CHAPTER 1

INTRODUCTION

1.1 Introduction

The rapid global adoption of computer networks and the Internet as an important business and personal communication medium in the past decade has dramatically increased the potential for information security breaches. An information security breach occurs when a malicious network user, or attacker, gains unauthorized access (read / write / modify) to information transmitted across the network or stored in network computers by other honest network users. The goal of information security engineering is to design information and communication systems which achieve confidentiality and integrity of the information over the network.

Present day public encryption and decryption services are based primarily on large prime numbers, occupying around 1024 bits. The field operations modulo on prime \( p \) easily make the available number of choices for a hacker to invest an enormous amount of available resources to find what the number \( p \) is. On the other hand, we could achieve, at least for dedicated systems, a protection by considering the residue arithmetic of the natural numbers, each of about 500 bits long. The purpose of this thesis is to use Claude Shannon’s principles of Confusion and Diffusion to develop
the encryption and decryption process a stream cipher using natural numbers and to develop access control system using Gaussian Farey numbers. These security measures can be easily provided for private communication in a public domain with the help of proposed methods. Principle of Confusion and Diffusion, as enunciated by Claude Shannon can be numerically implemented in a more secure manner for both the sender and the recipient.

1.2 Introduction to Cryptography

As the field of cryptography has advanced, the dividing lines for what is and what is not cryptography have become blurred. Cryptography today might be summed up as the study of techniques and applications that depend on the existence of difficult problems. Cryptanalysis is the study of how to compromise (defeat) cryptographic mechanisms, and cryptology (from the Greek kryptos logos, meaning ‘hidden word’) is the discipline of cryptography and cryptanalysis combined. Broadly cryptography is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history.

However, this is only one part of today’s cryptography. Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge (a key). Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back
into an intelligible form. Encryption and decryption generally require the use of some secret information, referred to as a key.

Today’s cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy, an example – signing of some document for instance. Important decisions and agreements are communicated electronically; hence there is a need to have electronic techniques for providing authentication.

Cryptography provides mechanisms for such procedures. A digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation at a particular time. These cryptographic mechanisms can be used to control access to a shared disk drive, a high security installation, or a pay-per-view TV channel.

The field of cryptography encompasses other uses as well. With just a few basic cryptographic tools, it is possible to build elaborate schemes and protocols that allow us to pay using electronic money, to prove we know certain information without revealing the information itself, and to share a secret quantity in such a way that a subset of the shares can reconstruct the secret.

While modern cryptography is growing increasingly diverse, cryptography is fundamentally based on problems that are difficult to solve. A problem may be difficult because its solution requires some secret knowledge, such as decrypting an encrypted message or signing some digital document. The problem may also be hard because it is intrinsically
difficult to complete, such as finding a message that produces a given hash value.

**Importance of Cryptography**

Cryptography allows people to carry over the confidence found in the physical world to the electronic world, thus allowing people to do business electronically without worries of deceit and deception. Every day hundreds of thousands of people interact electronically, whether it is through e-mail, ecommerce (business conducted over the Internet), ATM machines, or cellular phones. The perpetual increase of information transmitted electronically has lead to an increased reliance on cryptography.

**Cryptography on the Internet**

The Internet, comprised of millions of interconnected computers, allows nearly instantaneous communication and transfer of information, around the world. People use e-mail to correspond with one another. The World Wide Web is used for online business, data distribution, marketing, research, learning, and a myriad of other activities. Cryptography makes secure web sites and electronic safe transmissions possible.

For a web site to be secure all of the data transmitted between the computers where the data is kept and where it is received must be encrypted. This allows people to do online banking, online trading, and make online purchases with their credit cards, without worrying that any of their account information is being compromised.
Cryptography is very important to the continued growth of the Internet and electronic commerce. E-commerce is increasing at a very rapid rate. By the turn of the century, commercial transactions on the Internet are expected to total hundreds of billions of dollars a year. This level of activity could not be supported without cryptographic security. It has been said that one is safer using a credit card over the Internet than within a store or restaurant. It requires much more work to seize credit card numbers over computer networks than it does to simply walk by a table in a restaurant and lay hold of a credit card receipt. These levels of security, though not yet widely used, give the means to strengthen the foundation with which e-commerce can grow.

People use e-mail to conduct personal and business matters on a daily basis. E-mail has no physical form and may exist electronically in more than one place at a time. This poses a potential problem as it increases the opportunity for an eavesdropper to get a hold of the transmission. Encryption protects e-mail by rendering it very difficult to read by any unintended party. Digital signatures can also be used to authenticate the origin and the content of an e-mail message.

Authentication

In some cases cryptography allows to have more confidence in electronic transactions than in real life transactions. For example, signing documents in real life still leaves one vulnerable to the following scenario. After signing the will, agreeing to what is put forth in the document, someone can change that document and the signature is still attached. In the
electronic world this type of falsification is much more difficult because
digital signatures are built using the contents of the document being signed.

**Access Control**

Cryptography is also used to regulate access to satellite and cable
TV. Cable TV is set up so people can watch only the channels they pay for.
Since there is a direct line from the cable company to each individual
subscriber’s home, the Cable Company will only send those channels that
are paid for. Many companies offer pay-per-view channels to their
subscribers. Pay-per-view cable allows cable subscribers to ‘‘rent’’ a movie
directly through the cable box. What the cable box does is decode the
incoming movie, but not until the movie has been ‘‘rented.’’ If a person
wants to watch a pay-per-view movie, he/she calls the cable company and
requests it. In return, the Cable Company sends out a signal to the
subscriber’s cable box, which unscrambles (decrypts) the requested movie.

Satellite TV works slightly differently since the satellite TV
companies do not have a direct connection to each individual subscriber’s
home. This means that anyone with a satellite dish can pick up the signals.
To alleviate the problem of people getting free TV, they use cryptography.

The trick is to allow only those who have paid for their service to
unscramble the transmission; this is done with receivers (‘‘unscramblers’’).
Each subscriber is given a receiver; the satellite transmits signals that can
only be unscrambled by such a receiver (ideally). Pay-per-view works in
essentially the same way as it does for regular cable TV.
As seen, cryptography is widely used. Not only is it used over the Internet, but also it is used in phones, televisions, and a variety of other common household items. Without cryptography, hackers could get into our e-mail, listen in on our phone conversations, tap into our cable companies and acquire free cable service, or break into our bank/brokerage accounts.

Categories of Cryptography

A cryptosystem consists of a cipher along with one or two keys. The word cipher has been used in many different contexts with many different meanings. The term is also used synonymously with ciphertext or cryptogram in reference to the encrypted form of the message.

Cryptosystems can be categorized in “symmetric” and “asymmetric”:

- Symmetric or Secrete Key cryptosystems use the same key in the encryption process as well as in the decryption process. Cryptosystems in this category are for example DES, AES, and Blowfish. The proposed encryption and decryption process a stream cipher using natural numbers is a Symmetric or Secrete Key cryptosystem.

- Asymmetric cryptosystems use two different keys, one for encryption and one for decryption. Asymmetric cryptosystems are also known as public key cryptosystems. Cryptosystems in this category are RSA, ElGamal, and Merkle-Hellman.
Secret or Symmetric Key Cryptography

A secret key system consists of two transformations: An encryption transformation $E_K$ to encrypt a message $M$, and a decryption transformation $D_K$ to decrypt of the encrypted message, i.e. $D_K (E_K (M)) = M$. By imposing certain requirements to the transformations using parameter $K$, key as shown in figure 1.1, it is possible to withstand information integrity threats.

Suppose two parties, say Alice and Bob, are communicating messages on a public communication channel. Furthermore, suppose that a third party, say Eve has access to the communication channel: To prevent Eve from intercepting a message $M$ sent from Alice to Bob, Alice encrypts $M$ using $E_K$. Then, the resulting cipher text $C = E_k(M)$ is sent to Bob. Finally, Bob decrypts $C$ using $D_K$. The key $K$, used as parameter in the encryption and the decryption, is kept secret from Eve. Hence, by requiring that it is infeasible for Eve to compute $D_K(C)$ without knowledge of the key value, Alice and Bob have achieved privacy in their communication.

Figure 1.1: Illustration of a Secret key Cryptography
Furthermore, if it is infeasible for Eve to compute $E_K(M)$ without knowledge of the key value, Eve cannot pretend to be Alice in a communication where message $M$ is sent to Bob. The Data Encryption Standard (DES) system is the most widely used secret key crypto system.

**Public or Asymmetric Key Cryptography**

One of the reasons [DIFF88] for proposing public key cryptography was the problem of key distribution: If two people, who have never met before, are to communicate privately using secret key cryptography, they must somehow agree in advance on a key that will be known to themselves and to no one else. Another reason was the problems of signatures and of non-repudiation: A method was needed for providing the recipient of a purely digital electronic message with a way of demonstrating to other people, that the message had come from a legitimate person. Hence, the signature should allow the recipient to hold the author to the contents of the message.

In public key systems each user has key material which is divided into two portions, a private component and a public component as shown in figure 1.2. The public component generates a public transformation $E$ (encryption transformation), and the private component generates a private transformation $D$ (decryption transformation).

This is, however, an imprecise terminology: Depending on the actual system, it may be the case that $D(E(M)) = M$, and $E(D(M)) = M$, or both. A common requirement to the public transformation $E$ is that it must be a so-called trapdoor one-way function i.e. $E$ should be easy to compute from the
The public component of the key but hard to invert unless one possesses the corresponding private transformation $D$.

![Figure 1.2: Illustration of a Public key Cryptography](image)

The following examples show how privacy, signatures, and non-repudiation may be provided by a public key crypto system. The transformations $D_A$ and $E_A$ are those generated by Alice’s key, and the transformations $D_B$ and $E_B$ are those generated by Bob’s key:

- To prevent Charlie from intercepting a message $M$ sent from Alice to Bob, Alice encrypts the message by means of Bob’s public transformation $E_B$. Then, the cipher text $C = E_B(M)$ is sent to Bob, who decrypts $C$ by means of his own private transformation, $M = D_B(C)$. So, when the public key crypto system is used for obtaining privacy, only the transformations of the recipient are used. The requirement to the transformations is that $D_B(E_B$
\((M) = M\). It should be emphasised, that Bob never needs to share \(D_A\) with Alice.

- To convince Bob that the message \(M\) indeed originates from Alice and, hence, cannot have been generated by Charlie. Alice transforms the message by means of her own private transformation. Then, the resulting signed message \(S = D_A(M)\) is sent to Bob. To verify the signature, Bob applies Alice’s public transformation to obtain \(M = E_A(S)\). Since \(D_A\) is strictly private to Alice, Charlie could not possibly have generated the signed message. Note that only the transformations of Alice’s are used. In order to provide signatures, the transformations must obey \(E_A(D_A(M)) = M\).

- The signed message, \(S = D_A(M)\), could not even have been generated by Bob. Furthermore, the signature can be verified by every person who has access to Alice’s public transformation. Hence, Bob can prove to a third party that Alice indeed was the author of the signed message, and Alice cannot deny having signed the message. To provide privacy, the transformations used in public key systems must obey the condition \(D(E(M)) = M\), and to provide signatures they must obey \(E(D(M)) = M\). The Rivest-Shamir-Adleman (RSA) [RIV78] system that satisfies both conditions.

Compared to the secret key systems, the public key systems provide a wider range of information integrity functions and the key distribution problem is significantly reduced: There is no longer a need for exchanging secret keys. Apart from the private transformation of a user, only the public available transformations of the other users are required in order to apply public key cryptography.
1.3 Basic concepts and preliminaries

1.3.1 Natural Numbers

In mathematics, a natural number (also called counting number) can mean either an element of the set \{1, 2, 3, \ldots\} (the positive integers) or an element of the set \{0, 1, 2, 3, \ldots\} (the non-negative integers). The former is generally used in number theory, while the latter is preferred in mathematical logic, set theory, and computer science. A more formal definition will follow. Natural numbers have two main purposes: they can be used for counting and they can be used for ordering.

**Properties:** One can recursively define an addition on the natural numbers by setting \(a + 0 = a\) and \(a + S(b) = S(a + b)\) for all \(a, b\). This turns the natural numbers \((\mathbb{N}, +)\) into a commutative monoid with identity element 0, the so-called free monoid with one generator. This monoid satisfies the cancellation property and can be embedded in a group. The smallest group containing the natural numbers is the integers.

If \(1 := S(0)\), then \(b + 1 = b + S(0) = S(b + 0) = S(b)\). That is, \(b + 1\) is simply the successor of \(b\). Analogously, given that addition has been defined, a multiplication \(\times\) can be defined via \(a \times 0 = 0\) and \(a \times S(b) = (a \times b) + a\). This turns \((\mathbb{N}^*, \times)\) into a free commutative monoid with identity element 1; a generator set for this monoid is the set of prime numbers. Addition and multiplication are compatible, which is expressed in the distribution law: \(a \times (b + c) = (a \times b) + (a \times c)\). These properties of addition and multiplication make the natural numbers an instance of a commutative
Semirings are an algebraic generalization of the natural numbers where multiplication is not necessarily commutative (see section 1.3.2).

If the interpretation of the natural numbers is as "excluding 0", and "starting at 1", the definitions of $+$ and $\times$ are as above, except that we start with $a + 1 = S(a)$ and $a \times 1 = a$. Furthermore, one defines a total order on the natural numbers by writing $a \leq b$ if and only if there exists another natural number $c$ with $a + c = b$. This order is compatible with the arithmetical operations in the following sense: if $a$, $b$ and $c$ are natural numbers and $a \leq b$, then $a + c \leq b + c$ and $ac \leq bc$.

An important property of the natural numbers is that they are well-ordered: every non-empty set of natural numbers has a least element. The rank among well-ordered sets is expressed by an ordinal number; for the natural numbers this is expressed as "\( \omega \)". While it is in general not possible to divide one natural number by another and get a natural number as result, the procedure of division with remainder is available as a substitute: for any two natural numbers $a$ and $b$ with $b \neq 0$ we can find natural numbers $q$ and $r$ such that $a = bq + r$ and $r < b$.

The number $q$ is called the quotient and $r$ is called the remainder of division of $a$ by $b$. The numbers $q$ and $r$ are uniquely determined by $a$ and $b$. This, the Division algorithm, is key to several other properties (divisibility), algorithms (such as the Euclidean algorithm), and ideas in number theory. The natural numbers including zero form a commutative monoid under addition (with identity element zero), and under multiplication (with identity element one).
1.3.2 Theory of Finite Fields

Study Number Fields is required in generation of secure code in general in cryptography. The following description gives the insight of the basic algebraic structures.

Ordered pairs:

Let G be any set. An ordered pair (x, y) is defined as the unordered set \(\{x, \{x, y\}\}\), \(\forall x, y \in G\). The constructed has natural order of x first and then y can be verified by using the process of peeling of the set of its brackets. The unordered pair \(\{x, y\}\) thus becomes the ordered pair \((x, y)\). The set of all ordered pairs \(\{(x, y) \mid x, y \in G\}\) is called the Cartesian product denoted by the symbol \(G \times G\).

Groupoid \((G, \cdot)\):

The binary operation of G is a mapping of \(G \times G \rightarrow G\). Thus there is a unique element \(g\) associated with each pair of elements \((x, y) \in G \times G\); \((x, y) \rightarrow x \cdot y = g \in G\). The symbol \(\cdot\) is called a binary operation on the set G. Set G together with the binary operation \(\cdot\) is called a Groupoid \((G, \cdot)\).

Properties of Groupoid \((G, \cdot)\)

i. The Groupoid \((G, \cdot)\) is a commutative Groupoid when and only when \(x \cdot y = y \cdot x\) for all \(x, y \in G\).

ii. It is called a unitary Groupoid when and only when these exists element \(e \in G\) such that \(x \cdot e = x = e \cdot x\) for all elements \(x \in G\).
iii. The Groupoid \((G, \cdot)\) is called a semi group when and only when the associative law holds for all elements \(x, y, z \in G\):
\[ x \cdot (y \cdot z) = (x \cdot y) \cdot z \]

iv. The Groupoid \((G, \cdot)\) which is also a semi group and satisfies identity law is called Monoid.

**Semi group:**

Any Groupoid \((G, \cdot)\) is called a semi group when and only when binary operation \(\cdot\) satisfies the associative law
\[ x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad x, y, z \in G \]

**Monoid:**

Let \((G, \cdot)\) be any semi group in which there exists an element \(e\), to be called the identity in \(G\) such that that \(x \cdot e = x = e \cdot x\) for all elements \(x \in G\). If the relation \(x \cdot y = y \cdot x\) is valid for all \(x, y \in G\), then \(G\) is defined as the commutative and then the Monoid is called commutative Monoid.
The element \(e \in G\) satisfying the condition \(x \cdot e = x = e \cdot x\) for every element \(x \in G\) is unique and is called identity in the Monoid \(G\).

**Group:**

Any Monoid \((G, \cdot)\) is called a Group for each element \(g \in G\), there exists a unique element, denoted by the symbol \(g^{-1} \in G\), such that
\[ g \cdot g^{-1} = g^{-1} \cdot g = e \quad \text{where } e \text{ is the identity in the Monoid } (G, \cdot). \]
Let \((G, \cdot)\) be a Group such that \(x \cdot y = y \cdot x\) for every \(x, y \in G\), then the Group is called **Abelian or Commutative Group**.
1.3.3 Multiplicative Inverse Numbers

Inverse:

In mathematics, a multiplicative inverse for a number \( x \), denoted by \( \frac{1}{x} \) or \( x^{-1} \), is a number which when multiplied by \( x \) yields the multiplicative identity, 1. The multiplicative inverse of \( x \) is also called the reciprocal of \( x \). The multiplicative inverse of a fraction \( \frac{p}{q} \) is \( \frac{q}{p} \).

Relatively prime:

A pair of positive integers is said to be relatively prime if their greatest common divisor is 1. 3 and 5 are relatively prime because \( \gcd(3, 5) = 1 \). 4 and 15 are relatively prime because \( \gcd(4, 15) = 1 \). But, 6 and 33 are not relatively prime because \( \gcd(6, 33) = 3 \).

Multiplicative Inverse:

Any positive integer that is less than \( n \) and relatively prime to \( n \) has a multiplicative inverse modulo \( n \). This is a consequence of the Euclidean algorithm. Any positive integer that is less than \( n \) and not relatively prime to \( n \) does not have a multiplicative inverse modulo \( n \). \( \gcd(15, 26) = 1 \); 15 and 26 are relatively prime. Therefore, 15 has a multiplicative inverse of modulo 26.
1.3.3 Tribes of Gaussian Farey Fractions

**Tribes of Farey Fractions**

Farey sequences are named after the British geologist John Farey, Sr., whose letter about these sequences was published in the Philosophical Magazine in 1816. Farey conjectured that each term in a Farey sequence is the mediant of its neighbors — however, so far as is known, he did not prove this property. Farey's letter was read by Cauchy, who provided a proof in his Exercises de mathématique, and attributed this result to Farey. In fact, another mathematician, C. Haros, had published similar results which were almost certainly not known either to Farey or to Cauchy. Thus it was a historical accident that linked Farey's name with these sequences.

In mathematics, a Farey sequence of order $n$ is the sequence of completely reduced fractions between 0 and 1 which, when in lowest terms, have denominators less than or equal to $n$, arranged in order of increasing size. Each Farey sequence starts with the value 0, denoted by the fraction $0/1$, and ends with the value 1, denoted by the fraction $1/1$ (although some authors omit these terms).

The Farey sequence $F_n$ for any positive integer $n$ is the set of irreducible rational numbers $\frac{a}{b}$ with $0 < a < b \leq n$ and $(a, b) = 1$ arranged in increasing order, the first few are -
The Farey sequence is a well-known concept in number theory, whose exploration has lead to a number of interesting results.

**Theorem 1:**

If \( \frac{a}{b} \) and \( \frac{c}{d} \) are consecutive fractions in the \( n^{th} \) row with \( \frac{a}{b} \) to the left of \( \frac{c}{d} \) then \( cb - ad = 1 \)

**Theorem 2:**

If \( \frac{a}{b} \) and \( \frac{c}{d} \) are consecutive fractions. Then among all the rational fractions with values between them \( \frac{a + c}{b + d} \) is the unique fraction with smallest denominator.
**Definition 1:** Farey Sequence of order n

The sequence of all reduced with denominator not exceeding $n$, listed in order of their size is called the Farey sequence of order $n$.

**Theorem 3:** Rational approximation

If $\frac{a}{b}$ and $\frac{c}{d}$ Farey fractions of order $n$ such that no other Farey fraction of order $n$ lies between them then

$$\left| \frac{a}{b} - \frac{a+c}{b+d} \right| = \frac{1}{b(b+d)} \leq \frac{1}{b(n+1)}$$

And

$$\left| \frac{c}{d} - \frac{a+c}{b+d} \right| = \frac{1}{d(b+d)} \leq \frac{1}{d(n+1)}$$

**Tribes of Gaussian Farey fractions**

M. Nagaraj and Srinivas Murthy [NAG89] have associated the characteristic equation to a Farey fraction and defined the fundamental solutions. H. Chandrashekhar and M. Nagaraj [CHND94] have defined Gaussian Farey Fractions and found the solution for Gaussian Farey Fractions and they have studied the algebraic structures of these tribes.
Let \( \frac{\alpha}{\beta} \) be a Gaussian Farey Fraction and let

\[
\beta \epsilon - \alpha \eta = 1
\]

be its characteristic equation where \( \alpha = a + i \, b \) and \( \beta = c + i \, d \).

Then \(-b, -d\) and \((-a, -c)\) are fundamental solutions of the characteristic equation. The general solution of the characteristic equation using fundamental solution

\[
(-b, -d) \quad \text{is} \quad (-b + \lambda \alpha, -d + \lambda \beta).
\]

Where \( \text{N} (-b + \lambda \alpha) < \text{N} (-d + \lambda \beta) \) and

\[
(-b + \lambda \alpha) \quad \text{and} \quad (-d + \lambda \beta) \quad \text{are relatively prime.}
\]

The definition of tribe \( T_{\alpha/\beta} \) of the Gaussian Farey Fraction \( \frac{\alpha}{\beta} \) given by the set

\[
T_{\alpha/\beta} = \left\{ \frac{-b + \lambda \alpha}{-d + \lambda \beta} \mid \forall \lambda \in J[i] \right\}
\]

is called tribe of \( \frac{\alpha}{\beta} \).

And the real fractions \( \frac{a}{c} \) and \( \frac{b}{d} \) are Farey fractions.

Algebraic Structures of a tribe \( T_{\alpha/\beta} \):

Let \( T_{\alpha/\beta} = \left\{ \frac{-z_0 + \lambda \alpha}{-w_0 + \lambda \beta} \mid \forall \lambda \in J[i] \right\} \) be the tribe of \( \frac{\alpha}{\beta} \).
Let \[ \begin{aligned} \frac{-z_0 + \lambda \alpha}{-w_0 + \lambda \beta} \end{aligned} \] and \[ \begin{aligned} \frac{-z_0 + \mu \alpha}{-w_0 + \mu \beta} \end{aligned} \]
be any two elements of the tribe \( T_{\alpha/\beta} \), where \( \lambda \) and \( \mu \in J[i] \).

The two binary operations \( \otimes \) and \( \oplus \) on tribe \( T_{\alpha/\beta} \) are defined by

\[ \begin{aligned} \left\{ \frac{-z_0 + \lambda \alpha}{-w_0 + \lambda \beta} \right\} \otimes \left\{ \frac{-z_0 + \mu \alpha}{-w_0 + \mu \beta} \right\} &= \left\{ \frac{-z_0 + (\lambda \mu) \alpha}{-w_0 + (\lambda \mu) \beta} \right\} \end{aligned} \]

And

\[ \begin{aligned} \left\{ \frac{-z_0 + \lambda \alpha}{-w_0 + \lambda \beta} \right\} \oplus \left\{ \frac{-z_0 + \mu \alpha}{-w_0 + \mu \beta} \right\} &= \left\{ \frac{-z_0 + (\lambda + \mu) \alpha}{-w_0 + (\lambda + \mu) \beta} \right\} \]

\( \{ T_{\alpha/\beta}, \oplus, \otimes \} \) is a unitary commutative integral domain, which is isomorphic to the domain of Gaussian integers.