Chapter 1

Fundamentals of Algebra, Coding theory and Cryptography

In the following introductory chapter, the fundamental aim is to present background of the bits and pieces used in the succeeding chapters. This chapter is categorized in three sections. In section 1, we discussed about groups, rings and fields. Basic concepts of coding theory are described in section 2. Section 3 contains the basic ideas and terminologies of cryptography. Most part of this chapter is taken from [6], [13].

1.1 Algebraic notations and structures

Basic definitions and concepts are described in this section.

1.1.1 Binary Operation

Consider any non-empty set $\mathfrak{J}$, a function $* : \mathfrak{J} \times \mathfrak{J} \to \mathfrak{J}$ is a binary operation and is defined as follows, for all $\theta_1,\ \theta_2\ \in\ \mathfrak{J}$

$$*\,(\theta_1, \theta_2) = \theta_1 * \theta_2\ \in \mathfrak{J}$$

1.1.2 Groups

Let $\mathfrak{J} \neq \emptyset$, then $\mathfrak{J}$ will be called a group if it satisfies the following underlying conditions under the binary operation " $*$ ". $(\mathfrak{J},*)$ will be a group if $for\ all\ \theta_1, \theta_2, \theta_3 \in \mathfrak{J}$,

- $(\mathfrak{J},*)$ satisfies the closure law, $for\ all\ \theta_1, \theta_2 \in \mathfrak{J}$, this implies $\theta_1 * \theta_2\ \in \mathfrak{J}$.

- Associative law is satisfied by $(\mathfrak{J},*)$ if $for\ all\ \theta_1, \theta_2, \theta_3 \in \mathfrak{J}$ such that:

$$\theta_1 * (\theta_2 * \theta_3) = (\theta_1 * \theta_2) * \theta_3$$

- Identity element $\mathfrak{e}$ must be in $\mathfrak{J}$ $for\ all\ \theta_1 \in \mathfrak{J}$ such that:

$$\mathfrak{e} * \theta_1 = \theta_1 * \mathfrak{e} = \theta_1$$

- Inverses of all elements must exist in $\mathfrak{J}$. Let $\theta_1 \in \mathfrak{J}$ then θ_1^{-1} must be in $\mathfrak{J}$ such that:

$$\theta_1 * \theta_1^{-1} = \theta_1^{-1} * \theta_1 = \mathfrak{e}$$

Definition 1 A group is called Abelian group if operation " $*$ " is commutative, that is: $for\ all\ \theta_1, \theta_2 \in \mathfrak{J}$,

$$\theta_1 * \theta_2 = \theta_2 * \theta_1$$

Example 1 Under ordinary addition set of real numbers formed an Abelian group.

1.1.3 Rings

A ring $\mathfrak{J}$ is a set of elements in which two algebraic operations are defined, such that, " $+$ " called addition and " $\cdot$ " called the multiplication. $(\mathfrak{J}, +, \cdot)$ is called a ring if it satisfies the following three axioms if $for\ all\ \theta_1, \theta_2, \theta_3 \in \mathfrak{J}$,

i. $(\mathfrak{J}, +)$ is an abelian group.
ii. Semigroup is formed under multiplication operation, that is: $(\mathfrak{J}, \cdot)$.
iii. The operation " $\cdot$ " is distributive with respect to " $+$ ", that is:

$$\theta_1 \cdot (\theta_2 + \theta_3) = (\theta_1 \cdot \theta_2) + (\theta_1 \cdot \theta_3)$$

Example 2 Set of integers, rational and real numbers under addition and multiplication are all rings.

Definition 2 If multiplicative identity is present in a ring $\mathfrak{J}$ then that very ring termed as ring with identity.

Example 3 Set of integers.

Definition 3 If a ring $\mathfrak{J}$ with a binary operation " $\cdot$ " is commutative then $\mathfrak{J}$ will be a commutative ring.

Definition 4 If every non zero element of a ring $\mathfrak{J}$ possesses a multiplicative inverse then $\mathfrak{J}$ called division ring.

Definition 5 A ring $\mathfrak{J}$ have a zero divisor if $\theta_1 \cdot \theta_2 = 0$ for $\theta_1, \theta_2 \in \mathfrak{J}$ and both must be non-zero.

Example 4 Consider $\mathbb{Z}_4$ which is a ring of residue classes modulo 4, then it is interesting to see $2 \cdot 2 = 0$ but $2 \neq 0$. So $\mathbb{Z}_4$ has a zero divisor.

Definition 6 A commutative ring with unity and possesses no zero divisor called an integral domain.

1.1.4 Fields

A ring $(\mathfrak{J}, +, \cdot)$ is field if $(\mathfrak{J}, \cdot)$ is an Abelian group.

Example 5 Set of rational and real numbers except including zero in them are both fields.

Definition 7 Suppose $\mathfrak{J}$ is a ring with identity, let $\aleph$ be a non-empty subset of $\mathfrak{J}$ and is termed to be ideal if it undergoes following properties,

i. $\eth_1 - \eth_2 \in \aleph \; for \; all \; \eth_1, \eth_2 \in \aleph$

ii. $\theta_1 \eth \in \aleph \;\; for \; all \; \eth_2, \eth_2 \in \aleph \; and \; \theta_1 \in \mathfrak{J}$

Definition 8 Let 'q' be a nonzero noninvertible element in a ring $\mathfrak{J}$ with identity, q will be called an irreducible element if $q = mn$ with $m, n \in \mathfrak{J}$ and importantly one of them must be in $\mathfrak{J}$.

Definition 9 Suppose $\aleph$ is an ideal in a ring $\mathfrak{J}$ with a condition that $\mathfrak{J}$ and $\aleph$ are not equal, that is: $\mathfrak{J} \neq \aleph$ and $\aleph \subseteq \mathfrak{J}$ such that for any $\eth_1, \eth_2 \in \mathfrak{J}$,

$$\eth_1 \eth_2 \in \aleph \text{ implies that } \eth_1 \in \aleph \; or \; \eth_2 \in \aleph.$$

Then, the ideal $\aleph$ is prime.

Definition 10 A proper ideal $\mathcal{M}$ in a ring $\mathfrak{J}$ is said to be maximal ideal if for all ideals $\aleph$ in $\mathfrak{J}$, $\mathcal{M} \subseteq \aleph \subseteq \mathfrak{J}$ implies $\mathcal{M} = \aleph \; or \; \aleph = \mathfrak{J}$.

Example 6 $n\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ iff n is a prime number.

1.1.5 Finite field

A field of finite order or having finite number of elements is called a finite field.

Example 7:

- $\mathbb{Z}_p$ is a finite field for p being a prime number.
- Galois fields are well known finite fields.

Definition 11 A polynomial that cannot be factored into two non-constant polynomials over the same field called irreducible polynomial.

Example 8 $1 + \mathrm{x}^2$ is irreducible polynomial over the field of real numbers but it is reducible over the field of complex numbers, that is, $1 + \mathrm{x}^2 = (1 + ix)(1 - ix)$ and $(1 + ix)\ and\ (1 - ix) \in \mathbb{C}[x]$.

Definition 12 A primitive element α of a finite field F with order q is an element with multiplicative order $q - 1$, that is all the powers of ς gives the nonzero elements of the finite field. From the powers of ς we can easily point out the elements of a finite field.

Remark 1:

At least single primitive element must exist in every finite field.

Definition 13 A polynomial $g(y)$ is said to be primitive over $\mathcal{R}$ if $c\big(g(y)\big)$ is unit in $\mathcal{R}$, where $\mathcal{R}$ is a UFD.

Definition 14 $g(y) = a_0 + a_1 y + a_2 y^2 + \cdots + a_n y^n$ be a nonzero polynomial over $\mathcal{R}$ then content of $g(y)$ is denoted as $c\big(g(y)\big)$, that is, $c\big(g(y)\big) = g.c.d\{a_0, a_1, a_2, \cdots, a_n\}$.

1.1.6 Galois ring

Consider three positive integers $m, s\ and\ p$, where p is prime, then $GR(p^m, s)$ represents the Galois ring of order p^{ms}. It is the Galois extension of degree s of the $\frac{\mathbb{Z}}{\mathbb{Z}_{p^m}}$ of integer mod p^m. $GR(p^m, s)$ is $\left(\frac{\mathbb{Z}}{\mathbb{Z}_{p^m}}\right)$ while $GR(p, s)$is F_{p^s}.

1.1.7 Existence of a finite field

It was Galois who answered entirely the question of the existence of a finite field that:

- The number of elements should be of prime power $q = p^m$ that is the order of a finite field.
- For every prime power $q = p^m$, there exist a field of order q, and importantly it should be unique (up to isomorphism).

1.1.8 Galois field

Every element of a Galois field apart from zero is started as a power of a primitive element say ς, of the field. Cyclic group is formed from the nonzero elements of a field which are defined by binary primitive polynomial.

Example 9 $GF(2^4)$ is a Galois field of order 16. For the construction $GF(2^4)$, let $p(x) = x^4 + x + 1$ be primitive irreducible polynomial over $F_2[x]$. Let $\varsigma \in GF(2^4)$ be primitive element that generate all the field element.

Table 1: Galois field of order 16

Exp. Of a	Polynomial form	Bin.	Dec.	Exp. Of a	Polynomial form	Bin.	Dec.
0	0	0000	0	ς^8	$\varsigma^2 + 1$	0101	5
ς^1	ς^1	0010	2	ς^9	$\varsigma^3 + \varsigma^1$	1010	10
ς^2	ς^2	0100	4	ς^{10}	$\varsigma^2 + \varsigma^1 + 1$	0111	7
ς^3	ς^3	1000	8	ς^{11}	$\varsigma^3 + \varsigma^2 + \varsigma^1$	1110	14
ς^4	$\varsigma^1 + 1$	0011	3	ς^{12}	$\varsigma^3 + \varsigma^2 + \varsigma + 1$	1111	15
ς^5	$a^2 + a^1$	0110	6	ς^{13}	$\varsigma^3 + \varsigma^2 + 1$	1101	13
ς^6	$a^3 + a^2$	1100	12	ς^{14}	$\varsigma^3 + 1$	1001	9
ς^7	$a^3 + a^1 + 1$	1011	11	ς^{15}	1	0001	1

1.1.9 Operations in a Galois field

The irreducible polynomial $x^4 + x + 1$ that generates the field defines the modulus of the field for all arithmetic operations. The value of the modulus is $10011_2 = 19_{10}$

$$p(x) = 1x^4 + 0x^3 + 0x^2 + 1x + 1 = 10011_2 = 19_{10}$$

In Galois field the operations are:

- $GF(2^n)$ Addition.
- $GF(2^n)$ Multiplication.

i. $GF(2^n)$ Addition

Bit-wise XOR ($\oplus$) operation is used for doing the arithmetic of addition in $GF(2^n)$.

Example 10: $2 + 4 = 0010 \oplus 0100 = 0110 = 6$

Example 11: $8 + 9 = 1000 \oplus 1001 = 0001 = 1$

Since, $1 + 1 = 0\ and\ 1 - 1 = 0$, so addition and subtraction yield the same results.

ii. $GF(2^n)$ Multiplication

Binary arithmetic combined with XOR is used to perform the operation of multiplication and the modulus of the field is applied for determining the result of the multiplication. If the result is more than the modulus value, it is XORed with the modulus to acquire remainder in the field.

Example 12:

$$8 \times 9 = 1000 \times 1001 = 100 = 4$$

1 0 0 0

×1 0 0 1

1 0 0 0

0 0 0 0 ×

0 0 0 0 × ×

$$\underline{1\,0\,0\,0\times\times\times}$$

$$1\,0\,0\,1\,0\,0\,0$$

$$\underline{1\,0\,0\,1\,1\quad\quad}$$

$$\underline{0\,0\,0\,0\,1\,0\,0\quad}$$

Result is 4_{10}. Also $a^8.a^9 = a^{17} = a^2.a^{15} = a^2 = 100_2 = 4_{10}\ where\ a^{15} = 1\ in\ GF(16)$.

1.2 Introduction to coding theory

In the coming section, very important definitions as well as some details about algebraic codes is given which is very handy to learn.

Suppose F be a finite field of q (> 1) symbols and suppose $V = \mathrm{F}^n$ is the vector space of n-tuples over F where n is some positive integer greater than 1.

Definition 15 V consists of q^n elements that are called words or vectors.

Definition 16 Any nonempty subset C of V is called $q - ary$ code of length n. If $q = 2\ and\ 3$ then code C called binary and ternary code repectively.

Definition 17 The hamming distance between the two vectors $\varkappa_1\ and\ \varkappa_2$ of F^n is represented by $d(\varkappa_1, \varkappa_2)$ and is defined as follows;

$$d(\varkappa_1, \varkappa_2) = \left|\left\{1 \le i \le n | \varkappa_{1_i} \ne \varkappa_{2_i}\right\}\right|$$

Example 13 In $\{0,1\}^4$, $d(1100, 0110) = 2$.

Definition 18 $d(C)$ represents the minimum distance of a code C and defined as follows;

$$d(C) = min\{d(\varkappa_1, \varkappa_2) | \varkappa_1, \varkappa_2 \in C, \varkappa_1 \ne \varkappa_2\ \}$$

Example 14:

- The binary repetition code $C = \{00000, 11111\}$ has minimum distance is 5.
- The minimum distance of $C = \{00000, 10111, 10011\}$ is 1.

Definition 19 The weight of a vector $\varkappa \in \mathrm{F}^n$ is the number of nonzero components of $\varkappa$ denoted by $w(\varkappa)$.

Example 15 $w(10101) = 3$

1.2.1 Relation between minimum distance and hamming weight

- For any vectors $\varkappa_1, \varkappa_2 \in \mathrm{F}^n$, $d(\varkappa_1, \varkappa_2) = w(\varkappa_1 - \varkappa_2)$.
- For a linear $[n, k, d]$ code C, $d(C) = min\{w(\varkappa) | \varkappa \in C, \varkappa \neq 0\ \}$
- $d(C) \leq n - k + 1$.

1.2.2 Linear codes

Linear code over F is any subspace of the $V = \mathrm{F}^n$ vector space.

Definition 20 If the subspace C is of k dimension then C' is called a $[n, k]$ code and if a code C' has minimum distance d, then C' is called a $[n, k, d]$ code.

Example 16 The binary repetition code $C = \{00000, 11111\}$ is a $[5,1,5]$ code.

1.2.3 Generator matrix

Generator matrix G of a linear code C be a $k \times n$ matrix whose rows form a basis for C. Generator matrix is enough for the complete determination of a linear code.

Example 17 The generator matrix of $C = \{000, 111\}$ is $G = [1\ \ 1\ \ 1]$.

Definition 21 The dual code of a linear $[n, k]$ code C' over F, is defined as:

$$C^{\perp} = \{\varkappa_1 \in \mathrm{F} | \varkappa_1 \cdot \varkappa_i\ for\ all\ \varkappa_i \in \mathrm{F}\}$$

Example 18 $C^{\perp} = \{000, 110, 011, 101\}$ is dual code of $C = \{000, 111\}$.

Definition 22 Generator matrix H of a linear $[n, k]$ code C be a $(n - k) \times n$ matrix whose rows form a basis for $C^{\perp}$. Then H called the parity check matrix of C.

Example 19:

$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ be the parity check matrix of the code $C = \{000, 111\}$.

1.2.4 Canonical generator matrix

By performing the elementary row operations on G it can be transformed to $G^* = [I_k|A]$ which is in row-reduced echelon form where I_k be identity matrix of order k and A is a matrix of order $k \times (n-k)$.

Definition 23 Codes for which $d(C) = n - k + 1$ are called maximum distance separable codes or MDS codes.

Example 20 Reed Solomon codes or RS codes are MDS codes.

1.2.5 Advantages of a linear codes

We can define a code by its basis. Moreover, we can find a basis by Gaussian elimination of a matrix in which rows are included as a codewords. The code's minimum distance and weight is same. Mapping a message into the code and reverse is straight forward.

Definition 24 The mapping τ: $F^n \rightarrow F^n$ defined as $\tau(\varkappa_1, \varkappa_2, \cdots, \varkappa_n) = (\varkappa_n, \varkappa_1, \cdots, \varkappa_{n-1})$ is called a cyclic shift.

Example 21 $\tau(1,0,1,0,1) = (1,1,0,1,0)$

Definition 25 When a linear code $C \in F^n$ satisfying the under lying condition

$$\tau(\varkappa) \in C \; for \; all \; \varkappa \in C$$

the code formed called cyclic code.

Example 22 The code $C = \{101,011,110,000\}$ is a binary cyclic code.

1.2.6 Extension field

Given a finite field F and for a positive integer m, there exists an irreducible polynomial $g(y) \in F[y]$ of degree m. The field F_{p^r} is a result of constructing the quotient ring $\frac{\mathbb{Z}_p[y]}{\langle g(y) \rangle}$, where $g(y)$ is an irreducible polynomial of degree m in $\mathbb{Z}_p[y]$. In a more generalized way, for $F = F_q$, we construct F_{q^m} as a quotient ring $\frac{F_q[y]}{\langle g(y) \rangle}$, where $g(y)$ is an irreducible polynomial of degree m in $F_q[y]$.the field F_{q^m} is called extension field of F_q of degree m.

Definition 26 For $\varsigma \in \mathrm{F}_{q^m}$. Then there exists a monic polynomial $\mathcal{g}(y) \in \mathrm{F}_q[y]$ of least degree such that $\mathcal{g}(\varsigma) = 0$. The irreducible polynomial $\mathcal{g}(\varsigma) \in \mathrm{F}_q[y]$ is called the minimal polynomial of ς over F_q.

1.2.7 BCH codes

BCH are cyclic linear codes named after Bose, Chaudhuri and Hocquenghem. Let c, δ, q, n be a positive integer such that $2 \leq d \leq n$, q is a prime power and $(n, q) = 1$. Let m be the least positive integer such that $q^m \equiv 1(mod\ n)$. Thus $n|q^m - 1$. Let ς be a primitive nth root of unity in F_{q^m}. Let $m_j(y) \in \mathrm{F}_q[y]$ denote the minimal polynomial of ς^j. Let $\mathcal{g}(y)$ be the product of distinct polynomials among $m_j(y), j = c, c+1, \cdots, c+\delta-2$ that is

$$\mathcal{g}(y) = l.c.m\{m_j(y)|j = c, c+1, \cdots, c+\delta-2\} \in \mathrm{F}_q[y]$$

Since $m_i(y)$ divides $y^n - 1$ for each i, it follows that $\mathcal{g}(y)$ divides $y^n - 1$. Let C be a cyclic code with generator polynomial $\mathcal{g}(y)$ in the ring $\mathrm{F}_q[y]_n$. Then C is called a BCH code of length n over F_q having designed distance δ.

Definition 27 If $n = q^m - 1$ then the BCH code C is called primitive.

Definition 28 Narrow sense BCH code having the parameter $c = 1$.

Example 23:

[15,5,7] BCH code with length $n = 15$, dimension $k = 5$ and designed distance $\delta = 7$.

For this BCH code we must find the minimal polynomial of ς^i for $i = 1, \cdots, 6$. $\varsigma, \varsigma^2, \varsigma^4$ have the same minimal polynomial $p_1(\varkappa)$. To find the minimal polynomial $p_2(\varkappa)$ of ς^3, we conclude that $\varsigma^3, \varsigma^6, \varsigma^{12}, \varsigma^{24}$ have the same minimal polynomial and the minimal polynomial $p_3(\varkappa)$ of ς^5that $\varsigma^5 and\ \varsigma^{10}$ have same polynomial.

Hence,

$$p_1(\varkappa) = \varkappa^4 + \varkappa + 1$$

$$p_2(\varkappa) = (\varkappa - \varsigma^3)(\varkappa - \varsigma^6)(\varkappa - \varsigma^9)(\varkappa - \varsigma^{12})$$

$$p_2(\varkappa) = \varkappa^4 - (\varsigma^3 + \varsigma^6 + \varsigma^9 + \varsigma^{12})\varkappa^3 - (\varsigma^3 + \varsigma^6 + \varsigma^9 + \varsigma^{12})x^2 - (\varsigma^3 + \varsigma^6 + \varsigma^9 + \varsigma^{12})\varkappa + 1$$

$$p_2(\varkappa) = \varkappa^4 + \varkappa^3 + x^2 + \varkappa + 1$$

$$p_3(\varkappa) = (\varkappa - \varsigma^5)(\varkappa - \varsigma^{10})$$

$$p_3(\varkappa) = x^2 + \varkappa + 1$$

The required generator polynomial of BCH code is;

$$g_{BCH}(\varkappa) = l.c.m\{m_i(\varkappa)|i = 1,2,3,4,5,6\}$$

$$= p_1(\varkappa) \cdot p_2(\varkappa) \cdot p_3(\varkappa)$$

$$g_{BCH}(\varkappa) = \varkappa^{10} + \varkappa^8 + \varkappa^5 + \varkappa^4 + \varkappa^2 + \varkappa + 1$$

1.2.8 Reed Solomon codes

Reed Solomon codes are non-binary codes over the $GF(p^m)$ where p is a prime number and m is a positive integer. Let $\varsigma \in GF(p^m)$ be an element of order of n. We begin with the construction of the field $F = F_2[x]/(p(x))$ of order 2^m by choosing a primitive polynomial $p_1(x)$of degree m in $F_2[x]$ to construct a Reed-Solomon code. Reed-Solomon codewords includes the polynomials of degree less than $2^m - 1$. Reed-Solomon codewords are in $F[x]$, however, BCH codewords are elements in $F_2[x]$. Following generator polynomial $g_{RS}(x) \in F[x]$ is used for the construction of multiple $t\ error$ correcting RS-code.

$$g_{RS}(x) = \prod_{j=1}^{2t}(x - a^j)$$

The $RS[n = p^m - 1, k = p^m - d, d]$ be reed Solomon code of length n, dimension k and d is the designed distance of the code. The RS code generated by this generator polynomial is exactly the MDS code.

- **Properties of RS codes**

- Reed-Solomon codes are notably more popular among all other types of codes because they are distinctively perfect for correcting error bursts.

- Several errors occur very close together in a received vector is said to have error burst.
- Widespread and renowned use of Reed-Solomon codes is in the encoding of software, information on compact discs and music.

Example 24 For finding the Generator polynomial for $RS[n = 2^4 - 1, k = 2^4 - 3, d = 3]$ $over$ $GF(2^4)$, we will start from the general formula of the generator polynomial of RS code $g_{RS}(x) = \prod_{j=1}^{2t}(x - a^j)$ where all $a^{j's} \in GF(2^4 = 16)$. This is one error correcting code so that $t = 1$.

$$g_{RS}(x) = \prod_{j=1}^{2(1)}(x - a^j)$$

$$g_{RS}(x) = (\varkappa - a^1)(\varkappa - a^2)$$
$$g_{RS}(x) = (\varkappa^2 - a^1\varkappa - a^2\varkappa - a^3)\ mod\ 2$$
$$g_{RS}(x) = \varkappa^2 + a^1\varkappa + a^2\varkappa + a^3$$
$$g_{RS}(x) = \varkappa^2 + (a^1 + a^2)\varkappa + a^3$$
$$g_{RS}(x) = \varkappa^2 + a^5\varkappa + a^3$$

In decimal representation;

$$g_{RS}(x) = x^2 + 2x + 4x + 8$$
$$g_{RS}(x) = x^2 + 6x + 8$$

1.3 Introduction to cryptography

Currently, our society is strongly bounded by the domain of the information epoch, which classified by the researcher assets and is functional inside data being deliberated remarkably priceless. Enlightening data exists which is used in various forms such as military, political and economic. The security and protection of this data during saving, transmission and in using daily tasks is of prime importance because transfer of data may result in the revelation of various financial loss, armed forces top secret or marketing. Hence, all type of sensitive data like banking

transactions, social security numbers and debit cards must be secure. So, Cryptography pays a vital role in data securing during transmission of information or data [8].

Protection and security of data is studied under cryptography. In other way, cryptography is study of encrypting information, transforming data into secret codes or the way from which you can hide data from others. From the stone-age to current time, during time of war the facility to interconnect secretly has been significant. Cryptography is a Greek word which means “Secret Writing”. The art to personate a message, cryptography plays an important role so that only the authorized person has ability to recognize it. There are two thresholds to this course.

- The plain text or original data is veiled. This is known as encryption.
- The reverse of encryption is decryption, that is, to transform back the veiled data to original format.

The secret keys are mandatory for both deciphering and enciphering.

1.3.1 Purpose of cryptography

Cryptography is also used to hoist real-world complications that need safety for data or information rather than only decrypting and encrypting messages [18]. The following four are the main purposes of cryptography:

- **Confidentially**

This term covered the two underlying concepts

- **Privacy:** Assured the individual’s authority, that, what type of information associates with them might be accrued and collected, to whom and by whom that type of information might be shared.

- **Data confidentiality:** Non-availability or revelation of private or confidential data to unlawful folks is guaranteed.

- **Integrity**

  Integrity comprises the following:

a) **Data integrity:** Assured that information or data is rehabilitated merely in a lawful and specific way.
b) **System integrity:** A guaranteed system that accomplish proposed function in an unaffected manner, which is free from unintentional illegal exploitation of system.

- **Authenticity**

The competence of communicating reveals to recognize, each other and the source of the message.

- **Availability**

The accessibility of computer scheme to certified parties on requirement.

1.3.2 Components of cryptography

The methodical learning of any regulation essentially constructed upon difficult classifications arise from basic perceptions. Some basic concepts used in cryptography are followed in this section [4].

- **Plain text**

Any conversation with in the language that we say the mortal language, which took the shape of plain text. It's implicit by the receiver, sender and those who have access to that very message.

- **Cipher text**

Cipher is an unreadable or a secret message. While any appropriate scheme is applied over the plain text to hide it, then this hide text is known as cipher text.

- **Encryption**

The conversion of plain text messages to cipher text through an algorithm is called encryption.

- **Decryption**

The inverse process of encryption is decryption from which we can again got the plain text from the cipher text.

- **Key**

A key is a vital characteristic of performing encipherment and decipherment. To make the cryptographic procedure secure, key is utilized for both encryption and decryption.

- **Confusion**

For development of the vastly multifaceted connection between cipher text and key is termed as confusion.

- **Diffusion**

Diffusion states that by the shifting of one character or alphabet in the plain text messages numerous characters in the message of cipher text ought to alter, likewise, if we alter character of the cipher text message, then numerous characters in plain text message should be change. Diffusion refers to the property that in the statistics messages of the plain text redundancy is dissipated in the statistics messages of the cipher text. Diffusion relates with the dependency of the binary bits output on the binary bits input. A good diffusion in a cipher could be produced by flipping single input bit which should alter every output bit with a probability of one half. It is obtained by permutation boxes.

1.3.4 Categories of cryptography

Cryptography has two main categories.

- Symmetric (private) key cryptography
- Asymmetric (public) key cryptography

1. **Symmetric (private) key cryptography**

This category involves a person whom secret key should be known. Both the receiver and sender of message may also be kept it. In private key cryptography both receiver and sender have copy of secret key. In this instance, during this passage approach to the key is vouchsafe. There are two set-ups to ponder,

- The interactive parties are acquainted with each other. In this situation, without any encrypting scheme the key is shared.

- In second case, familiarity is limited. For example, when seeing secure websites, key should be swapped in a secure way [14].
- Same key is used for the encryption and decryption of the message while using **symmetric encryption**.
- Two types of keys are used in **asymmetric encryption**, one called the 'public key' used for encryption and the other one called the 'private key' used for decryption.

Figure 1.1: Keys for symmetric and asymmetric encryption

Symmetric key cryptography is further classified into two categories, block cipher and stream cipher.

a. Stream cipher

One-bit stream data should be encrypted at a time in a stream cipher. Vigenere cipher and RC4 are example of typical and modern stream cipher respectively. If keystream cryptographic is haphazard, then it is difficult to break this cipher by some means besides to find the keystream. Though, in advance the keystream should be known to both receiver and sender via some confident and independent channel. Stream cipher is relatively quicker and modest while implementing through programming. If the proposed data traffic is large it presents incredible logistical problems. For concrete reasons, the generator of bit stream necessarily executed as an algorithmic procedure, hence the bit stream cryptography could be designed by both receiver and sender. In this tactic, the generator bit stream is a key-controlled process which produce a cryptographically

robust bit stream. Present, both the user's only need to share the generating key and everyone could produce the key-stream.

b. Block cipher

Block cipher plays vital role in symmetric or private key-based cryptosystems, where only receiver and sender known the secret key. A block cipher refers to bit sequences of group of fixed length named as blocks, where input bit sequences of defined length (termed as plain text) are transformed via complex operations into output bit sequences of exactly same length (termed as cipher text) [20]. The common examples of block ciphers are Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

DES

Data encryption standard is one of the ancient technique in symmetric block cipher. In 1976, to encounter National Bureau Standards (NBS) criteria for encryption system, DES was authoritatively standardized. In methodology of DES symmetric block cipher encrypted data in length of 64 bits block. It occupies key length of 56 bits which is articulated as number of 64 bits. In each byte, the last bit behaves as a parity check for preceding bits [11].

AES

Like DES, AES is symmetric block cipher. In AES, same key would be used for data encryption and decryption. Moreover, AES differ from DES in several ways. Rijndael procedure allows many block and key sizes, not just for the block of DES of 64 and 56 bits size key. The key and block size could be elected from 128, 192 and 256 bits which are not to be same. But, the AES standard stated that the algorithm could only admit a block of 128 bits and a selection of three keys 128, 192 and 256 bits

Figure 1.2: symmetric encryption

2. Asymmetric (public) key cryptography

Cryptography of asymmetric key is usually termed as 'cryptographic public key'. In symmetric key cryptography, two keys are used. One is known as 'public key' that could be spontaneously shared over insecure channel also the other key could be kept secret and not easily shared is termed as 'Private Key' [17].

Figure 1.3: Asymmetric encryption

Table 1.1 Comparison of asymmetric and symmetric encryption

Basis for Comparison	Asymmetric encryption	Symmetric encryption
Basic	Asymmetric encryption uses a different key for encryption and decryption.	Symmetric encryption uses a single key for both encryption and Decryption.
Performance	This type of Encryption is slow in execution due to the high computational burden.	Symmetric encryption is fast in execution.
Algorithms	Diffie-Hellman, RSA.	DES, 3DES, AES, and RC4.
Purpose	This encryption is used for securely exchanging secret keys.	The symmetric encryption is used for bulk data transmission.

encryption strength could be checked by the assistance of the consequences from statistical and algebraic analysis.

In this chapter, the cryptographic tools and mainly the diffusion layer in cryptographic literature have been discussed.

2.2 Modern cryptographic tools

Before 1950, cryptography was known to people like an art, but the current scenario of cryptography relies on regimen which requires provision from various fields which includes mathematics, computer science and electronics. After the world war 2, military intelligence forces had found great importance of cryptographic research for the security of their countries. After a couple of decades, first symmetric cryptosystem that is, DES, were invented in 1970. The crypto researchers of that time recognized that worthy ciphers were developed by joining small tools. By the progress of information technology and modern fastest computers, scheming has become much faster as compared to these initial days. These small tools that are used are described below:

- **Substitution**

In cryptography, the process of replacing one symbol to another symbol is termed as substitution. In standard cryptography, Caesar shift chip is an example of substitution cipher, in which every plaintext letter should be replaced by the letter three places further down in the alphabet.

- **Permutation**

For a set, an exact reallocation of its two arbitrary members is termed, as permutation.

- **Diffusion and confusion**

The lexes diffusion and confusion are the basic properties for making a secure cipher presented by Shannon [21].

- **Diffusion** is a cryptographic technique concoct to increase the redundancy of the plain text to vague the statistical edifice of the plaintext to prevent attempts to deduce the key. It is achieved by dispersing out the idiosyncratic plaintext digit over numerous cipher text digits, such as when a single bit of the plaintext is altered it must affect the whole cipher

text or the change must occur on the entire cipher text. In some block ciphers by applying permutation function on data the diffusion can be obtained because of that original plain text bits on different positions will contribute to a single bit of the ciphertext.

- **Confusion** is a cryptographic technique devised to enhance the vagueness of the plaintext, in simple words the technique ensures that the cipher text gives no clue about the plaintext. In confusion, the relationship between the value of the encryption key and the statistics of the cipher text is maintained as complex as possible. The confusion can be obtained by using substitution and complex mumbled algorithm that relies on the input (plaintext) and key.

Table 2.1: Comparison of diffusion and confusion

Basis of comparison	**Diffusion**	**Confusion**
Basic	Utilized to generate obscure plain texts.	Utilized to generate vague cipher texts.
Seek to	The statistical connection between the ciphertext and plaintext is made as complicated as possible.	Make a relation between statistics of the ciphertext and the value of the encryption key as complicated as possible.
Achieved through	Transposition algorithm	Substitution algorithm
Used by	Block cipher only.	Stream cipher and block cipher
Result in	Increased vagueness	Increased vagueness

2.3 Literature review for diffusion layer

In cryptographic literature, the most common cipher that have diffusion layer are discussed in this section.

2.3.1 DES diffusion layer

DES was a modified version of a LUCIFER and was finally adopted as a data encryption standard by the National Bureau of standards (NBS) in 1977. DES is a block cipher, that transforms 64-bits input data through a series of complicated operations with using an effective key length of 56 bits

- **Key addition**

In this step, XOR operation is done between each 128-bits state array and each 128-bits round key that should be generated from the given key through key schedule.

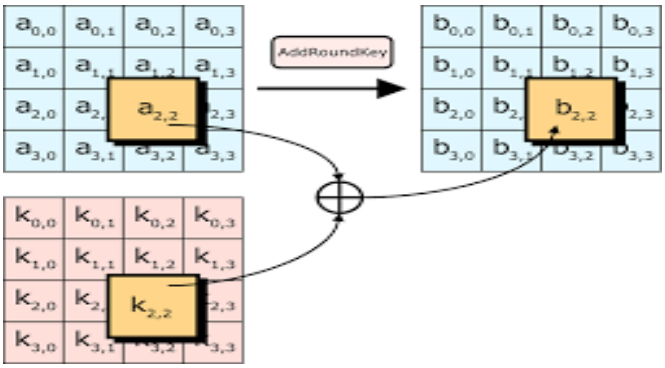

Figure 2.2: Key addition

- **Byte substitution(S-box)**

Byte substitution is a nonlinear operation, operating independently on each byte of the state array. Strong confusion is generated in the data by byte substitution.

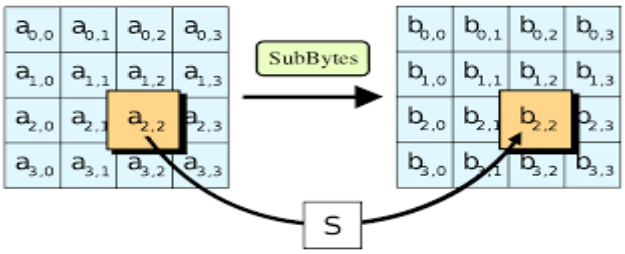

Figure 2.3: Byte substitution

- **Row shift**

This transformation is obtained by shifting the rows of the state array cylindrically. Means that, first row remains unchanged while the 2nd, 3rd and 4th row is moved toward left by one, two and three bytes respectively.

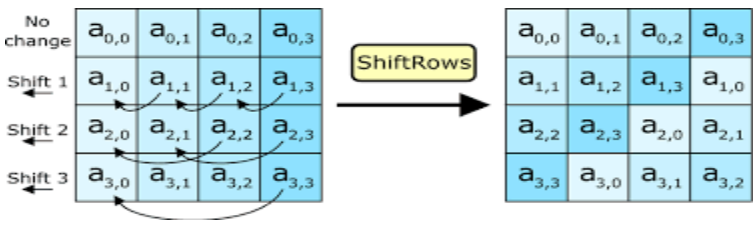

Figure 2.4: Row shift

- **Mix column**

Mix column is a step in which the state matrix is multiplied with a fixed matrix, that altered the columns of a state matrix. Mix column shuffled the columns of the state matrix.

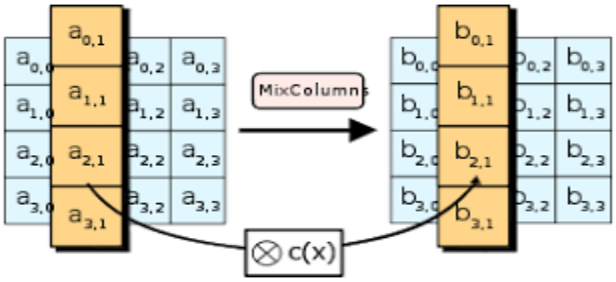

Figure 2.5: Mix column

In AES algorithm, the confusion is created by S-box substitution while the diffusion is created by mix column and the row shift operations. The diffusion layer of AES is explained below.

The Mix-Columns transformation works on the State matrix column-by-column. By considering each column as a four-term polynomial over $GF(2^8)$ and multiplied with a fixed polynomial $a_1(x)$ under reduction modulo $x^4 + 1$. $a_1(x)$ given by

$$a_1(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + 02$$

Or alternatively, in matrix multiplication, the current state matrix is multiplied with the fixed matrix CM_{AES} under the reduction modulo $x^4 + 1$.

$$CM_{AES} = \begin{bmatrix} 02_x & 03_x & 01_x & 01_x \\ 01_x & 02_x & 03_x & 01_x \\ 01_x & 01_x & 02_x & 03_x \\ 03_x & 01_x & 01_x & 02_x \end{bmatrix}$$

The diffusion layer of AES based on Mix column and row shift steps. Both these steps give best diffusing properties to AES algorithm. CM_{AES} is a generator matrix of a [8,4,5]-reed Solomon code over $GF(2^8)$ and is a MDS matrix. So, the diffusion step of AES comes from the codding theory and impart best results to the algorithm.

References:

[1] D. Augot, M. Finiasz, Direct construction of recursive mds diffusion layers using shortened BCH codes, 21st International Workshop on Fast Software Encryption, FSE 2014, Springer, 2014.

[2] J. Daemen, and V. Rijmen, AES Proposal: Rijndael. AES Algorithm Submission, September 3, 1999. http://www.nist.gov/CryptoToolKit

[3] J. Daemen, L.R. Knudsen, V. Rijmen, The block cipher SQUARE. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, Springer, Heidelberg 1997, pp. 149–165.

[4] D.E.R. Denning, Cryptography and data security, Addison-Wesley Longman Publishing Company Inc, 1982.

[5] J. Daemen, Cipher and hash function design strategies based on linear and differential cryptanalysis, Doctoral Dissertation, March 1995, K.U. Leuven.

[6] J.B. Fraleigh, A first course in abstract algebra, Seventh edition, Pearson education india, ISNB-10: 0201763907, 2003.

[7] J. Guo, T. Peyrin, A. Poschmann, The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer, Heidelberg (2011)

[8] I. Hussain, T. Shah, Literature survey on nonlinear components and chaotic nonlinear components of block ciphers, Nonlinear Dynamics, 74(4) 2013, 869-904.

[9] I. Hussain, T.Shah, M. A. Gondal, H. Mahmood, Generalized majority logic criterion to analysize the statistical strength of S-boxes, Zeitschrift fur Naturforschung A, 67(5) 2012, 282-288.

[10] P. Junod, S. Vaudenay, Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 84–99. Springer, Heidelberg (2004)

[11] P.T. Kenekayoro, The data encryption standard thirty-four years later, An overview, African Journal of Mathematics and Computer Science Research, 3(10), 2010, 267-269.

[12] J. Lacan, J. Fimes, Systematic MDS erasure codes based on vandermonde matrices. IEEE Trans. Commun. Lett. 8(9), 570–572 (2004)

[13] F.J. Mac Williams, N.J.A. Sloane, the theory of Error-correcting codes, Bell Laboratories Murray hill, N J press, USA, ISBN 0-44485009-4, 1977.

[14] N. McDonald, Past, present and future methods of cryptography and data encryption, Research Review, University of Utah, 2009.

[15]. [A] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error Correcting Codes. North Holland (1986)

[16] S.R. Nagpaul, S.K. Jain, Topics in Applied Abstract Algebra, Thomson, Brooks/Cole, U.S.A., 2005

[17] D. Pointchevel, Asymmetric cryptography and practical security, journal of Telecommunication and Information Technology, 2002, 41-56.

[18] S. K. Rakeshkumar, Performance Analysis of Data Encryption Standard Algorithm $ Proposed Data Encryption Standard Algorithm, International Journal of Engineering Research and development, e-ISSN, 11-20.

[19] V. Rijmen, J.Daemen, B. Preneel, A. Bosselaers, , E.D. Win, The cipher SHARK. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 99–112. Springer, Heidelberg (1996) 1999, 99-111.

[20] M. Sumathi, D. Nirmala, R.I. Rajkumar, Study of Data Security Algorithms using Verilog HDL, International Journal of Electrical and Computer Engineering, 5(5) 2015, 1092-1101.

[21] C. E. Shannon, Communication theory of secrecy systems, Bell Labs Technical Journal 28(4) 1949, 656-715.

[22] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish: A 128-bit block cipher. In: The First AES Candidate Conference, National Institute for Standards and Technology (1998)

[23] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, The Twofish encryption algorithm. Wiley (1999)

[24] M. Sajadieh, M. Dakhilalian, H. Mala, B. Omoomi, On construction of involutory MDS matrices from Vandermonde Matrices in *GF* (2*q*). Design, Codes Cryptography, 1–22 (2012)

[25] A.M. Youssef, S. Mister, S.E. Tavares, On the Design of Linear Transformations for Substitution Permutation Encryption Networks. In: Workshop on Selected Areas in Cryptography, SAC 1997, pp. 40–48 (1997)