),(R,+)$ and $(R\backslash\{0\},.)$ are all abelian groups. Also the set M consisting of all $n \times n$ matrices is an Abelian group w.r.t binary operation of + (matrix addition), but the subset of the above set M consisting of non-singular (invertible) matrices is non-abelian group with respect to binary operation of matrix multiplication.

Remark 2: Abelian group is also called commutative group.

Subgroup

A non-void set H of a group M is said to be subgroup of a group M if H itself form a group with respect to the same binary operation defined on M.

Example 3: Consider the binary operation of usual addition $+$, the set $\mathbb{E}$ of even integers is subgroup of the group $\mathbb{Z}$ of integers.

1.1.6. Homomorphism

Let $(M,\circ)$ and $(H,\ *)$ be any two groups. A function $f: M \to H$ is said to be a group homomorphism if

$$\forall\, m_1, m_2 \in M, \qquad f(m_1 \circ m_2) = f(m_1) * f(m_2)$$

Endomorphism is a group homomorphism $f: M \to H$ if $M = H$, i.e. a homomorphism from a group to itself is called endomorphism.

Epimorphism is a group homomorphism $f: M \to H$ which is onto (surjective), i.e. if $img(f) = H$.

Monomorphism is a group homomorphism $f: M \to H$, which is 1-1 (injective), i.e. if distinct elements have distinct images $f(m_1) \neq f(m_2) \Longrightarrow m_1 \neq m_2\ for\ m_1, m_2 \in M$.

Isomorphism is a group homomorphism $f: M \to H$, which are both 1-1, and onto, i.e. a bijective group homomorphism is called a group isomorphism

Remark: Two groups $M\ and\ H$ are said to be isomorphic if there is an isomorphism between $M\ and\ H$.

1.1.7. Coset

Let $(M,\circ)$ be a group and H be the subgroup of M, then for any $m \in M$, the set

$m \circ H = \{m \circ h : h \in H\}$ is said to be left coset of H in M. Similarly, the right coset is defined to be the set $H \circ m = \{h \circ m\ ; h \in H\}$.

Example 4: Let $M = (\mathbb{Z}_8, +)$ and $H = \{0,2,4,6\}$, then H is a subgroup of M and so the left coset of H in M are given by:

$$1 + H = 3 + H = 5 + H = 7 + H = \{1,3,5,7\},$$

$$2 + H = 4 + H = 6 + H = 8 + H = \{0,2,4,6\}$$

Normal subgroup

A subgroup H of a group M is said to be normal subgroup if $mhm^{-1} \in H, \forall m \in M\ and\ h \in H$. In other word, H is said to be normal if $\forall\ m \in M, mH = Hm$, i.e. if left and right cosets coincide.

1.1.8. Quotient group

Let $(M, +)$ be a group with normal subgroup H. Then the quotient group of $M\ modulo\ H$ is defined to be the group of all cosets of $H\ in\ M$ and is denoted as:

$$M/_H = \{m + H : m \in M\}$$

The binary operation in $M/_H$ is defined as: $(a + H) + (b + H) = (a + b) + H, \forall\, a, b \in M$

Example 5: Consider the group $M = (\mathbb{Z}, +)$. Then for any $n \in N, H = \{0 \pm n, \pm 2n, ...\}$ is a normal subgroup of M and thus the set $\mathbb{Z}/_{n\mathbb{Z}} = \{x + n\mathbb{Z} : x \in \mathbb{Z}\}$ is the quotient group having n elements.

Finite group

A group G is said to be finite if it has a finite number of elements. The number of elements in a group G is denoted by $|G|$ and is called order of G. We some time say that a group is finite if $|G| < \infty$.

Remark 3: In a finite group G, for $a \in G$ and for any $n \in N, a^n \in G$, due to closure property in G.

Cyclic group

A group M is said to be cyclic if there is an element $a \in M$ such that every element of M can be written as some integer power of a, i.e if $x \in M, then\ \exists\ k \in N$ such that $x = a^k$, where N is the set of natural numbers. The element a is then said to be generator of the group M and we write as $M = \langle a \rangle$.

Example 6: If $M = \{1, \omega, \omega^2 :\ \omega^3 = 1\}$ then $(M, .)$ is a cyclic group generated by ω. Also $(\mathbb{Z}_m, +)$ is a cyclic group generated by $1\ and - 1$

Remark: It is to be noted that a cyclic group have more than one generator and when binary operation is addition, then the term integer power of a reduces to integral multiple of a.

Group Action

Let us consider that $(M,\circ)$ be a group and H be a non-empty set. We say that M acts on a set H (from left) if the mapping $* : M \times H \to H$ satisfied the followings:

(i) $*\ (e, h) = e\ * h = h :\ \forall h \in H\ where\ e \in M$ is an identity.

(ii) $* \left(m_1, * \,(m_2, h)\right) = * \,(m_1 \circ m_2, h)\ , \forall\, m_1, m_2 \in M\ and\ h\ \in H.$

1.1.9. Ring

A non-empty set R together with two binary operations, $+ : R \times R \to R\ and\ \circ : R \times R \to R$ is said to be ring if

(1) $(R, +)$ Form an abelian group.

(2) $(R,\circ)$ Is a semigroup.

(3) Left and Right distributive laws of $\circ$ over $+$ holds in R that is, for all $r_1, r_2, r_3 \in R$

$$r_1 \circ (r_2 + r_3) = (r_1 \circ r_2) + (r_1 \circ r_3) and\ (r_1 + r_2) \circ r_3 = (r_1 \circ r_2) + (r_2 \circ r_3)$$

Commutative Ring

A ring $(R,+,\circ)$ is said to be commutative ring if in R, commutative law holds with respect to " $\circ$ "

Example 7: The sets $(\mathbb{Z},+,.)$, $(\mathbb{R},+,.)$and the set of integers modulo n, $(\mathbb{Z}_n,\oplus,\odot)$ are examples of the commutative ring.

Zero Divisor

Let R be a ring. An element $a \neq 0\ in\ (R,+,\circ)$ is said to be a zero divisor if there is an element b in R such that $a \circ b = 0$ implies $b \neq 0$, where "0" is an identity w.r.t $+$ in R.

Example 8: Let $R = \mathbb{Z}_8$, then $2.4 = 8 = 0\ mod(8)$, while $2 \neq 0\ and\ 4 \neq 0$. So 2 and 4 are Zero divisor in $\mathbb{Z}_8$.

Ring with identity

A ring $(R,+,\circ)$ is said to be ring with identity if identity element e w.r.t $\circ$ exists in R i.e. for all $r \in R$, $r \circ e = e = e \circ r$.

Unit element

An element a in R is said to be unit element in R if there is an element b in R such that $a \circ b = e$ where e is identity element w.r.t $\circ$ in R.

1.1.10. Ideal of a Ring

Let $(R,+,.)$ be a ring. A non-empty subset I of R is said to be ideal of a ring R, if I is an additive subgroup of R and for every $a \in R, aI \subseteq I\ and\ Ia \subseteq I$ i.e. for every $x, y \in I\ and\ a \in R, x - y \in I\ and\ ax, xa \in I$.

Prime ideal

Let $I \neq R$ be an ideal of a commutative ring R. Then I is said to be prime ideal if $xy \in I$ implies that either $x \in I$ or $y \in I$ for every $x, y \in R$.

Maximal ideal

An ideal M of a ring R is said to be Maximal ideal if $M \neq R$ and there is no other proper ideal P of R which properly contains M.

Principle Ideal

An ideal I of a ring R is called a principal ideal if there exists an element $a \in I$ such that $I = < a >$ where $< a > = \{ ar : r \in R \}$. The element a is called the generator of I and I is said to be generated by a.

Remark: A ring R is called principal ideal ring if every ideal of R is principal.

Local Ring

A ring $(R, +, \circ)$ is said to be local ring if $(R \backslash R^*, +)$ form an abelian group, where R^* is the set of all unit elements of R. A local ring have only one maximal ideal.

Example 9: The integers modulo rings $\mathbb{Z}_{p^k}$ where p is prime and k is any positive integer is an example of a local ring, i.e. $\mathbb{Z}_8,\ \mathbb{Z}_9,\ \mathbb{Z}_{16}$ are all local rings.

Quotient ring

Let $(R, +, \circ)$ be a ring and I be an ideal of R then the quotient set $R/_I = \{a + I : a \in R\}$ form a ring w.r.t the binary operations, defined as:

$$(a + I) + (b + I) = (a + b) + I \ and\ (a + I).(b + I) = (a.b) + I$$

Polynomial Ring

Let R be a ring, then the set of all polynomials of degree n whose coefficients are element of R is denoted by $R[x]$ and form a ring with binary operations defined as: If $p = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ and $q = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n$ then $p + q = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$ and $p \cdot q = d_0x^n + d_1x^{n-1} + \cdots + d_{n-1}x + d_n$ where$c_i = a_i + b_i$ and $d_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_1$ and the ring $(R[x], +, .)$ is so called polynomial ring.

Reducible Polynomial

A polynomial p in $R[x]$ is said to be reducible if it can be written as a product of two non-invertible polynomials in $R[x]$ i.e. if there exists non-invertible polynomials q and r in the ring $R[x]$ such that $p = q\ .r$.

For example if $f(x)$ is from the polynomial ring of integers $Z[x]$ such that $p = x^2 - 1$ then there is $q = x - 1$ and $r = x + 1$ in $Z[x]$ such that $p = q.r$

Irreducible Polynomial

An element $p(x)$ in a polynomial ring $R[x]$ is said to be irreducible polynomial if $p(x)$ is non-invertible and cannot be written as a product of two non-invertible elements in $R[x]$.

Monic Polynomial

A polynomial $p(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n$ is said to be monic if $b_0 = 1$.

Primitive Polynomial

A polynomial $p(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n$ is said to be primitive polynomial if the greatest common divisor of all the coefficients of $p(x)$ is 1.

Remark: Every monic polynomial $p(x)$ is primitive.

1.1.11. Field

A field $\mathbb{F}$ is the set of points together with two binary operations $+ \, and \circ$ which satisfies the following axioms:

- Elements of $\mathbb{F}$ form an abelian group with respect to operation $+$ with neutral element 0.
- Elements of $\mathbb{F}$ form an abelian group with respect to operation $\circ$ with neutral element 1
- When these two operations are mixed, the distributive law holds, i.e. $\forall\ x, y, z \in \mathbb{F}$,

$$x \circ (y + z) = (x \circ y) + (x \circ z)$$

Example 10: The set of real numbers $\mathbb{R}$ together with binary operations of usual addition and multiplication is a field with additive neutral element 0 and multiplicative neutral element 1. The set of integers modulo n is a field if n is a prime, i.e. $(\mathbb{Z}_n, \oplus, \odot)$ is a field if n is a prime number.

Remark: If R is a field. Then ideal generated by an irreducible polynomial $p(x)$ is maximal ideal in the ring $R[x]$. If $(R, +, \circ)$ is a field, then the set $R/\{0\}$ is a cyclic group with binary operation $\circ$, where 0 is the identity in R with respect to $+$.

Galois Field

The field whose order is a prime or power of some prime is known as Galois field. For every prime number p and an integer n, there exists exactly one (up to an isomorphism) Galois field $GF(p^n)$ of order p^n. $GF(p) = \{0,1,2, \dots, p-1\}$ is the field of residue classes modulo p which has p elements. For any prime p and $k > 1$, the set of equivalence classes of polynomials whose coefficients from $GF(p)$ is a field of order p^k, isomorphic to $GF(p^k)$ and k is the degree of some irreducible polynomial over $GF(p)$' i.e. if $g(x)$ is the irreducible polynomial of degree k, then

$$\frac{GF(p)[x]}{\langle g(x)\rangle} = GF(p^k) = \{a_1x^{k-1} + a_2x^{k-2} + \cdots + a_{k-1}x + a_k : a_i \in GF(p)$$

Example 11: If $p = 2$, and the irreducible polynomial of degree 2 is $g(x) = x^2 + x + 1$. Then elements of $GF(2^2)$ are equivalence classes which are obtained by constructing the quotient ring $\mathbb{Z}_2[x]/\langle g(x)\rangle$. So that the elements of $GF(2^2)$ are all polynomials whose coefficients belong to $\mathbb{Z}_2$ and degree less than 2, i.e. $GF(2^2) = \{0,1, x, x + 1\}$

Galois Ring:

If $f(x)$ is irreducible over $\mathbb{Z}_q[x]$ where q is power of some prime p, then the quotient ring $\frac{\mathbb{Z}_q[x]}{\langle f(x)\rangle} = R$ is isomorphic to the Galois ring $GR(q,\ m)$ of order q^m where m is the degree of the polynomial $f(x)$.

Basic irreducible polynomial

Let R be a local commutative ring with unity and M be its only maximal ideal. An irreducible polynomial $g(x)$ in $R[x]$ over R is said to be a basic irreducible polynomial if $\overline{g(x)}$ is irreducible over the corresponding residue field $\mathbb{F} = {}^{R}/_{M}$.

Example 12: The polynomial $g(x) = x^4 + 3x + 3$ is basic irreducible over $\mathbb{Z}_4$, because it is irreducible over $\mathbb{Z}_4$ and $\overline{g(x)} = x^4 + x + 1$ is irreducible over the corresponding residue field $\mathbb{Z}_2$.

1.1.12. Boolean Algebras

[17] Let B be a nonempty set and $\wedge, \vee$ are binary operations on B, $\sim$ is a unary operation on B. Then B is called Boolean algebra if the following condition satisfied:

(B1) $a \vee b = b \vee a\ and\ a \wedge b = b \wedge a\ for\ all\ a, b \in B.$

(B2) $a\vee(b\wedge c) = (a\vee b)\wedge (a\vee c) and\ a\wedge(b\vee c) = (a\wedge b)\vee(a\wedge c) for\ all\ a, b, c \in B$

(B3) There exist elements $0,1 \in B\ with\ 0 \neq 1$ such that $0\vee a = a\ and\ 1\wedge a = a\ for\ all\ a \in B$

(B4) $a\wedge(\sim a) = 0\ and\ a\vee(\sim a) = 1\ for\ all\ a \in B.$

The binary operations $\wedge$ and $\vee$ are known as AND and OR respectively and the unary operation $\sim$ is called negation.

Remark: $a \vee b$ and $a \wedge b$ are also written as $a + b$ and $a.b$ respectively.

Example 13: Let X be a non-empty set. Then the power set of X is the set of all subsets of X denoted by $P(X)$ is Boolean algebra with $0 = \varphi$ and $1 = X$. The binary operations are $\cup$ and $\cap$ and the unary operation is complement of set $i.e. A^c = X - A$.

Boolean Function

Let B be a Boolean algebra, then the function $f: B^m \to B$ is said to be Boolean function, where m is any positive integer. But the multi-valued Boolean functions from cryptographic point of view is a function from vector space ${F_2}^k$ of binary vector of length k to vector space ${F_2}^m$, where k and m are any positive integers and $F_2 = \{0,1\}$ is a finite field. These functions becomes single valued when $m = 1$.

1.1.13. Some Logic Operations

- **AND Operation**

Let $B = \{0,1\}$, then AND operation on B gets two inputs $s, t \in B$ and their output denoted by $s \wedge t$ and will be equal to 1 whenever both inputs are 1, otherwise equal to 0. The truth table of AND operation is given as follows:

s	t	$s \wedge t$
1	1	1
1	0	1
0	1	1
0	0	0

- **OR Operation**

The OR operation on B also gets two inputs $s, t \in B$ and their output denoted by $s \vee t$ and equal to 0 whenever both inputs are 0 otherwise equal to 1. The truth table of OR operation is as follows:

s	t	$s \vee t$
1	1	1
1	0	1
0	1	1
0	0	0

- **XOR Operation**

The XOR operation on B also gets two inputs $s, t \in B$ and their output denoted by $s \oplus t$ and equal to 0 whenever both inputs are same otherwise equal to 1. The truth table of XOR operation is given as follows:

s	t	$s \oplus t$
1	1	0
1	0	1
0	1	1
0	0	0

Remark: In XOR operation, the input may be more than two and their output will be 1 when the number of 1's is odd and will be 0 when the number of 1 is even.

1.2. Basic Terminologies of Cryptography

[17, 18, 24]In this section, some basic notions of cryptography are discussed.

Plain Text

The readable form of a data or message is called Plain text. It may be English alphabets, characters, etc.

Cipher Text

The text or message, which is transformed by some algorithm, is called Cipher text. It may be English alphabet, characters etc.

Encryption algorithm

The process of conversion of plain text to cipher text along with secret key is called Encryption algorithm. The encryption algorithm shall be decided before the interaction between the sender and receiver. The key is kept secret, even an attacker may know the algorithm.

Decryption algorithm

The reverse process of encryption algorithm is called decryption algorithm, i.e. in decryption algorithm, we recover the plain text from cipher text by using secret decryption key.

Interceptor

The person or party who try to decrypt the plaintext other than the sender and receiver is called an interceptor or an attacker.

Plaintext Alphabet

Plaintext alphabet is the set of letters or characters, which are used in writing the plaintext. These plaintext alphabets are generally consist of the letters of English alphabet, or it may possibly include some other characters, for example punctuation marks, numerals etc.

Cipher text Alphabet

Cipher text alphabet is the set of letters or characters, which are used for the cipher text. The plaintext alphabet and cipher text alphabet may be the same or might be different. For example plaintext alphabet may be consist of capital letters $\{A, B, C, \dots, Z\}$ but the cipher alphabet might be the set of numbers $\{0,1,2, \dots, 25\}$.

Key Size

Key size is the size of the key which is using in encryption and decryption process. Obviously, the key size depends on the algorithm uses in encryption and decryption process. For instance, Advanced Encryption Standard (AES) has key sizes 128, 192 and 256 bits and Data Encryption Standard (DES) has its key size 64 bits.

Cryptanalysis

In cryptanalysis, the interceptor try to find out the algorithm used in the encryption process and with the help of algorithm the interceptor decrypt the message.

Brute force attack

It is also known as exhaustive key search. In this method, the interceptor try to find the secret key by checking all possible keys in key space.

Classification of Cryptography

Cryptography is divided into two main types with respect to the key operation used,

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

1.2.1. Symmetric Key Cryptosystem

The cryptosystems in which the key used in the encryption and decryption algorithm are same are known as symmetric key cryptosystem. In this type of cryptography, the key is kept secret between the receiver and the sender of a message. This type of cryptosystem are also known as single key or private key cryptosystems. The main symmetric key cryptosystems are DES, Triple DES, AES, RC4, Two fish etc.

The symmetric key cryptography is further divided into two main types,

- Stream Cipher
- Block Cipher

Stream Cipher

A stream cipher is a cipher that encrypt a digital data stream one bit at a time. Examples of classical stream ciphers are the auto keyed Vigenere cipher and in modern cryptography RC4, Fish and ChaCha are examples of stream cipher. If the cryptographic keystream is random, then this cipher is unbreakable by any means other than finding the keystream. However, the keystream must be provided to both sender and receiver in advance via some independent and secure channel. Stream cipher are simple and comparatively faster in programming. This introduces impossible logistical problems if the intended data traffic is very large. For practical reasons, the bit-stream generator must be implemented as an algorithmic procedure, so that the cryptographic bit stream can be produced by both sender and receiver. In this approach, the bit-stream generator is a key-controlled algorithm and must produce a bit stream that is cryptographically strong. Now, both the users need only to share the generating key, and each can produce the keystream.

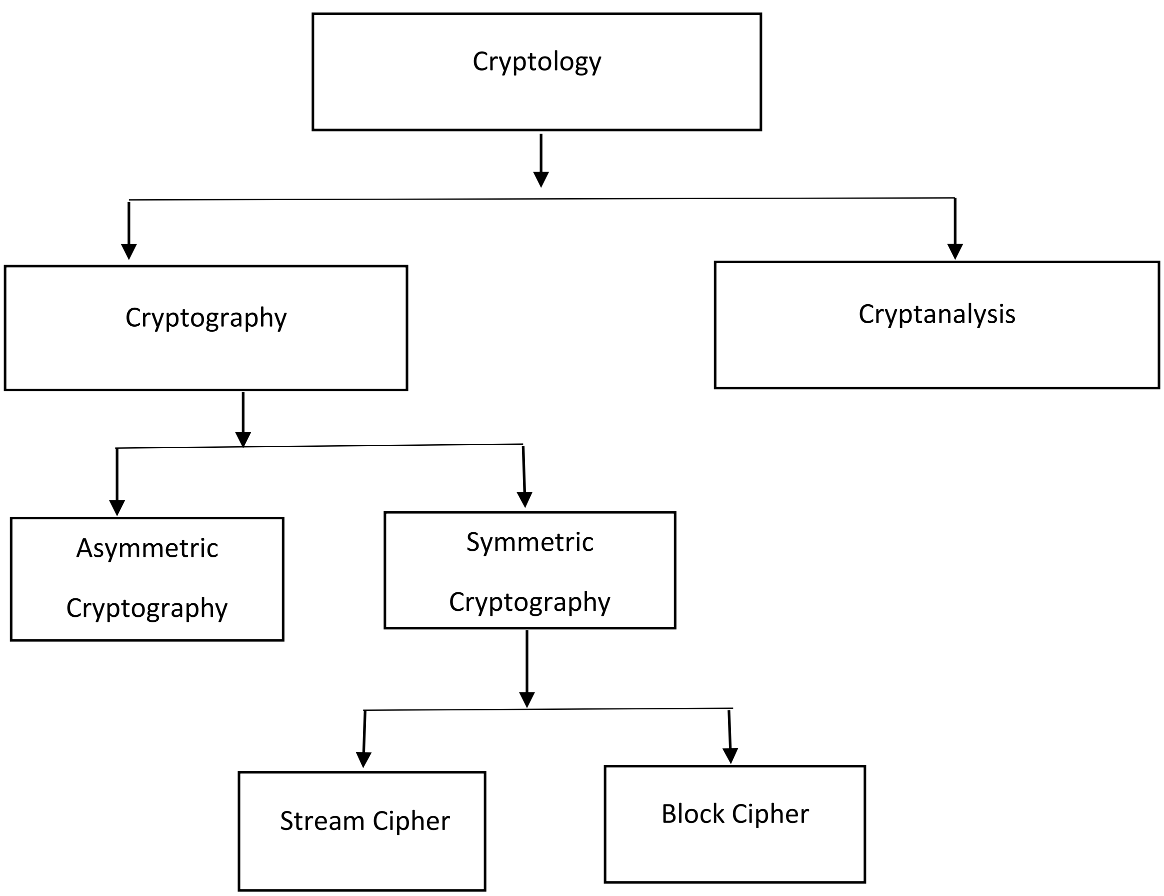
Block Cipher

A block cipher is a cipher that process a block of plaintext as a whole and used to produce a block of cipher text of same length. Typically, a block size of 64 or 128 bits is used. Block cipher are comparatively slower and complex in their program. In general, they seem applicable to a broader range of applications than stream ciphers. The most commonly used Block ciphers are DES, Triple DES, and AES.

1.2.2. Asymmetric Key Cryptosystem

Asymmetric key cryptosystem also known as public key cryptosystem is a form of cryptosystem in which encryption and decryption are done by using different keys, one key is made public, so that anyone who interest in it can have access to it and the other key is kept secret, so that only authorized person can have access to it. Asymmetric key cryptosystem can be used for confidentiality, authentication, or both. The most widely used public-key cryptosystem is RSA.

Figure 1.1.Classification of Cryptology



1.3. Some Classical and Modern Ciphers

1.3.1. Classic Ciphers

Caesar Cipher

[17, 18, 24] The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher replaced each letter of the alphabet with the letter standing three places further down the alphabet. For example,

Plain text: meet us after the juice party

Cipher text: PHHW XV DIWHU WKH MXLFH SDUWB

Note that the alphabet is enfolded around, so that the alphabet X is replaced by A.

We can substitute each characters by shifting three places as follows:

Plain characters: 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

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

Now let us assign a numerical value to each letter, then the Caesar algorithm is expressed as follows:

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

If C is cipher value and p is plain text value, then the enciphering algorithm is described as:

$$C = E(p,3) = (p+3)mod26$$

A shift may be any value from 1 to 25 so the general Caesar algorithm is of the form:

$$C = E(p,h) = (p+h)mod26$$

The deciphering algorithm is simply defined as:

$$p = D(h,C) = (C-h)mod26$$

Example 14: when $k = 5$ then the term “PARTY” becomes ‘UFWYD”.

Affine Cipher

Affine cipher is the general form of a Caesar cipher in which the bijective function $f: \mathbb{Z}_m \to \mathbb{Z}_m$ is defined as, $f(r) = (ar + b)\ mod\ m\ where\ a, b \in \mathbb{Z}_m\ and\ a$ is invertible in Z_m.

Remark: The reason for a to be invertible is that it make the function f to be invertible. In order to maximize the possible values of a, m is used such that $\mathbb{Z}_m$ is a field.

Example 15: Consider the finite field $\mathbb{Z}_{29}$ for the plaintext "$PARTY\ TIME$", where the space is represented by 0, and comma, full stop are represented by 27 and 28 respectively. Now define $f: \mathbb{Z}_{29} \to \mathbb{Z}_{29}\ by\ f(x) = (5x + 12)mod\ 29$

$Plaintext$	P	A	R	T	Y		T	I	M	E
x	16	1	18	20	25	0	20	9	13	5
$5x + 12$	92	17	102	112	137	12	112	57	77	37
$(5x + 12)mod\ 29$	5	17	15	25	21	12	25	28	19	8
$Ciphertext$	E	Q	O	Y	U	L	Y	.	S	H

So that the ciphertext becomes "$EQOYULY.SH$". The decryption process is similar to by taking only the inverse of f. In this case inverse function of f is defined by $f^{-1}(x) = (6x - 12)mod\ 29\ or\ equivalently\ f^{-1}(x) = (6x + 17)mod\ 29$.

Hill Cipher

The generalization of the affine cipher is known as the Hill cipher. Let A denotes the set of plaintext, $\mathbb{Z}_m$ be integers modulo ring and k be a positive integer greater than 1. The mapping $f: A \to \mathbb{Z}_m$ can be extended to $f: A^k \to (\mathbb{Z}_m)^k$ by defining $f(a_1, a_2, \dots, a_k) = (f(a_1), f(a_2), \dots, f(a_k))$.

Now

$$\mathbb{Z}_m^r = \left\{ \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix} : b_i \in \mathbb{Z}_m \right\}$$

And

$$\mathbb{Z}_m^{r\times r} = \left\{ \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1k} \\ b_{21} & b_{22} & \cdots & b_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ b_{k1} & b_{k2} & \dots & b_{kk} \end{bmatrix} : \; b_{ij} \in \mathbb{Z}_m \right\}$$

Now if $U \in \mathbb{Z}_m^{r\times r}$ is such that U is invertible, then $\det(U)$ is invertible in $\mathbb{Z}_m$ and the function $f: \mathbb{Z}_m^r \to \mathbb{Z}_m^r$ defined by $f(B) = UB + V$ where $V \in \mathbb{Z}_m^r$. Now by defining this type of function in encryption system is so called Hill cipher. The decryption algorithm is done by defining the inverse function of f.

Example 16: Consider the plaintext "$SCORPION$" and the Hill cipher $f: \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2 \; defined \; as \; f(X) = (UX + V) \; mod 26$ where $U = \begin{bmatrix} 5 & 3 \\ 5 & 4 \end{bmatrix} \; and \; V = \begin{bmatrix} 9 \\ 7 \end{bmatrix}. Now \det(U) = 5 \; and \; (5,26) = 1, so \; that \; U$ is invertible and the plaintext is encrypted as:

$$\begin{array}{ccccc} Plaintext & SC & OR & PI & ON \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} & \begin{bmatrix} 19 \\ 3 \end{bmatrix} & \begin{bmatrix} 15 \\ 18 \end{bmatrix} & \begin{bmatrix} 16 \\ 9 \end{bmatrix} & \begin{bmatrix} 15 \\ 14 \end{bmatrix} \\ f\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) & \begin{bmatrix} 9 \\ 10 \end{bmatrix} & \begin{bmatrix} 8 \\ 24 \end{bmatrix} & \begin{bmatrix} 12 \\ 19 \end{bmatrix} & \begin{bmatrix} 22 \\ 8 \end{bmatrix} \\ Ciphertext & IJ & HX & LS & VH \end{array}$$

So that the ciphertext becomes "IJHXLSVH". The decryption algorithm is processed by defining $f^{-1}: \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2 \; as \; f^{-1}(X) = \begin{bmatrix} 6 & 15 \\ 25 & 1 \end{bmatrix} X + \begin{bmatrix} 23 \\ 28 \end{bmatrix}$.

1.3.2. Modern Cryptosystems

[4,17,18,24] The most widely used encryption scheme is based on the Data Encryption Standard (DES) was adopted in January, 1977 by the National Bureau of Standards (NBS), now a days which is known for the National Institute of Standards and Technology (NIST). The algorithm itself is referred to as the Data Encryption Algorithm (DEA) and soon it became the most broadly used cryptosystem in the world. For DES, data are encrypted in 64-bits blocks using a key of 56-bits. The algorithm transforms 64-bit input in a series of steps into a 64-bits output. The same steps, with the same key, are used to reverse the encryption. The size of key space in DES is 2^{56} (approximately 7.2×10^{16}). The "DES Cracker" machine was built in 1998 by Electronic Frontier Foundation that could search 88 billion DES keys in one second. So that the DES secret key could be find in 56 hours. In 1999, working in conjunction with a worldwide network of one lac computers, the DES Cracker could search 245 billion keys per second and so succeeded in finding a DES secret key in approximately 22 hours. Thus it was clear that DES was no long secure cryptosystem. So it was essential to adopt a new cryptosystem instead of DES.

By now, the choice of algorithm for many applications has become the Advanced Encryption Standard (AES). For several decades, AES is with its three key lengths of 128, 192 and 256 bit secure against brute-force attacks and there are no analytical attacks with any reasonable chance of success known.

As a result of an open competition, AES was selected in the last phase of the selection process in four other finalist algorithms. The other are the block ciphers, $RC6, Serpent,\ Twofish\ and\ Mars$. All of these algorithm are cryptographically strong and quite fast, particularly in software. They can all be recommended on the basis of today's knowledge. Mars, Serpent and Twofish can be used royalty-free.

Now a day, the Advanced Encryption Standards (AES) is the most broadly used symmetric key cryptosystem. Even though the term "Standard" is only refers to US government applications, the AES block cipher is also compulsory in several industry standards and is used in many commercial systems. Among the commercial standards that include AES are the Internet security standard IPsec, TLS, the secure shell network protocol SSH (Secure Shell), the Wi-Fi encryption standard IEEE 802.11i, the Internet phone Skype and many others security products throughout the world.

In 1999 the US National Institute of Standards and Technology (NIST) specified that DES should only be used for legacy systems and instead of DES, triple DES (3DES) should be used. But there are several problems with $3DES$, even though it resists brute-force attacks. First is that it is not very effective in software implementations. DES is also not particularly well suitable for software and 3DES is more than three times slower than DES. Another drawback is the relatively short block size of 64 bits, which is a weakness in many applications. Finally, if one is troubled about attacks with quantum computers, which might become reality in few decades, key lengths on the order of 256 bits are required. All these thought led NIST to the decision that a new block cipher was needed as a replacement for DES.

In 1997, NIST called for proposals for a new Advanced Encryption Standard (AES). Unlike the DES development, to choose the algorithm for AES was an open process administered by NIST. In three subsequent AES evaluation rounds, NIST and the international scientific community discussed the benefits and drawbacks with presence of cryptanalysis of the submitted ciphers and pointed down the number of potential candidates. In 2001, NIST confirmed the block cipher Rijndael as the new AES and published it as a final standard (FIPS PUB 197). Rijndael was designed by two young Belgian cryptographers. Within the call for proposals, the following requirements for all AES candidate submissions were mandatory:

- Block cipher with 128 bit block size
- Three key lengths must be supported: 128, 192 and 256 bit
- Security comparative to other submitted algorithms
- Effectiveness in software and hardware

The invitation to submit appropriate algorithms and the estimation of the replacement of DES was a public process. A solid chronology of the AES selection process is given as:

NIST announced on January 2, 1997, the need of a new block cipher and on September 12, 1997, the formal call for AES was announced. And fifteen researcher's submitted different algorithms from several countries on August 20, 1998, in which five algorithm were announced in final list. Following are the list of these five final algorithm for AES.

- RC6 by RSA Laboratories.
- Rijndael, by Joan Daemen and Vincent Rijmen.
- Mars by IBM Corporation.
- Twofish by Bruce Schneier, John Kelsey, Doug Whiting, DavidWagner, Chris

Hall and Niels Ferguson

- Serpent, by Ross Anderson, Eli Biham and Lars Knudsen

And lastly on October 2, 2000, Rijndael had selected as the AES by NIST and AES was officially approved as a US standard on November 26, 2001.

For different key length, AES have different number of rounds. For key length of 128 bits, number of rounds is 10, while for key length of 192 and 256 bits, the number of rounds are 12 and 14 respectively. AES consists of different layers. Each layer process on all 128 bits of the data. There are only three different types of layers. Each round, except first, consists of all three layers. Moreover, the last round does not make use of the Mix Column transformation, which helps the encryption and decryption scheme to be symmetric. If we denote the message space by M, the key space by K and the cipher space by C, then we assume that $M = K = C = (\mathbb{Z}_2)^{128}$, i.e. we take the case, where the block size and key size are both 128 bits.

A brief description of the layers is given below:

Key Addition: A 128-bits round key, or subkey, which has been derived from the main key in the key schedule, is XORed to the data.

Byte Substitution (S-Box): With special mathematical properties, each element of the data is nonlinearly transformed to another element by use of lookup tables. This creates confusion to the data.

Diffusion layer: It provides diffusion to over all data and it consists of two sublayers, both of which perform linear operations:

- The Shift Row sublayer permutes the data on a byte level.
- The Mix Column layer is a matrix operation which mixes blocks of four bytes.

To explain these four operations, we write $m \in M$ to denote the current state of data. Byte Substitution layer:

In this layer, each state byte X_i is replaced by another byte Y_i, i.e.

$$S(X_i) = Y_i$$

The S-Box is the only nonlinear part of AES, i.e., it holds that $S(X+Y) \neq S(X) + S(Y)$ for two states $X \; and \; Y$. The S-Box substitution is a bijective mapping, i.e. each of the $2^8 = 256$ possible input elements is one-to-one mapped to one output element. And due to bijective mapping, the inverse S-box can be determined, which is required for decryption. The substitution is performed only on 8-bit string by using a particular permutation $f: (\mathbb{Z}_2)^8 \to (\mathbb{Z}_2)^8$. Now since $m \in M$ consists of 128-bit string, so m can be written as 16 bytes. Let $m = (m_1, m_2, \dots, m_{16}), where \; m_1, m_2, \dots m_{16} \in (\mathbb{Z}_2)^8$, then

$$m = (m_1, m_2, \dots, m_{16}) \to (f(m_1), f(m_2), \dots, f(m_{16}))$$

The permutation $f: (\mathbb{Z}_2)^8 \to (\mathbb{Z}_2)^8$ used in Rijndael algorithm is obtained by identifying each element of $(\mathbb{Z}_2)^8$ with corresponding element of the finite field $\mathbb{F}_{2^8} = \mathbb{F}_{256}$. To obtain a representation of a finite field $\mathbb{F}_{256}$, Rijndael uses the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, so that the field $\mathbb{F}_{256}$ is given by

$$\mathbb{F}_{256} = \{a_7 u^7 + a_6 u^6 + \dots + a_1 u + a_0 : \; where \; a_0, a_1, \dots, a_7 \in \mathbb{Z}_2\}$$

Where u satisfies the relation $u^8 + u^4 + u^3 + u + 1 = 0$. Also we have a 1-1 correspondence between the elements of $(\mathbb{Z}_2)^8 \; and \; \mathbb{F}_{256}$ given by:

$$g(a_7, a_6, \dots, a_1, a_0) = a_7 u^7 + a_6 u^6 + \dots + a_1 u + a_0$$

With this identification of elements of $(\mathbb{Z}_2)^8 \; with \; \mathbb{F}_{256}$, the mapping $f: \mathbb{F}_{256} \to \mathbb{F}_{256}$ is defined to be a composite of two bijective mappings, $h \; and \; \sigma, i.e. f = h \circ \sigma$ where $h: \mathbb{F}_{256} \to \mathbb{F}_{256} \; and \; \sigma: \mathbb{F}_{256} \to \mathbb{F}_{256}$ are defined as

$$h(t) = \begin{cases} 0 & : \quad if\ t = 0 \\ t^{-1} & : \quad if\ t \neq 0 \end{cases}$$

The second mapping is defined in a way that if $t = a_7u^7 + a_6u^6 + \cdots + a_1u + a_0 = \sum_{i=0}^{7} a_iu^i$, $then\ \sigma(t) = \sum_{i=0}^{7} b_iu^i$ where b_i is obtained as follows:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Diffusion layer: For the operations of Row shift and Mix column, we represents element of the message space M by a 4×4 matrix. We write $m = (m_1, m_2, \dots, m_{16})$ as

$$m = \begin{bmatrix} m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \\ m_4 & m_8 & m_{12} & m_{16} \end{bmatrix}$$

This representation of m is used in the Row shift and Mix column operations.

Row shift: In this operation, the row i $(i = 0,1,2,)$ in the matrix m is shifted cycle wise to the left by i places. Thus the top row remains unchanged, the second row is shifted to the left one place, the third row is shifted to the left two places and last row is shifted three places to the left. The process of the operation is given below:

$$m = \begin{bmatrix} m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \\ m_4 & m_8 & m_{12} & m_{16} \end{bmatrix} \rightarrow \begin{bmatrix} m_1 & m_5 & m_9 & m_{13} \\ m_6 & m_{10} & m_{14} & m_2 \\ m_{11} & m_{15} & m_3 & m_7 \\ m_{16} & m_4 & m_8 & m_{12} \end{bmatrix}$$

Mix column: In this operation, the linear transformation is used, which mixes each column of a state matrix m. The matrix of inputs m is multiplied from the left by a fixed invertible matrix. The main diffusion part of AES is he Mix Column operation. The combination of the operations, Row shift and Mix Column makes it possible that after only three rounds every byte of the matrix m depends on all 16 plaintext bytes. The process of this operation is given below:

$$m = \begin{bmatrix} m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \\ m_4 & m_8 & m_{12} & m_{16} \end{bmatrix} \rightarrow \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \\ m_4 & m_8 & m_{12} & m_{16} \end{bmatrix}$$

We discuss now the details of the matrix multiplication which are include in the Mix Colum operations. We recall that each state byte m_1 is an 8-bit value represented by an element from $GF(2^8)$. The addition and multiplication involving the coefficients is done in this Galois field $GF(2^8)$. For the constants used in the fixed matrix, a hexadecimal notation is used, i.e. "01" refers to the element of $GF(2^8)$, i.e. polynomial with the coefficients (00000001), (it is the identity element 1 of the Galois field $GF(2^8)$, "02" refers to the polynomial with the coefficients (00000010), i.e., refer to the polynomial *x in* $GF(2^8)$, and "03" refers to the polynomial with the bit vector (00000011), i.e. the polynomial $x + 1$ in the Galois field $GF(2^8)$. The additions in the matrix multiplication are additions of the elements of $GF(2^8)$, that is simple bitwise $XORs$ of the respective bytes. For the multiplication of the constants, we have to realize multiplications with the constants 01, 02 and 03. These are quite simple, and in fact, the three constants were chosen such that software implementation is easy. Multiplication by 01 is multiplication by the identity and does not involve any other operation. Multiplication by 02 can be applied as a multiplication by "x", which is a left shift by one bit, and a modular reduction with $P(x) = x^8 + x^4 + x^3 + x + 1$. Similarly, multiplication by 03, which represents the polynomial, "$x + 1$" can be performed by a left shift by one bit and addition of the original value followed by a modular reduction with $P(x)$.

Example: We continue with assuming that the input state to the Mix Column layer is $B = (35,35,\ldots,35)$. In this special case, only two multiplications in $GF(2^8)$ have to be done. These are $02 \cdot 35$ *and* $03 \cdot 35$, which can be computed in polynomial notation as:

$$\begin{aligned} 02 \cdot 35 &= x \cdot (x^5 + x + 1) \\ &= x^6 + x^2 + x \\ 03 \cdot 35 &= (x + 1) \cdot (x^5 + x + 1) \\ &= (x^6 + x^2 + x) + (x^5 + x + 1) \\ &= x^6 + x^5 + x^2 + 1. \end{aligned}$$

Since both the value after multiplication have a degree smaller than 8, so no modular reduction with $P(x)$ is necessary. Now by adding $01 \,.\, 35,\ 01 \,.\, 35,\ 02 \,.\, 35$ *and* $03 \,.\, 35$, we get $x^5 + x + 1 = 35$ as output, which yields that output after Mix column operation in this special case is $C = (35,35, \ldots, 35)$.

Chapter 2

Construction of S-box over Galois Ring $GR(4,4)$

2.1. Introduction

There are many algebraic notions, which if incorporated in Computer and Information technologies, can have remarkable impacts. For instance, Galois fields, Galois rings, and maximal cyclic subgroups of groups of units of Galois rings. In modern symmetric key cryptography, the S-boxes are usually constructed over finite Galois fields ($GF(2^n)\ for\ 2 \leq n \leq 8$). For instance, AES S-box [4], Gray S-box [25], APA S-box [3], Residue Prime S-box [14], Skipjack S-box, S_8 AES S-box [15], and Xyi S-box [27]. The strength of cryptographic algorithms is determined on the base of this nonlinear component of the algorithm. Therefore, the construction of cryptographically strong S-box is vital in the design of secure cryptosystems. For safe communication, diverse nature of S-box has been constructed, which is based on algebraic and practical structures. S-boxes constructed on algebraic structure have much more attraction due to their strong cryptographic characteristics [11–13].

The substitution box (S-box) is one of the most vital and indispensable source in the area of cryptography. The process of encryption creates confusion and diffusion in data, and the S-box plays a key role to make confusion in data because it is the only non-linear part in the encryption process. The strength of encryption technique depends on the ability of S-box in twisting the data hence, the process of finding new and powerful S-boxes is of great importance in the field of cryptography.

A $p \times q$ S-box is a mapping $h: \mathbb{Z}_2^p \to \mathbb{Z}_2^q$ from p input bits to q output bits, whereas, there are 2^p and 2^q number of inputs and outputs, respectively. Subsequently, an S-box is just a set of q single output Boolean functions combined in a fixed order. The dimension of an S-box has an effect on the uniqueness of the output and the input, which might affect the properties of the S-box. If there is an S-box with dimension $p \times q$, where $p > q$ such that the number of input bits is greater than output bits, then some entries in the S-box must be repeated, whereas, an $p \times p$ S-box might either contains different entries, where each input is mapped to different output, or repeat several entries of the S-box. The S-boxes which are both injective and surjective are called bijective S-boxes and they are reversible, i.e. the inverse S-box of these S-boxes exists.

The most widespread application of Galois fields, Galois rings, and maximal cyclic subgroups of groups of units of Galois rings can be seen in the coding theory. As an alternative of a cyclic Galois group, for the valued practice and a matchless role, maximal cyclic subgroup of the group of units of a Galois ring catches an abundant consideration in algebraic coding theory. In this covenant, mainly Shankar [24] introduced a construction procedure of a BCH code over a local commutative ring $\mathbb{Z}_{p^k}$ with the use of maximal cyclic subgroup of the group of units of the Galois ring extension of the ring $\mathbb{Z}_{p^k}$. In [24], it is shown that the existence of this maximal cyclic subgroup is based on a modulo p reduction map from the integer modulo ring $\mathbb{Z}_{p^k}$ to its residue field $\mathbb{Z}_p$. Whereas, Shanbhag et al. [23] has given exponential sums and an upper bound for hybrid sum over the Galois rings by the usage of maximal cyclic subgroups of the groups of units of these Galois rings . In continuation, Andrade and Palazzo [1], with the help of maximal cyclic subgroup of a Galois ring, gives a construction technique of BCH codes based on locator vector having components from maximal cyclic group. Galois rings, and maximal cyclic subgroups of groups of units of Galois rings are used firstly by Shah at al [21] in the construction of different S-boxes.

Once the S-box is formed, it is essential to analyze the properties exhibited by them. With the help of the results from algebraic and statistical analysis [14, 19-22], we can determine the encryption strength of this newly generated S-boxes and their ability of creating confusion in the encryption process.
In this chapter, the construction technique of 4×4 S-boxes with the utility of maximal cyclic subgroups of groups of units of the Galois rings $\mathrm{GR}(2^2, 4)$ and $GF(2^2)$ are discussed [21].

2.2. Tools used in Modern Cryptography

Cryptography was considered as an art before 1950, but modern cryptography is a science that needs support from other fields like mathematics, electronics and computer science. The importance of cryptography and its scientific research became an aim for military intelligence after World War *II*. It did not take long when in 1970's the greatest breakthrough of the field was seen (invention of public key ciphers and DES; the first modern symmetric cryptosystem). This was the time when algorithms were developed for computers, by computers. It was realized that good ciphers were developed by combining small tools. Some of these tools were used as ciphers themselves but with the invention of computers, calculations have become much faster than the old days.

2.2.1. Substitution

As the term implies, a substitution can be defined as an operation, which replaced one thing, by the other. In cryptography, it represents a process in which one symbol (or group of symbols) is replaced with another symbol (group of symbols). The example of substitution cipher in classical cryptography is Caesar Shift Chip. Here, each letter of the plaintext is replaced by the latter three places further down in the alphabet.

2.2.2. Transposition

When the places of two things are swapped with each other, they are said to be transposed. There is a condition that is applied to this process for which only the two things involved in the transposition are swapped and the rest remains the same.

2.2.3. Permutation

An arbitrary reordering or swapping of exactly two members of a set is known as permutation. While using the proper sequence of transposition, any permutation can be accomplished.

2.2.4. Confusion and Diffusion

In cryptography, we usually use substitutions and permutations, and combine them to create confusion and diffusion in the data. The confusion and diffusion creates distortions in the data and in the image, making it unreadable.

- The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.
- Diffusion is the process, which spread the influence of a single plaintext bit over many ciphertext bits. A scheme is diffusing if a change in the character of the plaintext (cipher text) produces changes in several characters of the cipher text (plaintext) respectively. In a block cipher, bit changes are propagated by the help of diffusion, from one part of the block to the other parts.

To maintain a maximum level of confusion and diffusion, substitution-permutation ciphers are used. These are the symmetric encryption representing a combination of permutations and substitutions. Some of the most relevant symmetric encryption systems are DES and AES.

2.2.5. Linear Fractional Transformation

The linear fractional transformation (LFT) is a mapping of the form $g(m) = {}^{sm+t}/_{um+v}$ where, $s, t, u, v \in \mathbb{C}$ are such that $sv - ut \neq 0$. In cryptography, LFT were used in the construction of S-boxes on Galois fields [9-14]. The process to obtain the image $g(m)$ of m, is different from the usual LFT. In the construction of S-box, the LFT $g: GF(2^8) \to GF(2^8)$ is used. The process of obtaining image of $m \in GF(2^8)$ is such that we first select $s, t, u, v \in GF(2^8)$ such that $sv - ut \neq 0$. Then we convert the element m, s, t, u, v to decimal representation and simplify $sm + t \ and \ um + v$ and then write it as a power of the generator α of the Galois cyclic group $GF(2^8)^* = GF(2^8) - \{0\}$, i.e. for example if $sm + t = \alpha^k$ and $um + v = \alpha^n$ then $g(m) = {\alpha^k}/{\alpha^n} = \alpha^{k-n} \in GF(2^8)$.

2.3. Maximal Cyclic Subgroups of Group of Units of Galois Rings

Let K^* and R^* be the multiplicative group of units of field K of order p^k and ring R respectively. Then R^* is a multiplicative commutative group and can be written in the direct product of cyclic subgroups. By the following Theorems (1,2), between these cyclic subgroups, there is only one cyclic subgroup of order $\mathrm{p}^\mathrm{k} - 1$.

Theorem 1: The cyclic subgroup of R^* of order $\mathrm{p}^\mathrm{h} - 1$ has one and only one cyclic subgroup of order relatively prime to p.

Theorem 2: suppose $\overline{x}$ generates a cyclic subgroup of order $s = p^k - 1$ in $K^* = K\backslash\{0\}$, then x generates a cyclic subgroup of order $sd \ in \ R^* \ where \ d \geq 1$ and so x^d generates the cyclic subgroup G_s of group of units of $R^*, i.e. G_s = \{\langle x^d \rangle : \ x^{sd} = 1\}$.

This subgroup can be generated by the generator of the corresponding finite field. It is denoted by G_s, where $s = p^h - 1$. Because of the fact that the orders of K^* and G_n are same, i.e., $p^h - 1$ and they both are cyclic. So, G_s is isomorphic to K^*.

With the utility of maximal cyclic subgroups of groups of units of the Galois rings, while, in this case the maximal cyclic subgroup of orders 15 are isomorphic to the cyclic Galois group $GF(2^4)^*$. The association of maximal cyclic subgroups with admiring cyclic Galois group, which are produced by the mod-2 reduction maps from local commutative rings and to their common residue field, supports in construction of the S-boxes over maximal cyclic subgroups. Of course these newly designed S-box increasing complexity during encryption and decryption.

2.3.1. Algorithm for S-box Construction Based on Galois Rings

Given below is the procedure, defining the S-box in 3 steps:

1 Inversion function I: $G_s \mathrm{U} \{0\} \to G_s \mathrm{U} \{0\}$ by $I(0) = 0 \ and \ I(x) = x^{-1} : \forall \ x \in G_s$

2 Linear scalar multiple function $f : G_s \mathrm{U}\{0\} \to G_s \mathrm{U}\{0\}$ by $f(x) = cx$

3 Take composition of Iof to get $(n+1)\times(n+1)$ S-box.

The maps described above is nothing more than a substitution within the set $G_n \cup \{0\}$. An element of the set is substituted with the element next to its respective inverse. In other words, the scalar multiplied with the inverse.

In the example below, we discuss and analyze this construction method for *4×4* S-box.

Let us consider the local rings $\mathbb{Z}_4 = \{0,1,2,3\}$, whereas $\mathbb{Z}_2 = \{0,1\}$, is its residue field. The monic polynomial $f(x) = x^4 + x + 1$ is basic irreducible over the local rings such that $\overline{f}(x) = f(x)$ mod $2 = x^4 + x + 1$ is irreducible polynomial over $\mathbb{Z}_2$.

S-box based on GF(2^4):

Take the polynomial ring $\mathbb{Z}_2[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_2, n \in \mathbb{Z}^+\}$ in one indeterminate x over binary field $\mathbb{Z}_2$. Let $<\bar{f}(x)> = \{a(x).\bar{f}(x) : a(x) \in \mathbb{Z}_2[x]\}$ be the principal ideal in $\mathbb{Z}_2[x]$, generated by $\bar{f}(x)$ where $\bar{f}(x) = x^4 + x + 1$. Then elements of Galois extension field $K = \frac{Z_2[x]}{<\bar{f}(x)>}$, of order 16 are given in Table 2.5.

Table 2.5

Exp	$Polynomial$	$Coff$	Exp	$Polynomial$	$Coff$
$-\infty$	0	0000	7	x^3+x^2+1	1101
0	1	0001	8	x^2	0100
1	$x+1$	0011	9	x^3+x^2	1100
2	x^2+1	0101	10	x^2+x+1	0111
3	x^3+x^2+x+1	1111	11	x^3+1	1001
4	x	0010	12	x^3	1000
5	x^2+x	0110	13	x^3+x+1	1011
6	x^3+x	1010	14	x^3+x^2+x	1110

S-box based on Galois ring GR(2^2, 4):

Take finite local ring $\mathbb{Z}_{2^k}$, with corresponding residue field $\mathbb{Z}_2$. $\mathbb{Z}_{2^k}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_{2^k}, n \in \mathbb{Z}^+\}$ is the polynomial extension of $\mathbb{Z}_{2^k}$ in the variable x and $\mathbb{Z}_2[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_2, n \in \mathbb{Z}^+\}$ is the polynomial extension of $\mathbb{Z}_2$ in the variable x.

Let $f(x) \in \mathbb{Z}_{2^k}[x]$, $f(x) = x^4 + x + 1$ be the basic irreducible polynomial of degree 4. Ideal generated by $f(x)$ is denoted as $< f(x) >$ and defined as $< f(x) >= \{a(x).f(x): a(x) \in \mathbb{Z}_{2^k}[x]\}$. Let $\boldsymbol{R} = \frac{\mathbb{Z}_{2^k}[x]}{<f(x)>} = \left\{a_0 + a_1x + a_2x^2 + \cdots a_{h-1}x^{h-1}: a_i \in \mathbb{Z}_{2^k}\right\}$ represent the set of residue classes of polynomials in x over $\mathbb{Z}_{2^k}$ modulo the polynomial $f(x)$. This ring, denoted by $GR(2^k, h)$ is a commutative ring with identity and is called the Galois extension of $\mathbb{Z}_{2^k}$. where $\bar{f} = r_2(f) =$ polynomial, f which has coefficient modulo *2*.

$K^*(= K\backslash\{0\}$ becomes the multiplicative group of units of the field K. Now, let R^* be the multiplicative group of units of the Galois ring R. Then the maximal cyclic subgroup of R^*, isomorphic to the cyclic Galois group K^*, of order *15* is denoted by G_{15} and it is given in Table 2.6.

Table 2.6

Exp	$Polynomial$	$Coff$	Exp	$Polynomial$	$Coff$
$-\infty$	0	0000	14	$x + 3x^2 + x^3$	0131
0	1	0001	16	$3 + 3x$	3300
2	$1 + 2x + x^2$	1210	18	$3 + x + x^2 + 3x^3$	3113
4	$3x + 2x^2$	0320	20	$x + 3x^2 + 2x^3$	0132
6	$2 + x + 3x^3$	2103	22	$1 + 3x^2 + x^3$	1031
8	x^2	0010	24	$3x^2 + 3x^3$	0033
10	$3 + 3x + x^2 + 2x^3$	3312	26	$3 + x^3$	3001
12	$2 + 2x + 3x^3$	2203	28	$1 + 3x + 2x^2 + x^3$	1321

Table 7. S-Box on $GR(4,4)$

0	193	215	246
100	15	240	4
64	77	29	147
121	30	163	56

Table 8. S-box over $GF(2^4)$

0	11	12	6
3	8	4	2
1	9	13	15
14	7	10	5

2.3.2. Majority Logic Criterion for the Analysis of Substitution Boxes

In [10] a majority logic criterion (MLC) has given. The MLC is used to analyze the statistical strength of the S-box in image encryption application. The encryption process creates distortions in the image, and the type of these distortions determines the strength of the algorithm.

The quantity of randomness in a system is estimated by entropy. In an image, the degree of entropy is linked to the arrangements of pieces, which aid the human to recognize the image. Contrast permits the viewer to recognize the objects in an image. Due to the method by which the image is encrypted, the magnitude of randomness increases results in the height of contrast level to a very high value. The higher level of contrast in the encrypted image displays strong encryption. Correlation is an inquiry, which measures the correlation of a pixel to its neighbor by possession into attention the texture of the entire image. The homogeneity analysis measures the closeness of the distribution of elements in the grey level co-occurrence matrix (GLCM) to GLCM diagonal. The GLCM displays the statistics of combinations of pixel brightness values or grey levels in tabular form. In the analysis of energy, we measure the energy of the encrypted images as preserved by various S-boxes. This amount deals the sum of square elements in GLCM.

The results of MLC, arranged in Table 9, show that the proposed S-boxes satisfy all the criteria up to the standard and can be used for secure communication.

Table 9.

Images	**Entropy**	**Contrast**	**Correlation**	**Energy**	**Homogeneity**
S-box over $GF(2^4)$	5.9698	0.2491	0.9778	0.1689	0.9181
S-box over $GR(4,4)$	**5.9437**	**0.2299**	**0.9789**	**0.1722**	**0.9256**

Chapter 3

A Novel Method to Construct S-boxes on Galois Ring $GR(8,8)$

3.1. Introduction

For secure communication, the most essential part of symmetric cryptography known as substitution box is improved in different ways. For these purposes, initially only Galois fields were used, but now Galois ring is also used to increase the algebraic complexity of the substitution box. In the construction of S-box on Galois ring $GR(4,4)$ in chapter 2, only two bijective maps are used but in this chapter, we proposed a new method to construct 16×16 S-boxes by using the elements of maximal cyclic subgroup of group of units of Galois ring $GR(8,8)$. We also used the elements of corresponding Galois field $GF(2^8)$ in the proposed method.

3.2. Algorithm for the Proposed S-boxes

Consider the finite local ring $\mathbb{Z}_8 = \mathbb{Z}_{2^3} = \{0,1,2,\ldots,7\}$ together with its residue field $\mathbb{Z}_2$. The ring $\mathbb{Z}_8[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_8, n \in \mathbb{Z}^+\}$ is the polynomial extension ring of $\mathbb{Z}_8$ in one indeterminate x and $\mathbb{Z}_2[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_2, n \in \mathbb{Z}^+\}$ is the polynomial extension ring of $\mathbb{Z}_2$ in one indeterminate x. The polynomial $\mathrm{P(x)} = x^8 + 3x^4 + x^3 + 3\mathrm{x} + 7$ is basic irreducible polynomial over $\mathbb{Z}_8$. The ideal generated by $P(x)$ is denoted and defined as:

$$\langle P(x)\rangle = \{a(x).P(x) : a(x) \in \mathbb{Z}_8[x]\}$$

Let $\boldsymbol{R} = \frac{\mathbb{Z}_8[x]}{\langle P(x)\rangle} = \{a_0 + a_1x + a_2x^2 + \cdots a_{h-1}x^{h-1} : a_i \in \mathbb{Z}_8\}$ represent the set of residue classes of polynomials in x over $\mathbb{Z}_8$ modulo the polynomial $P(x)$. This ring, denoted by $GR(2^3, 8)$ is a commutative ring with identity and is called the Galois extension of $\mathbb{Z}_8$ and $GR(p,h) = \frac{\mathbb{Z}_2[x]}{\overline{P}(x)} = \boldsymbol{K}$ is isomorphic to the

Galois field $GF(2^8)$, an extension of $\mathbb{Z}_2$ having 2^8 elements, where $\bar{P}(x) = x^8 + x^4 + x^3 + \mathrm{x} + 1$ is irreducible polynomial over $\mathbb{Z}_2$.

$K^*(= K\backslash\{0\})$ becomes the multiplicative cyclic group of units of the field K. Now, let R^* be the multiplicative group of units of the Galois ring R, then the maximal cyclic subgroup of R^*, isomorphic to the cyclic Galois group K^*, of order 255 is denoted by G_{255}. The elements of maximal cyclic subgroup G_{255} are obtained by considering β as a root of $\bar{P}(x)$ in $\mathbb{Z}_2$. In this case, by calculating successive power of β modulo 2 and modulo $\bar{P}(x)$, we get that $\beta^{255} = 1$. Hence, the maximal cyclic subgroup has 255 elements and to find these elements, we consider $\overline{\beta}$ be the root of $P(x)\ in\ \mathbb{Z}_8$, and so by calculating the consecutive power of $\overline{\beta}$, we get that $\overline{\beta}^{1020} = 1$. So that by theorem 2 (chapter 2), the elements of G_{255} are generated by $\alpha = \overline{\beta}^4$. These elements are listed in Table 3.1. The polynomials in Table 3.1 are given in decreasing power of α, i.e. the element 75023105 is represented by $7x^7 + 5x^6 + 2x^4 + 3x^3 + x^2 + 5$.

Following steps are required for the construction of new S-box on $G_{255} \cup \{0\}$:

- **Step 1:** Firstly we define an inversion map $I: G_{255} \cup \{0\} \to G_{255} \cup \{0\}$ by

$$I(n) = \begin{Bmatrix} 0 & : & if\ n = 0 \\ n^{-1} : & & if\ n \neq 0 \end{Bmatrix}$$

- **Step 2:** Secondly we define scalar multiple map $h: G_{255} \cup \{0\} \to G_{255} \cup \{0\}\ by$

$$h(n) = \begin{Bmatrix} 0 & : & if\ n = 0 \\ cn & : & if\ n \neq 0 \end{Bmatrix},$$

Where c is any element of G_{255}.

- **Step 3:** After taking composition of $I\ and\ h$, we define a map $\varphi: G_{255} \cup \{0\} \to GF(2^8)$ by

$$\varphi(0) = 0\ and$$

$$\varphi(\alpha^k) = \beta^k : 1 \leq k \leq 255$$

- **Step 4:** After applying map φ, all the values convert to byte in $GF(2^8)$, where we define a couple of maps $f\ and\ g\ from\ GF\left(2^8\right)\ to\ GF(2^8)\ by$

$$f(x) = \begin{Bmatrix} 0 & : & if\ x = 0 \\ x^{-1} & : & if\ x \neq 0 \end{Bmatrix} and\ g(x) = y \oplus H$$

Where

$$y = \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} and\ H = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

The proposed S-box given in Table 3.1 whose entries are bytes is then obtained by taking the composition of $f\ and\ g$, i.e. $S - box = g \circ f(x) = Tx^{-1} \oplus H$

Where

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} and\ H = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

- **Step 5:** After construction of S-box whose entries from $GF(2^8)$, we also turn back to $G_{255} \cup \{0\}$ by applying the inverse map of φ, $\varphi^{-1}: GF(2^8) \rightarrow G_{255} \cup \{0\}$ defined as:

$$\varphi^{-1}(0) = 0\ and\ \varphi^{-1}(\beta^k) = \alpha^k, where\ 1 \leq k \leq 255$$

- **Step 6:** In this last step, we apply the functions $I\ and\ h\ from\ G_{255} \cup \{0\}\ to\ G_{255} \cup \{0\}$, used in step 1 and step 2 with different value of $c \in G_{255}$, i.e.

$$I(n) = \begin{Bmatrix} 0 & : & if\ n = 0 \\ n^{-1} & : & if\ n \neq 0 \end{Bmatrix}\ and\ h(n) = \begin{Bmatrix} 0 & : & if\ n = 0 \\ kn & : & if\ n \neq 0 \end{Bmatrix}\ where\ k \neq c$$

So that the proposed S-box whose entries are from $G_{255} \cup \{0\}$ is formed and by applying $mod(8^8)$, each entry of the S-box becomes 24 bits, which are given in Table 3.7.

Table 3.1. Element representation of G_{255}.

Exp	Poly	Exp	Poly	Exp	Poly	Exp	Poly	Exp	Poly
0	00000001	51	75455303	102	76276614	153	45020540	204	60225230
1	00010000	52	05216645	103	15032127	154	42332702	205	34306222
2	00057501	53	67111221	104	71276403	155	65100133	206	53432430
3	75023105	54	77602411	105	12412427	156	64133510	207	36526243
4	63605702	55	50365760	106	75124741	157	13020313	208	55662052
5	30134360	56	62636636	107	71732712	158	51347502	209	34735366
6	30265713	57	42511163	108	55677073	159	05700534	210	44423373
7	44277626	58	57154751	109	04114067	160	06163570	211	73356642
8	36437727	59	55445015	110	44774111	161	33637416	212	16371435
9	62704543	60	64165144	111	01410777	162	60366263	213	61131137
10	21361270	61	37355216	112	04253641	163	44367636	214	70520013
11	35703736	62	42075035	113	32245525	164	36255236	215	31506252
12	25006570	63	16525507	114	44111624	165	45630725	216	54424150
13	04412052	64	22020052	115	56740111	166	44777463	217	50627642
14	21053141	65	20560402	116	12744274	167	34130777	218	01361262
15	54575205	66	22335656	117	13530674	168	70715313	219	17421736
16	61677757	67	76446133	118	54257253	169	04711571	220	61573142
17	56015467	68	10417244	119	01462525	170	11632171	221	10250457
18	65124301	69	41554541	120	22546746	171	75174063	222	53466125
19	26631712	70	06020255	121	07577654	172	72165017	223	73463146
20	33315563	71	00756002	122	71752257	173	03766016	224	61705146
21	41141031	72	60346175	123	50265275	174	67145176	225	30167407
22	51315514	73	43461434	124	65211626	175	36347314	226	61442616
23	65033631	74	57052146	125	71527221	176	66136234	227	05236544
24	11413403	75	37620005	126	20536352	177	42000513	228	66127423
25	00014641	76	76470162	127	01040753	178	43354200	229	54721012
26	46467501	77	22701464	128	04444504	179	05056435	230	27116672
27	37212446	78	34175270	129	41000044	180	65673605	231	07716411
28	14644421	79	43761717	130	41714100	181	11735067	232	67522471
29	17103364	80	52521176	131	02636671	182	24541073	233	01715152
30	02153613	81	26741355	132	60343163	183	32667054	234	56752671
31	30450315	82	37401274	133	13341434	184	67063066	235	37513775
32	70422145	83	02337740	134	62444734	185	15570506	236	27003451
33	52331242	84	71164133	135	23366644	186	55153057	237	55042700
34	27201133	85	77256416	136	03263136	187	44605615	238	36451101
35	32044720	86	13704025	137	30214126	188	16732460	239	05002445
36	36767604	87	16754370	138	36314521	189	71061573	240	25760500
37	61410476	88	10107775	139	30211331	190	43161706	241	24007376
38	63041641	89	46146010	140	00444521	191	52623116	242	15522400
39	77742704	90	22415214	141	45610444	192	46641462	243	74160752
40	53746374	91	72575741	142	41141261	193	56266264	244	34136216
41	75004774	92	02611557	143	53615514	194	73361426	245	53105313
42	71557500	93	17105761	144	67522061	195	44100136	246	65412310
43	23313255	94	21136710	145	05615152	196	41011410	247	06621241
44	57360031	95	02734013	146	52625261	197	55423601	248	10431062
45	16476536	96	42250173	147	67371462	198	42007742	249	17752743
46	32636147	97	47341325	148	71456237	199	35644200	250	71507075
47	50726163	98	52617334	149	10116245	200	30075164	251	26250150
48	74266272	99	00052761	150	31615511	201	46571307	252	25357725
49	17023226	100	27623105	151	47550661	202	05736157	253	16644635
50	04037102	101	52146462	152	45400055	203	62300473	254	1301326b4

Table 3.2. The Proposed S-box in $GF(2^8)$

63	7b	6b	76	82	c3	Fc	16	A2	31	40	90	31	41	7d	96
CF	f8	07	52	61	8f	2a	49	68	77	6f	6	72	93	33	ac
d9	18	4a	69	9a	CB	e9	f7	02	AE	35	51	60	62	8E	C7
ED	E6	F2	FE	FA	EB	1B	4B	84	3E	45	6C	66	9F	37	BD
29	48	85	D3	E1	E2	E3	0E	AA	24	A1	30	AD	34	BC	C4
EC	0B	56	70	7F	7A	86	D2	0C	46	6D	8B	3B	B9	38	B8
D5	1C	5B	99	CA	04	53	8C	2B	A4	CC	F9	EA	F6	EF	0A
BB	D4	F1	FF	17	4F	95	CE	15	A3	DC	E4	1E	B7	D0	E0
0F	47	80	2F	B5	3C	A9	25	4C	94	23	B1	2D	59	75	83
2E	58	98	27	A0	DD	09	BA	39	55	71	92	DE	08	57	9D
DB	F4	03	43	91	DF	E5	F3	13	5E	65	9E	DA	19	A7	CD
14	4E	78	6A	9B	26	4D	79	87	3F	A8	C8	E8	1A	A6	20
B0	C0	FD	FB	06	BF	C5	01	AF	D8	F5	EE	E7	1F	5A	74
6E	8A	D6	1D	B6	3D	44	81	C2	11	B2	2C	B4	D1	0D	AB
C9	05	BE	28	A5	21	5D	64	73	7E	97	22	5C	89	D7	F0
12	B3	C1	10	5F	88	3A	54	9C	36	50	8D	C6	00	42	7C

3.3. Algebraic Analyses

In this section, we discuss some valuable analyses of S-boxes based on residue of prime number to determine the strength of the proposed S-box [19, 20].

Nonlinearity

The distance between the Boolean function f and the set of all affine linear functions is said to be nonlinearity of f. In simple words, Nonlinearity of a Boolean function "f" represents the number of bits which changed in the truth table of f to reach the nearby affine function. The upper bound of nonlinearity of a function f is $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$ [7], so that for $n = 8$, the maximum value of nonlinearity is 120.

Strict avalanche criteria

The SAC was first introduced in 1895 by Webster and Tavares [26]. The SAC constructs on the notions of completeness and avalanche. It is satisfied if, whenever a single bit of input changed, each of the output bits changes with a 0.5 probability that is, when one bit of input is changed, half of its corresponding output bits will changes.

Bit independent criterion

The BIC was also first introduced by Webster and Tavares [5, 6], which is another required property for any cryptographic methods. A Boolean function $g: \mathbb{F}_2{}^k \rightarrow \mathbb{F}_2{}^k$ satisfies the BIC if for all $p, q, r \in \{1,2, \dots, k\}$ with $q \neq r$, change in bit p, causes change in the output bits $q\ and\ r$ independently.

Linear approximation probability

The maximum value of the imbalance of an event is said to be the linear approximation probability. The parity of the input bits selected by the mask G_x is equal to the parity of the output bits selected by the mask G_y. According to Matsui's original definition [16], linear approximation probability of a given S-box is defined as:

$$LP = \max_{G_x, G_y \neq 0} \frac{\{x \in X \,/\, x.G_x = S(x).G_y\}}{2^n} - \frac{1}{2}$$

Where G_x and G_y are input and output masks, respectively, "X" the set of all possible inputs and 2^n is the number of elements of X.

Differential Approximation Probability

[2] The differential approximation probability (DP) of S-box is a measure for differential uniformity and is defined as:

$$\mathrm{DP}\ (\Delta \mathrm{p} \rightarrow \Delta \mathrm{q}) = \frac{\{\mathrm{p} \in \mathrm{X} / \, S(\mathrm{p}) \oplus S(\mathrm{p} \oplus \Delta \mathrm{p}) = \Delta \mathrm{q}\}}{2^m}$$

This means, an input differential Δp_i should uniquely map to an output differential Δq_i, so that ensuring a uniform mapping probability for each i.

Table 3.3. Performance Indexes for S-box based on maximal cyclic subgroup G_{255} of Galois ring $GR(8,8)$

Analysis	Max.	Min.	Average	Square Deviation	DP	LP
Nonlinearity	109	103	**106.25**			
SAC	0.554688	0.445313	**0.492432**	0.0153784		
BIC		102	**105.5**	1.97303		
BIC- SAC		0.484375	**0.502302**	0.0104275		
DP					**0.0390625**	
LP	157					**0.117188**

Table 3.4. Comparison of Performance indexes of S-box based on maximal cyclic subgroup G_{255} of Galois ring $GR(8,8)$ and different 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
Proposed S-box	**106.25**	**0.492432**	**0.502302**	**105.5**	**0.0390625**	**0.117188**

3.4. Image Encryption using 8 bits S-box

In this section, we analyze the original and encrypted images by some statistical analysis methods. This analysis is done on the basis of energy, homogeneity, contrast, correlation and entropy.

Energy

The energy of encrypted image can be measure by energy analysis. For this purpose, the gray-level co-occurrence matrix (GLCM) is used. The sum of squared components in GLCM is said to be Energy. The mathematical formulation for this analysis is given by:

$$E = \sum_{m}\sum_{n} f^2 \text{ (m, n)}$$

Here m and n are the pixels in the image and p (m, n) provides the number of gray-level co-occurrence matrices. Note that the value of energy is 1 for constant image.

Entropy

By entropy, we evaluate the quantity of randomness in a system. The high level of randomness make the image difficult to detect and by substituting non-linear components, the randomness of an image is increased in the system and its mathematical form is:

$$H = \sum_{i=0}^{n} f(x_i) \log_b f\, x_i$$

Where x_i represents the Histogram calculations.

Contrast

Contrast used by the viewer to recognize the objects in an image. Due to image encryption method, the randomness in the encrypted image increases results in the height of contrast level to a very high value. The higher level of contrast in the encrypted image offerings strong encryption. It is directly related to the confusion caused by S-box. For measuring contrast the mathematical formula is given by:

$$C = \sum_{m}\sum_{n} (m-n)^2 f(m,n)$$

Homogeneity

The contents of an image are naturally distributed. The analysis to measures the closeness of distributed elements of GLCM to GLCM diagonal is homogeneity analysis. It is also known as gray tone spatial dependency matrix. The GLCM shows the statistics of arrangement of pixel gray levels in tabular form. This analysis can be extended more by processing entries from GLCM table. The mathematical form of Homogeneity analyses is given by:

$$H^* = \sum_{m}\sum_{n} \frac{f(m,n)}{1-|m-n|}$$

The value of contrast is zero for constant image.

Correlation

In Correlation analysis, we analyze the correlation of pixel to its neighbors by considering the texture of entire image. Correlation analysis is done in three ways, the horizontal, vertical, and diagonal formats are selected for this purpose. For this purpose, the entire image is also analyzed along with partial regions. The correlation is calculated as:

$$K = \frac{(\mathrm{m} - \alpha\mathrm{m})(\mathrm{n} - \alpha\mathrm{n})\mathrm{f}(\mathrm{m}, \mathrm{n})}{\sigma_m \sigma_n}$$

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

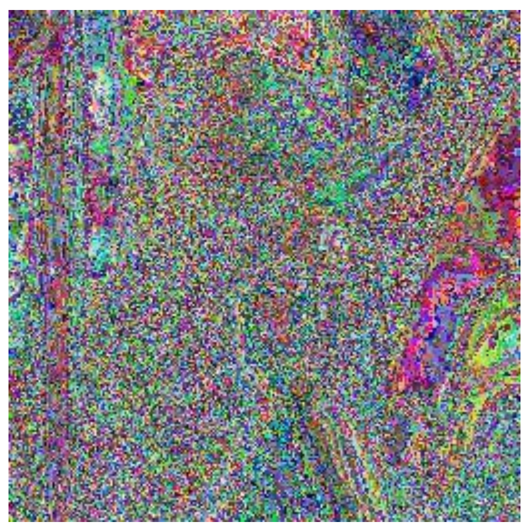
The result of all these analyses are given in Table 3.5. The comparison of the analyses of the proposed S-box with some well-known S-boxes is given in Table 3.6.

Table 3.5: Second order texture analyses for proposed S-box with one round.

	Plain image	Plain color components of image			Cipher image	Cipher color components of image		
		Red	Green	Blue		Red	Green	Blue
Contrast	0.360279	0.369317	0.384743	0.36129	4.78347	4.75432	4.88329	4.72728
Homogeneity	0.880754	0.871235	0.871275	0.875008	0.489707	0.4898	0.487004	0.487588
Entropy	7.77044	7.729631	7.58034	7.07804	7.75576	7.74498	7.77744	7.72567
Correlation	0.92102	0.92441	0.930748	0.855138	0.0760063	0.183539	0.200078	0.156543
Energy	0.122479	0.138046	0.099876	0.169255	0.0287946	0.026298	0.0246558	0.027055

Figure 3.1(a) Plain image of Lena

Figure 3.1(b) Encrypted image using bytes



From figure 3.1(a) and figure 3.1(b), we see that plain image of Lena (512×512) is successfully encrypted using the proposed S-box of 8 bits (in one round). After analyzing the results in Table 3.5, Table 3.6 and figure 3(a), 3(b), we comprehended that the proposed algebraic substitution box have strong cryptographic properties and can be useful for encryption and decryption processes.

3.5. Image Encryption Scheme over 24 bits S-box

The entries of S-box in Table 3.7 are the decimal representation of elements of G_{255} and by converting these entries into binary form, we can obtain maximum 24 binary bits. The image encryption technique based on this S-box is given in the following steps:

- Take an image and transformed the pixels of this image to 24 bits.
- Divide the pixel into three bytes and split first byte into two parts, the left 4 and right 4 bits.
- Convert these bits to decimals. $p, and\ q$ respectively
- Pick $S(p,q)$, i.e. the element of S-box in p^{th} row and q^{th} column.
- Convert this element from decimal to binary (24 bits).
- Replace binaries of S-box with the pixel of the image and continue this process for whole image to get the encrypted image.

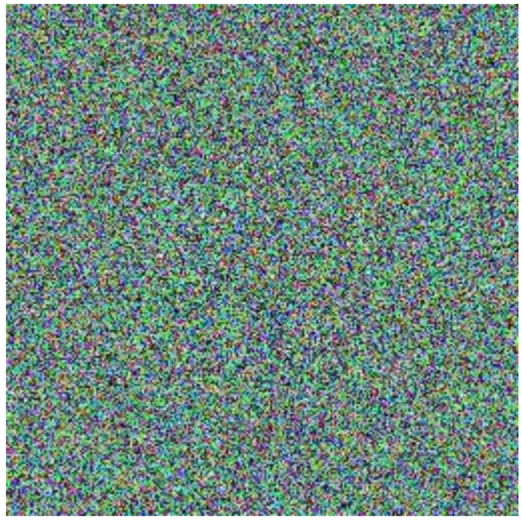
By using this encryption scheme, the original image and encrypted image of Lena are given in Figure 3.2(a) and Figure 3.2(b):

Table 3.7. Proposed S-box of entries 24 bits:

3800784	3658014	5056153	10034615	10107775	4253641	5242836	1040753	4584054	1180934	8015877	16371435	3925605	15468309	12056012	2773665
394515	7051888	6823103	7914241	2293613	11413403	5637998	2700804	8453310	10493547	6020255	9607274	15080662	12113086	9472934	2611557
3411149	3411149	15858931	10116245	82984	8346439	10011515	413607	7716411	13341434	7230160	15267504	8159668	16731418	2337740	13274054
15032127	10868941	9854496	413197	12744274	1361262	12304988	4243557	8229354	12709993	7157408	13488497	11110968	8695741	11241494	8065199
14644421	4711052	983866	7456978	5002445	11219679	10633840	1999594	13390191	10723194	581784	14768485	2760089	6354282	13704025	5700534
13436910	11845623	13530674	10799489	4711571	4055269	4448636	14879978	751790	4037102	16710843	6536039	11051183	36312	2896669	5091953
4359494	2883295	4167539	2357	246010	3100782	5330404	14641	7586829	1715152	13016875	13020313	10014527	57501	5466877	4389364
4347373	2291468	7763857	975527	5683819	13297948	6421023	12076293	6408463	5616152	11632171	10250457	15795775	4643393	3766016	16732460
16644635	5345425	9964139	3263136	6763570	11968825	3952709	756002	13087030	7586599	4065573	8000109	34112	644520	13786893	15804586
6621241	5924248	576345	14838295	7445612	4275925	8956731	2734013	11346109	4398211	6589428	13434115	16476536	11735067	1015854	16754370
10813204	5113367	1	9337269	7895910	10147552	11373498	10423917	15522400	1410777	6720498	2792882	2285686	3283866	16538347	5934616
9893582	4418357	9799768	4092502	2189528	295994	4821409	7028383	444521	10557192	3414726	10417244	9361298	10431062	15889838	2636671
5216645	12412427	12372895	4444504	10339456	52761	5558440	10000	9907002	10226235	2971811	326148	1462525	16525507	2153613	1814814
10545704	14701983	262598	13996229	10207285	4114067	5736157	3606449	7577654	8580509	6252562	9167750	13357144	2089768	14792653	6247778
4623848	13013264	14729036	5056435	13833496	8520603	5769530	328545	3959343	12591578	2149304	5236544	3134477	3846842	15570506	11466108
3313281	11223031	620838	13801862	8983284	8446081	3759136	3783186	10845889	13673099	8778270	12913069	3213172	0	11078828	4412052

Figure 3.2(a): Original image of Lena

Figure 3.2(b): encrypted image of Lena by 24-bits



3.6. Analysis of S-box of 24 bits' values:

In this section, we analyze the original and encrypted images by some statistical analysis, included contrast, energy, homogeneity, correlation and entropy. The results of these analysis are given in the Tables 3.8, 3.9, 3.10 and 3.11.

Table 3.8: Second order texture analyses for proposed S-box with one round.

	Plain image	Plain color components of image			Cipher image	Cipher color components of image		
		Red	Green	Blue		Red	Green	Blue
Contrast	0.360279	0.369317	0.384743	0.36129	4.75492	4.58575	4.8981	4.6881
Homogeneity	0.880754	0.871235	0.871275	0.875008	0.507578	0.503674	0.502144	0.501368
Entropy	7.77044	7.729631	7.58034	7.07804	7.75779	7.713191	7.7901	7.69629
Correlation	0.92102	0.92441	0.930748	0.855138	0.121812	0.233256	0.230363	0.161865
Energy	0.122479	0.138046	0.099876	0.169255	0.0316347	0.0266638	0.0253099	0.0283091

Table 3.9: Second order texture analyses for proposed S-box with two rounds.

	Plain image	Plain color components of image			Cipher image	Cipher color components of image		
		Red	Green	Blue		Red	Green	Blue
Contrast	0.360279	0.369317	0.384743	0.36129	5.571110	5.355740	5.71988	5.52646
Homogeneity	0.880754	0.871235	0.871275	0.875008	0.460391	0.463644	0.457663	0.460043
Entropy	7.77044	7.729631	7.58034	7.07804	7.752790	7.654860	7.77014	7.73147
Correlation	0.92102	0.92441	0.930748	0.855138	-0.005837	0.0397641	0.0751045	0.0543705
Energy	0.122479	0.138046	0.099876	0.169255	0.0278643	0.0269354	0.024186	0.0255029

Table 3.10: Second order texture analyses for proposed S-box with three rounds.

	Plain image	Plain color components of image			Cipher image	Cipher color components of image		
		Red	Green	Blue		Red	Green	Blue
Contrast	0.360279	0.369317	0.384743	0.36129	5.60313	5.36719	5.76397	5.53044
Homogeneity	0.880754	0.871235	0.871275	0.875008	0.458551	0.461704	0.456284	0.458297
Entropy	7.77044	7.729631	7.58034	7.07804	7.74951	7.63751	7.76913	7.72563
Correlation	0.92102	0.92441	0.930748	0.855138	-0.0128951	0.026995	0.0662226	0.0433087
Energy	0.122479	0.138046	0.099876	0.169255	0.0279192	0.0270493	0.0242703	0.025794

3.7. Comparison of the proposed S-boxes

Table 3.11 shows the comparison of statistical analysis between the two constructed S-boxes. Due to randomness, the values of contrast increases which makes the encrypted image difficult to detect. Also the value of contrast, after apply 8-bits S-box is greater than that of the other, so compare to contrast 8-bits S-box is greater than 24-bits S-box. The homogeneity, correlation and energy values are also different in original and encrypted images.

Table 3.11.

Images	**Entropy**	**Contrast**	**Correlation**	**Energy**	**Homogeneity**
Plain image	7.77044	0.360279	0.92102	0.122479	0.880754
Encrypted image over 1 byte entries	7.75576	4.78347	0.0760063	0.0287946	0.489707
Encrypted image over 3bytes entries	7.75779	4.75492	0.121812	0.0316347	0.507578

Chapter 4

Construction of S-box on Maximal ideal of local ring $\mathbb{Z}_{512}$

4.1. Introduction

In this chapter, we present a technique to design a substitution box, which has a powerful algebraic complexity. We used elements of maximal ideal M of the local ring $\mathbb{Z}_{512}$ to construct 8×8 S-box. We used the maximal ideal of a local ring for the very first time in S-box construction. For the construction of 8×8 S-box, we first define a couple of bijective mappings from M to M and then apply linear fractional transformation as: $\mathrm{f}(m) = (am + b)/(cm + d)$, where m is any arbitrary element in M, and a, b, c, d are fixed elements from the Galois field $GF(2^8)$. The strength of the proposed S-box is analyzed by Nonlinearity test, Strict Avalanche Criterion (SAC), Linear Approximation Probability (LP), Bit Independent Criterion (BIC), and Differential Approximation Probability (DP). In addition, by the majority logic criterion (MLC), energy, entropy, homogeneity, contrast and correlation of a plain image and its encrypted image by newly proposed S-box are checked. Further, we compare the results of all these analyses with AES, APA, Prime, Gray, Xyi, Skipjack and S_8 AES S-boxes to fix the rank of our proposed S-box.

4.2. Algorithm for proposed S-box

The designing procedure of the new S-box is based on the maximal ideal $M = \{0, ,2,4, \dots ,510\}$ of a local ring $R = \mathbb{Z}_{512}$ and the projective linear group $PGL(2, GF(2^8))$ applied to Galois field $GF(2^8)$. We first define inverse mappings $I: M \to M$ by $I\,(m) = -m,$ where $-m$ is additive inverse of m in R. Then a mapping like affine transformation is defined as: $f: M \to M,\ f(m) = r\,.\,m + n$, where r and n are fixed in $U(R)$ and M respectively. Thus the composition of I and f will be defined as $Iof(m) = -rm + n$.
As the elements of M are 9 binary bits representation, so we define a bijection $g: M \to \mathbb{Z}_{256}$ by $g(2m) = m$, where $0 \leq m \leq 255$. Also there is one-one correspondence between $\mathbb{Z}_{256}$ and $GF(2^8)$. so, lastly the

linear fractional transformation used in the construction of S-boxes is given as; $h: PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8)$ $h(m) = \frac{45m+10}{2m+9}$, where $45,10,2,9 \in GF(2^8)$. Figure 4.1 shows the flow chart of the construction method. For the construction of the new S-box, the algorithm begin with the maximal ideal M of a local ring $R = \mathbb{Z}_{512}$ and use of $GF(2^8)$. The function $h(m)$ is formed with the action of $PGL\ (2, GF(2^8))$ on $GF(2^8)$. The function $I, f, g\ and\ h$ are used in the process to create the new designed S-box. Further details of last step of the algorithm is shown in Table 4.1. In Table 1, column 1 denotes the elements of $GF(2^8)$ ranging from 0 to 255. Column 2 represents the analytical details of the linear fractional transformation and the results from the evaluation of $h(m)$ are listed. The numbers in $h(m)$ are substituted with their binary value equivalent, represented as some power of α, where α is defined as the root of the primitive irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x^2 + 1$. The resulting values from $GF(2^8)$ are then converted to the eight-bit binary values to be used in S-box. The final column displays the elements of the proposed S-box.

The new S-box, created through the proposed algorithm is shown in Table 2. This is a 16×16 look up table and can be used to process eight binary bits of data.

Figure 1. Flow chart for proposed S-box

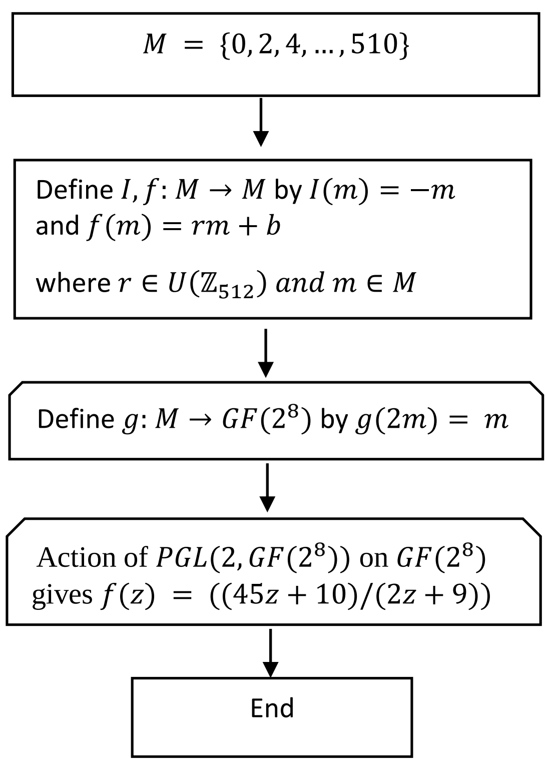


Table 4.1. **The Algorithm for LFT**

$GF\ (2^8)$	$h(m) = (45m + 10)/(2m + 9)$	Proposed S-box elements
0	$h(0) = \frac{45(0)+10}{2(0)+9} = \frac{10}{9}$	221
1	$h(1) = \frac{45(1)+10}{2(1)+9} = \frac{55}{11}$	69
.	.	.
.	.	.
.	.	.
254	$h(254) = \frac{45(254)+10}{2(254)+9} = \frac{176}{5}$	44
255	$h(255) = \frac{45(255)+10}{2(255)+9} = \frac{221}{7}$	239

Table 4.2. **The Proposed S-box**

69	44	87	140	249	211	61	166	247	59	17	210	169	88	83	144
24	200	56	171	85	191	103	124	111	30	35	192	5	95	109	118
2	245	94	133	91	163	113	114	66	184	107	120	86	180	14	213
3	187	108	119	39	4	195	32	181	227	135	92	68	38	121	106
126	31	145	82	127	131	178	49	204	129	76	151	84	117	73	154
153	10	0	241	81	158	239	243	25	233	123	104	232	235	148	79
18	58	12	215	99	203	51	176	8	142	201	26	37	116	150	77
238	222	205	22	179	225	155	72	229	136	41	186	212	161	11	216
134	141	29	198	165	224	71	156	102	188	9	218	55	46	53	174
50	159	149	78	130	101	162	65	254	100	67	160	220	23	157	70
236	143	231	251	54	74	45	182	242	146	6	221	183	202	234	248
16	250	13	214	168	209	112	115	139	128	60	167	27	219	122	105
36	190	57	170	197	244	185	42	132	48	207	20	237	253	230	252
64	15	1	226	43	93	208	19	47	62	147	80	40	125	175	52
223	172	89	138	255	177	90	137	189	97	33	194	196	228	152	75
96	7	199	28	98	246	164	63	110	173	21	206	217	240	193	34

4.3. Algebraic Analysis

It is also observed from Table 4.3, and figure 4.2 that average nonlinearity of proposed S-box is **103** which is better than some well-known S-boxes like Xyi S-box, Prime S-box and Skipjack S-box. Table 4.3, also shows the results of BIC analysis of proposed S-box and in the sense of encryption strength, the BIC of the proposed S-box is acceptable. Table 4.4 shows that the rank of our proposed S-box is comparable with S-boxes from literature and we observed that the proposed S-box satisfied BIC close to the best possible value. We also see from Table 4.3 that the average value of linear approximation probability (LP) of the proposed S-box is $\mathbf{0.148438}$ which is appropriate against linear attacks. The average value of differential approximation probability for proposed S-box is **0.140625** (Table3) and Table 4.5 shows the comparison of differential approximation probability (DP) of proposed S-box with AES, APA, Gray, S8 AES, Skipjack, Xyi and residue prime S-boxes and we observed that the results of DP of proposed box are relatively better from S-box constructed on residue of prime numbers.

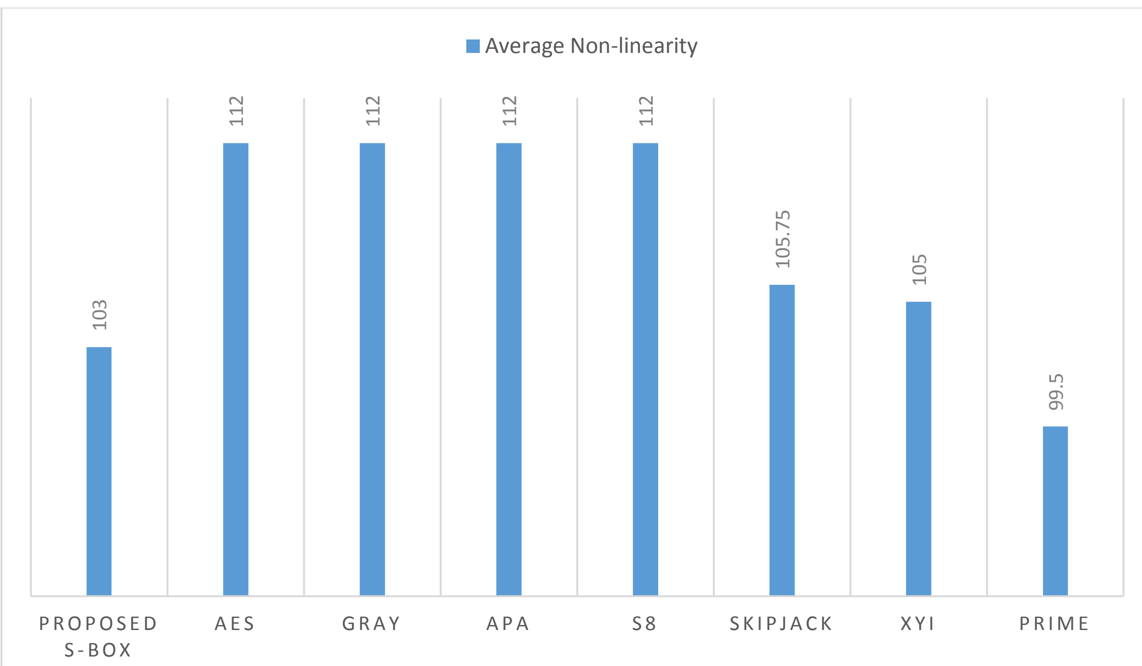
Table 4.3: Performance Indexes for S-box based on Maximal ideal M of $\mathbb{Z}_{512}$

$Analysis$	$Max.$	$Min.$	$Average$	$Square\ Dev$	DP	LP
$Nonlinearity$	106	100	**103**			
SAC	0.71875	0.1875	$\mathbf{0.503418}$	0.0395832		
BIC	114.858	90	$\mathbf{102.429}$	4.35421		
$BIC - SAC$		0.470703	$\mathbf{0.502093}$	0.0174062		
DP					$\mathbf{0.140625}$	
LP						$\mathbf{0.148438}$

Table 4.4: Comparison of Performance indexes of S-box based on Maximal ideal of $\mathbb{Z}_{512}$ and different 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
Proposed S-box	**103**	**0.503418**	**0.502093**	**102.429**	**0.140625**	**0.148438**

Figure 4.2. Comparison of Non-linearity of the proposed S-box with some different well-known S-boxes



4.4. Encryption Using Proposed S-box

From figure 4.3(a) and figure 4.3(b), we see that plain image of (512×512) is successfully encrypted using the proposed S-box (in one round). After analyzing the results in Table 4.5, Table 4.6 and figure 4.3(a), 4.3(b), we comprehended that the proposed algebraic substitution box have strong standing cryptographic properties and can be useful for encryption and decryption processes.

Figure 4.3 (a). Original image of Lena

Figure 4.3 (b). Encrypted image of Lena

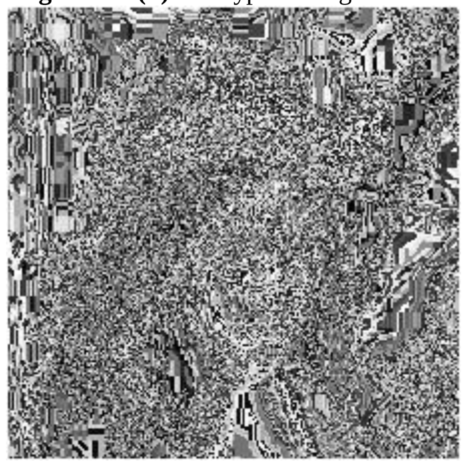


Table 4.5. Contrast, Correlation, Energy, Homogeneity and entropy of plain image and cipher image of Lena $(512x512, \text{png})$

Images	Entropy	Contrast	Correlation	Energy	Homogeneity
Plain image	7.4451	0.2100	0.9444	0.1455	0.9084
Encrypted image	**7.5841**	**9.4258**	**0.1013**	**0.0178**	**0.4659**

Table 4.6. Comparison of Contrast, Correlation, Energy, Homogeneity and entropy of plain image and cipher image of Lena $(512x512, \text{png})$ of S-box based on Maximal ideal of $\mathbb{Z}_{512}$ and different S-boxes

Images	Entropy	Contrast	Correlation	Energy	Homogeneity
Plain image	7.4451	0.2100	0.9444	0.1455	0.9084
Proposed S-box	**7.5841**	**9.4258**	**0.1013**	**0.0178**	**0.4659**
AES	7.2531	7.5509	0.0554	0.0202	0.4662
APA	7.2531	8.1195	0.1473	0.0183	0.4676
Prime	7.2531	7.6236	0.0855	0.0202	0.4640
S8_AES	7.2357	7.4852	0.1235	0.0208	0.4707
Gray	7.2531	7.5283	0.0586	0.0203	0.4623
Xyi	7.2531	8.3108	0.0417	0.0196	0.4533
Skipjack	7.2531	7.7058	0.1025	0.0193	0.4689

Chapter 5

Conclusion

In the construction technique of S-box over maximal cyclic subgroup G_s of group of units of Galois ring $GR(p^k, m)$ in the second chapter, we observed that if we take eight degree irreducible polynomial over $\mathbb{Z}_{p^k}$ then there is 0% chance of obtaining S-box having entries one byte (8 bits). Whereas all the real applications are in eight bits, making this technique a very week one. But now we define a relation between the elements of G_{255} and $GF(2^8)$, from which we can construct S-boxes whose entries are eight bits and can be used in image encryption applications and other encryption schemes. This method of construction has great algebraic complexity. In this chapter, we constructed two different S-boxes on maximal cyclic subgroup G_{255} of group of units of Galois ring $GR(8,8)$ by selecting particular parameters $c, k, H\ and\ T$. Entries of one S-box is eight bits and of the other is twenty-four bits, which are used in different image encryption algorithms. By this method, we can construct many different S-boxes over G_{255} corresponding to different basic irreducible polynomials and by changing the value of parameters $c, k, H\ and\ T$. So that it is very difficult by exhaustive search method to break S-box, constructed in Galois rings. In addition, we observe that if we made only 8-bits S- box, then by changing irreducible polynomial, there is no change in this S-box because it depends on generators of G_{255} and of $GF(2^8)^*$. On the other hand, if we return to the second S-box whose entries are 24-bits, then corresponding to different irreducible polynomials, we can obtain different S-boxes. Therefore, we conclude that the S-box of entries 24-bits has much more algebraic complexity than the S-box of entries 8-bits. We also find that the proposed S-boxes have applications in image encryption algorithms. Further, we can think about the relation between Galois ring and chaos theory, which creates more confusion, and diffusion.

In the presented work in fourth chapter, a novel technique for the construction of 8×8 Substitution box over the elements of Maximal ideal of the integers modulo ring $\mathbb{Z}_{512}$ was proposed. The maximal ideal of a local ring is not used in any other previous cryptosystem. We used it first time for the construction of S-box in this work and observed that the proposed S-box exhibit an enhanced level of security. A high level of randomness is achieved by this newly proposed S-box, which creates algebraic complexity due to the algorithm defined over Maximal ideal of the integers modulo ring $\mathbb{Z}_{512}$. We can construct 256×256 (65536) different S-boxes by changing value of r and n in $U(Z_{512})$ and in maximal ideal M of Z_{512}. Also for different value of a, b, c, and d such that $ad \neq bc$ used in linear fractional transformation, one can construct many different S-boxes. We can also think about $\boldsymbol{U}(\mathbb{Z}_{512})$ which has cardinality 256 and can be used to increase algebraic complexity of the proposed S-box.

References

[1] Andrade, A.A., Palazzo, R. (1999). Construction and decoding of BCH codes over finite rings, *Linear Algebra Applic*.286, 69-85.

[2] Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.

[3] Cui, L., & Cao, Y. (2007). A new S-box structure named Affine-Power-Affine.*International Journal of Innovative Computing, Information and Control*, *3*(3), 751-759.

[4] Daemen, J., & Rijmen, V. (2002). The design of rijndael: AES. *The Advanced Encryption Standard*.

[5] Dawson, M. H., & Tavares, S. E. (1991, April). An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In *Advances in Cryptology—EUROCRYPT'91* (pp. 352-367). Springer Berlin Heidelberg.

[6] Detombe, J., & Tavares, S. (1992). On the design of S-boxes. *Advances in cryptology: proceedings of CRYPTO_92. Lecture notes in computer science*.

[7] Feng, D., & Wu, W. (2000). Design and analysis of block ciphers.

[8] Fraleigh, J. B. (2003). A first course in abstract algebra. *Pearson Education India*.

[9] Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2013). A projective general linear group based algorithm for the construction of substitution box for block ciphers. *Neural Computing and Applications*, *22*(6), 1085-1093.

[10] Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, *23*(1), 97-104.

[11] 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.

[12] Hussain, I., Shah, T., Gondal, M.A, Mahmood, H. (2013). An efficient approach for the construction of LFT S-boxes using chaotic logistic map, *Nonlinear Dyn* 71:133–140.

[13] Hussain, I., Shah, T., Mahmood, H. (2012) A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Comput. Appl.* doi:10.1007/s00521-012-0914-5

[14] Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, U. Y. (2011). Some analysis of S-box based on residue of prime number. *Proc Pak Acad Sci*, *48*(2), 111-115.

[15] Kim, J., & Phan, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. *Cryptologia*, *33*(3), 246-270.

[16] Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In *Advances in Cryptology—EUROCRYPT'93* (pp. 386-397). Springer Berlin Heidelberg.

[17] Nagpaul, S. R. (2005). Topics in applied abstract algebra (Vol. 15). *American Mathematical Soc*.

[18] Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. *Springer Science & Business Media*.

[19] Shah, T., Hussain, I., Gondal, M. A., & Mahmood, H. (2011). Statistical analysis of S-box in image encryption applications based on majority logic criterion. *Int. J. Phys. Sci*, *6*(16), 4110-4127.

[20] Shah, T., Hussain, I., Gondal, M.A., Mahmood, H. (2011). Statistical Analysis of S-boxes based on Image Encryption, *International Journal of the Physical Sciences,* Vol. 6(16), 4110-4127.

[21] Shah, T., Qamar, A., Hussain, I. (2013). Substitution box on maximal cyclic subgroup of units of a Galois ring. *Z. Naturforsch A*, 68a, 567-572

[22] Shah, T., Mehmood, N., Andrade, A.A., and Palazzo Jr., R.: Maximal cyclic subgroups of the groups of units of Galois rings: A computational approach, *Computational and Applied Mathematics*- (40314/CAM) DOI 10.1007/s40314-015-0281-9

[23] Shanbhag, A.G., Kumar, P.V., Helleseth, T. (1996). Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q-ary sequences. *IEEE Trans. Inform. Theory*, 42(1), 250-254

[24] Shankar, P. (1979) On BCH codes over arbitrary integer rings. *IEEE Trans. Inform.* 25(4), 480-83

[24] Stallings, W. (2006). Cryptography and network security: principles and practices. *Pearson Education India*.

[25] Tran, M. T., Bui, D. K., & Duong, A. D. (2008, December). Gray S-box for advanced encryption standard. In *Computational Intelligence and Security, 2008. CIS'08. International Conference on* (Vol. 1, pp. 253-258). IEEE.

[26] Webster, A. F., & Tavares, S. E. (1985, August). On the design of S-boxes. In *Advances in Cryptology—CRYPTO'85 Proceedings* (pp. 523-534). Springer Berlin Heidelberg.
[27] Yi, X., Cheng, S. X., You, X. H., & Lam, K. Y. (1997, November). A method for obtaining cryptographically strong 8× 8 S-boxes. In *Global Telecommunications Conference, 1997. GLOBECOM'97, IEEE* (Vol. 2, pp. 689-693).