

MATHEMATICS OF SECURE COMMUNICATION

A project report submitted to St. Joseph's College (Autonomous)

Devagiri, Calicut

Affiliated to University of Calicut

IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD

OF THE DEGREE OF

BACHELOR OF SCIENCE(B.S.c)

IN COMPUTER SCIENCE & MATHEMATICS(DOUBLE MAIN)

By

ANASWARA PYARILAL

DVAWSCM020



DEPARTMENT OF MATHEMATICAL SCIENCES

ST.JOSEPH'S COLLEGE (AUTONOMOUS)

DEVAGIRI, CALICUT - 08

2022-2025



ST. JOSEPH'S COLLEGE (AUTONOMOUS)
DEVAGIRI, CALICUT

MATHEMATICS OF SECURE COMMUNICATION

Report of the project submitted to St. Joseph's College (Autonomous), Devagiri, Calicut

Affiliated to the University of Calicut

ANASWARA PYARILAL

DVAWSCM020

Programme: Bachelor of Science (B.Sc.)
in Computer Science and Mathematics (Double main)
Semester: VI

DEPARTMENT OF MATHEMATICAL SCIENCES

March 2025

Principal

Head of the Department

Supervisor

College Seal

CERTIFICATE

This is to certify that the project report titled

MATHEMATICS OF SECURE COMMUNICATION

is a bonafied record of work done by

ANASWARA PYARILAL

DVAWSCM020

at St.Joseph's College (Autonomous), Devagiri, Calicut, in partial fulfillment of the requirements for the award of the degree of Bachelor of Science (B.Sc.)Computer Science and Mathematics(Double Main) during the academic year 2024-2025.

Internal Guide

Head of the Department

Internal Examiner

External Examiner

DECLARATION

I hereby declare that the project entitled **MATHEMATICS OF SECURE COMMUNICATION** has been undertaken by me for the award of the degree of Bachelor of Science (B.Sc.) in Computer Science and Mathematics(Double Main). I have completed this project under the guidance of **Ms.Sandra** , Department of Mathematical Sciences, St. Joseph's College (Autonomous), Devagiri, Calicut.

ANASWARA PYARILAL

DVAWSCM020

Place: Calicut

Date: 17.03.2025

ACKNOWLEDGEMENT

I express my deep sense of gratitude to my supervisor **Ms.Sandra R**, Assistant Professor, Department of Mathematical Sciences, St. Joseph's College (Autonomous), Devagiri, Calicut, for the inspiring advice, timely help, and constructive suggestions offered during the entire period of the project.

I place on record my indebtedness to **Dr. Bobby Jose**, Principal, St. Joseph's College (Autonomous), Devagiri, Calicut, for providing necessary facilities for developing my project.

I am also grateful to **Dr. Shija Gangadharan**, Head of the Department of Mathematical Sciences, St. Joseph's College (Autonomous), Devagiri, Calicut, for constructive suggestions and help during my project work. Also, the help rendered by all other faculty members of the Department is thankfully acknowledged.

I also extend my sense of indebtedness to the Librarian, St. Joseph's College (Autonomous), Devagiri, Calicut, and other members in the library for their timely help.

The acknowledgment will not be complete without expressing thanks to my family and friends who filled me with their optimism.

Above all, I am thankful and bow in gratitude to God Almighty, whose gracious blessings gave me the required strength and devotion for the completion of this work.

ANASWARA PYARILAL

Contents

Introduction to Cryptography	7
0.1 History of Cryptography	8
0.2 Evolution of cryptography	9
0.3 Types of Cryptography	10
Chapter 1: Cryptography	13
1.1 Basis Notions	13
1.2 Some Simple Cryptosystems	14
1.3 Some Examples of Secrecy Systems	20
Chapter 2: Graph theory in Cryptography	23
2.1 Introduction	23
2.2 Proposed Algorithm	24
2.3 Encryption Algorithm	24
2.4 Decyption Algorithm	25
2.5 Illustration	25
Chapter 3: Applications of Cryptography	32
3.1 WhatsApp Encryption	32
3.2 Network Security Using Graph Theory in Cryptography	34
Conclusion	36
References	37

Introduction to Cryptography

Cryptography is the science of securing information and communication through mathematical techniques. It is used to protect data from unauthorized access, ensuring confidentiality, integrity, and authenticity. By transforming readable data (plaintext) into an unreadable format (ciphertext) through encryption, cryptography helps prevent unauthorized access. Decryption allows authorized users to convert ciphertext back into plaintext using a specific key.

One of the key reasons cryptography is essential is its role in modern security systems. It enables secure online transactions, protects sensitive information such as passwords and financial data, and ensures the authenticity of digital communications. Without cryptography, data transmitted over the internet would be vulnerable to interception and manipulation.

The Concise Oxford English Dictionary defines cryptography as “the art of writing or solving codes.” This is historically accurate, but does not capture the current breadth of the field or its present-day scientific foundations. The definition focuses solely on the codes that have been used for centuries to enable secret communication. But cryptography nowadays encompasses much more than this: it deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic auctions and elections, digital cash, and more. Without attempting to provide a complete characterization, we would say that modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.

Cryptography is widely used in various fields, including secure messaging, online banking, digital signatures, and blockchain technology. It plays a fundamental role in cybersecurity, making it a critical component of digital life today. As technology advances, cryptographic methods continue to evolve to counter new threats and challenges, ensuring the safety of digital information in an increasingly interconnected world.

0.1 History of Cryptography

The history of cryptography began thousands of years ago. The art of cryptography is considered to be born along with the art of writing. From an early age, humans had two inherent needs: to share information and to communicate selectively. These needs set off the rise of the art of coding in such a way that only intended people can have access to the information. Unauthorized people can't extract any information, even if the scrambled message is accessed by them.

The first known invented cryptography was found in 1900 BC in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt. Hieroglyphs carved into monuments from Egypt's Old Kingdom (4500+ years ago) is the earliest known use of cryptography found in non-standard forms. In most of the major early civilizations, evidence of some use of cryptography has been identified.

"Risalah fi istikhraj al-mu'amma" is the book written by Al-Kindi (a manuscript for the Deciphering of Cryptographic Messages), in 850 CE. He was a pioneer in cryptanalysis and cryptology and devised new methods of breaking ciphers, including the frequency analysis method. Until the development of the polyalphabetic cipher, essentially all ciphers remained vulnerable to the cryptanalytic technique of frequency analysis.

Leon Battista Alberti explained the polyalphabetic cipher around the year 1467, for which he was called the "father of Western Cryptology". Kautilya wrote a treatise on statecraft named "Arthashastra," which describes the assignment given to spies in secret writing. Edgar Allan Poe used systematic methods to solve ciphers in the 1840s. He placed a notice of his abilities in the Philadelphia paper, inviting submissions of ciphers, of which he proceeded to solve almost all. It created a public stir for some months. Later, he wrote an essay on methods of cryptography, which was useful in providing introductions for novice British cryptanalysts working with codes and German ciphers during World War I.

The Teletype cipher, introduced by Gilbert Vernam in 1917, combined a paper tape with the plaintext message to produce ciphertext. This led to the development of electromechanical devices as cipher machines. Mechanical and electromechanical machines were widely

used during World War II, although-where such machines were impractical-manual systems continued in use. Nazi Germany widely used the Enigma machine, where as SIGABA was used by British army. The earlier invented method of cryptography is a Roman method popularly known as Ceaser shift method. Around 100 BC, Julius Caesar used a form of encryption, which was later known as Caesar cipher to convey secret message to army generals in war front. During the beginning of the 19th, Century Hebern developed an electro mechanical contraption which was known as Hebern rotor machine. A single router was used in the encryption in which the secret key is embedded in a rotating disc. Later the Enigma machine was invented by a German Engineer Arthur Scherbius during the end of World War I which used three or more rotators for its functioning. This Enigma machine was heavily used by the German forces during the Second World War. In the early 1970s, due to the high demand on encryption by the customers, IBM formed a group “Crypto group” headed by Horst-Feistel and they have the signed a site for called Lucifer. Eventually Lucifer was accepted worldwide and was called DES. Further in 2000, the AES was developed.

0.2 Evolution of Cryptography

After the European Renaissance, various Italian and papal states led the rapid proliferation of cryptographic techniques. Attack techniques and various analysis were researched in this era to break the secret codes. Coding techniques has improved such as Vigenere coding came in to existence in the 15 th century, which offered moving letters in messages with a number of variable places instead of moving them the same number of places.

A technique for encrypting alphabetic text is the Vigenere Cipher. It employs a straightforward method of polyalphabetic substitution. Any substitution-based encryption that employs numerous substitution alphabets is referred to as a polyalphabetic cypher. With the Vigen‘ere square or Vigen‘ere table, the original text is encrypted. The table has the 26 potential Caesar Ciphers written out 26 times in various rows, with each alphabet shifting cyclically to the left in comparison to the previous alphabet. The cipher switches to an alphabet from one of the rows at various stages of the encryption process. Each point’s

alphabet is determined by a keyword that appears repeatedly.

After 19th century, cryptography approaches to encryption to the more sophisticated art and science of information security. At the close of World War I, German engineer Arthur Scherbius created the Enigma machine. There were several distinct Enigma models made, but the German military versions with a plugboard were the most intricate. There were several distinct Enigma models made, but the German military versions with a plugboard were the most intricate. Models from Italy and Japan were also in use. Enigma gained widespread recognition in the military after being adopted (in a somewhat modified version) by the German Navy in 1926 and the German Army and Air Force shortly after. German military strategy prior to World War I focused on quick, mobile units and blitzkrieg tactics, which rely on radio transmission for command and coordination. Radio signals had to be encrypted securely since enemies would probably try to intercept them. The Enigma machine satisfied that need by being small and portable.

In the period of World War II, cryptography and cryptanalysis became excessively mathematical. Government organizations, military units, and some corporate houses started adopting the applications of cryptography. They use cryptography as a guard their secrets from others. The arrival of computers and the internet has brought effective cryptography within the reach of common people.

0.3 Types of Cryptography

Cryptography is broadly classified into two categories: symmetric key cryptography and asymmetric key cryptography.

0.3.1 Symmetric Key Cryptography

The cryptographic method in which the same key is used for both encryption and decryption of information is called symmetric key cryptography. Therefore, the sender and the receiver will have access to the key. Since both parties have access to the secret key, it is considered a major drawback of symmetric key encryption compared to public key encryption.

Symmetric key cryptography is commonly used in today's internet. AES and DES

are common encryption algorithms used in symmetric key cryptography. It is faster than asymmetric key cryptography.

Symmetric key encryption either uses a stream cipher or a block cipher:

- **Stream Cipher:** Encrypts digits or letters of a message one at a time.
- **Block Cipher:** Considers bits as a single unit and encrypts them as a whole.

Some applications of symmetric key cryptography include payment systems, random number generation, and hashing.

0.3.2 Asymmetric Key Cryptography

Asymmetric key cryptography is a public key cryptographic scheme that requires two different keys. One key is used for the encryption process, and the other is used for the decryption of the ciphertext.

One of the keys in asymmetric key encryption is a public key, which is accessible to the public, while the other key is kept private and is known as the private key. Asymmetric key encryption is also known as public key cryptography.

Advantages:

- Non-reliance on a single point of failure for the key.
- Increased data security.

Drawbacks:

- Slower encryption speed due to longer key lengths.

Applications of asymmetric key cryptography include digital signatures, TLS/SSL handshakes, and cryptocurrency.

0.3.3 Hashing

Hashing is the process of transforming any given key or a string of characters into another value. Implementing hash tables is one of the most well-known applications of hashing.

How it works:

- Value and key pairs are stored in a list that can be accessed using a hash table's index.
- The hash function maps keys to the size of the table since value and key pairs are infinite.
- The index for a given element is then changed to a hash value.

Hashing uses functions or algorithms to map object data to a representative integer value. A hash can then be used to narrow down searches when locating items in the object data map.

Chapter 1

Cryptography

1.1 Basic notions

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the **plaintext** and the disguised message is called **ciphertext**. The plaintext and ciphertext are written in some alphabet(usually, but not always, they are written in the same alphabet) consisting of a certain number N of letters. The term “letter” (or “character”) can refer not only to the familiar A-Z, but also to numerals, blanks, punctuation marks, or any other symbols that we allow ourselves to use when writing the messages(if we don’t include a blank, for example, then all of the words are run together, and the messages are harder to read). The process of converting a plaintext to a ciphertext is called enciphering or encryption, and the reverse process is called deciphering or decryption.

Example: Assume for example that Bob wants to send a message to Alice in such a way that Eve – who reads/listens/spies the communication of Alice and Bob – cannot understand the message (Alice, Bob and Eve are the usual participants of the cryptographic setup). The scheme of the solution is the following. Bob sends through the communication something else than his original message. Eve can read only this something else. Alice knows how this something else should be understood to get the original message.

1.2 Some simple cryptosystems

The plaintext and ciphertext are broken up into ‘message units’. A message unit might be a single letter, a pair of letters(digraph), a triple of letters(trigraph) or a block of 50 letters. An enciphering transformation is a function that takes any plaintext message unit and gives us a ciphertext message unit. In other words, it is a map f from the set P of all possible plaintext message units to the set C of all possible ciphertext message units. We shall always assume that f is a 1-to-1 correspondence, i.e., given a ciphertext message unit, there is one and only one plaintext message unit for which it is the encryption. The deciphering transformation is the map f^{-1} which goes back and recovers the plaintext from the ciphertext. We can represent the situation schematically by the diagram

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P$$

Any such set-up is called a ‘cryptosystem’. The first step in inventing a cryptosystem is to “label” all possible plaintext message units and all possible ciphertext message units by means of mathematical objects from which functions can be easily constructed. These objects are often simply the integers in some range. For example, if our plain text and ciphertext message units are single letters from the 26-letter alphabet A-Z, then we can label the letters using the integers 0,1, 2, ...,25, which we call their ‘numerical equivalents’. Therefore, in place of A we write 0,B we write 1,in place of X as 23,Y as 24, Z as 25, etc. As another example, if our message units are digraphs (i.e. pair of letters) in the 27-letter alphabet consisting of A-Z and a blank, we might first let the blank have numerical equivalent 26(one beyond Z), and then label the digraph whose two letters correspond to $x, y \in \{0, 1, 2, \dots, 26\}$ by the integer $[27x + y] \in \{0, 1, \dots, 728\}$.

If we view the individual letters as digits to the base 27 and we view the digraph as a 2-digit integer to that base. For example, the digraph “MY” corresponds to the integer $27 \cdot 12 + 24 = 348 \in \{0, 1, \dots, 728\}$.

In similar way, if we were using trigraphs as our message units, we could label them by integers $[729x + 27y + z] \in \{0, 1, \dots, 19682\}$. In general, we can label blocks of k letters

in an N -letter alphabet by integers between 0 and $N^k - 1$ by regarding each such block as a k -digit integer to the base N .

In some situations, one might want to label message units using other mathematical objects besides integers—for example, vectors or points on some curve. But we shall only consider integers throughout this section. Let us start with the case when we take a message unit (of plaintext or ciphertext) to be a single letter in an N -letter alphabet labeled by the integers $0, 1, 2, \dots, N - 1$. Then by definition, an enciphering transformation is a rearrangement of these N integers.

1.2.1 Shift Transformations

Suppose we are using the 26-letter alphabet A-Z with numerical equivalents 0-25. Let the letter $P \in \{0, 1, 2, \dots, 25\}$ stand for a plaintext message unit. Define a function f from the set $\{0, 1, \dots, 25\}$ to itself by the rule,

$$f(P) = \begin{cases} P + 3, & \text{if } x \leq 22 \\ P - 23, & \text{if } x > 22 \end{cases}$$

In other words, f simply adds 3 modulo 26: $f(P) \equiv P + 3 \pmod{26}$. Thus, with this system, to encipher the word “YES” we first convert to numbers: 24 4 18, then add 3 modulo 26: 1 7 21, then translate back to letters: “BHV”. To decipher a message, one subtracts 3 modulo 26. For example, the ciphertext “ZKB” yields the plaintext “WHY”. This cryptosystem was apparently used in ancient Rome by Julius Caesar, who supposedly invented it himself.

The example given above can be generalized as follows. Suppose that we are using an N -letter alphabet with numerical equivalents $0, 1, 2, \dots, N-1$. Let b be a fixed integer.

By a shift transformation, we mean that the enciphering function f defined by the rule is $C = F(P) \equiv P + b \pmod{N}$. Julius Caesar cryptosystem was the case $N=26$, $b=3$.

To decipher a ciphertext message unit $C \in \{0, 1, 2, \dots, N - 1\}$, we simply compute $P = f^{-1}(C) \equiv C - b \pmod{N}$.

1.2.2 Cryptanalysis

Now suppose that you are not aware of the enciphering and deciphering information but you would nevertheless like to be able to read the coded messages. This is called breaking the code, and the science of breaking codes is called cryptanalysis.

In order to break a cryptosystem, one needs two types of information. The first is the general nature (that is, the structure) of the system. For example, suppose that we know that the cryptosystem uses a shift transformation on single letters of the 26-letter alphabet A-Z with numerical equivalents of 0-25, respectively. The second type of information is knowledge of a specific choice of certain parameters connected with the given type of cryptosystem. In our example, the second type of information that one needs to know is the choice of the shift parameter "b". Once you have that information, you can encipher and decipher it by formulas $C \equiv P + b \pmod{N}$ and $P \equiv C - b \pmod{N}$.

We shall always assume that the general structural information is already known. In practice, cryptographic users often have equipment for enciphering and deciphering that is constructed to implement only one type of cryptosystem. Over a period of time the information about what type of system they are using might leak out. To increase their security, therefore, they frequently change the choice of parameters used with the system. For example, suppose that two users of the shift cryptosystem are able to meet once a year. At that time, they agree on a list of 52 choices of the parameter b, one for each week of the coming year. The parameter b (more complicated cryptosystems usually have several parameters) is called a key, or more precisely, the enciphering key.

Example. So suppose that we intercept the message "FQOCUDEM", which we know was enciphered using a shift transformation on single letters of the 26-letter alphabet. It remains for us to find the b. One way to do this is by frequency analysis. This works as follows. Suppose that we have already intercepted a long string of ciphertext, say several hundred letters. We know that "E" is the most frequently occurring letter in the English language. So it is reasonable to assume that the most frequently occurring letter in the ciphertext is the encryption of E. Suppose that we find that "U" is the most frequently occurring character in the ciphertext. That means that the shift takes in the ciphertext. That

means that the shift takes “E” = 4 to “U” = 20, i.e., $20 \equiv 4 + b \pmod{26}$, so that $b = 16$. To decipher the message, then, it remains for us to subtract 16 (working modulo 26) from the numerical equivalent of “FQOCUDEM”:

$$\text{“FQOCUDEM”} = 5 \quad 16 \quad 14 \quad 2 \quad 20 \quad 3 \quad 4 \quad 12$$

$$\rightarrow 15 \quad 0 \quad 24 \quad 12 \quad 4 \quad 13 \quad 14 \quad 22 = \text{“PAYMENOW”}.$$

1.2.3 Affine Transformation

In the case of a shift encryption of single letters of a 26-letter alphabet, it is not even necessary to have a long string of ciphertext to find the most frequently occurring letter. After all, there are only 26 possibilities for b , and one can simply run through all of them. Most likely, only one will give a message that makes any sense, and that b is the enciphering key.

Thus, this type of cryptosystem is too simple to be much good. It is too easy to break.. An improvement is to use a more general type of transformation of Z/NZ , called an affine map: $C \equiv aP + b \pmod{N}$, where a and b are fixed integers (together they form the enciphering key). For example, working again in the 26-letter alphabet, if we want to encipher our message “PAYMENOW” using the affine transformation with enciphering key $a=7, b=12$, we obtain: $15 \ 0 \ 24 \ 12 \ 4 \ 13 \ 14 \ 22 \rightarrow 13 \ 12 \ 24 \ 18 \ 14 \ 25 \ 6 \ 10 = \text{“NMYSOZGK”}$

To decipher a message that was enciphered by means of the affine map $C \equiv aP + b \pmod{N}$, one simply solves for P in terms of C , obtaining $P \equiv a'C + b' \pmod{N}$ where a' is the inverse of a modulo N and b' is equal to $-a^{-1}b'$. Note that this works only if $\text{g.c.d}(a, N)=1$; otherwise we cannot solve for P in terms of C . If $\text{g.c.d}(a, N) > 1$, then it is easy to see that more than one plaintext letter will give the same ciphertext, so that we cannot uniquely recover the plaintext from the ciphertext. For example, if we were to encipher the message “PAYBACK” by means of the affine map $C \equiv aP + b \pmod{N}$ where $a = 10$, $b = 12$, again in the 26-letter alphabet. Here $\text{gcd}(a, N) = 2 > 1$ and we observe that the plaintext units “P” and “C” correspond to ciphertext unit “G”. By definition, that is not an enciphering transformation: we always require that the map be 1-to-1, i.e., that the plaintext

be uniquely determined from the ciphertext.

To summarize, an affine cryptosystem in an N -letter alphabet with parameters $a \in (Z/NZ)^*$ and $b \in (Z/NZ)$ consists of the rules:

$$C \equiv aP + b \pmod{N}, \quad P \equiv a'C + b' \pmod{N},$$

Where $a' \equiv a^{-1} \pmod{(Z/NZ)^*}$, $b' \equiv -a^{-1}b$.

As a special case of the affine cryptosystems we can set $a = 1$, thereby obtaining the shift transformations. Another special case is when $b = 0$: $P \equiv aC \pmod{N}$, $C \equiv a^{-1}P \pmod{N}$. The case $b = 0$ is called a linear transformation, meaning that the map takes a sum to a sum, i.e., if C_1 is the encryption of P_1 and C_2 is the encryption of P_2 , then $C_1 + C_2$ is the encryption of $P_1 + P_2$ (where, of course, we are adding modulo N).

Now suppose that we know that an intercepted message was enciphered using an affine map of single letters in an N -letter alphabet. We would like to determine the enciphering key a, b so that we can read the message. We need to know two bits of information to do this.

Example 1. Still working in our 26-letter alphabet, suppose that we know the most frequently occurring letter of ciphertext is “K”, and the second most frequently occurring letter is “D”. It is reasonable to assume that these are the encryptions of “E” and “T”, respectively, which are the two most frequently occurring letters in the English language. Thus, replacing the letters by their numerical equivalents and substituting for P and C in the deciphering formula, we obtain:

$$10a' + b' \equiv 4 \pmod{26}$$

$$3a' + b' \equiv 19 \pmod{26}.$$

We have two congruences with two unknowns, a' and b' . The quickest way to solve is to subtract the two congruences to eliminate b' . We obtain $7a' \equiv 11 \pmod{26}$, and $a' \equiv 7^{-1}11 \equiv 9 \pmod{26}$. Finally, we obtain b' by substituting this value for a' in one of the

congruences:

$$b' \equiv 4 - 10a' \equiv 18 \pmod{26}.$$

So, messages can be deciphered by means of the formula

$$P \equiv 9C + 18 \pmod{26}.$$

Example 2. You are trying to cryptanalyze an affine enciphering transformation of single-letter message units in a 37-letter alphabet. This alphabet includes the numerals 0-9, which are labeled by themselves (i.e., by the integers 0-9). The letters A-Z have numerical equivalents 10-35, respectively, and blank=36. You intercept the ciphertext **"OH7F86BB46R3627O266BB9"** (here the O's are the letter "oh", not the numeral zero). You know that the plaintext ends with signature "007". What is the message?

From the given information, we know that "B" is the encryption for "0" (zero), and "9" is the encryption for "7".

Thus, replacing the letters by their numerical equivalents and substituting for P and C in the deciphering formula, we obtain:

$$0 \equiv 11a' + b' \pmod{37}$$

$$7 \equiv 9a' + b' \pmod{37}$$

Subtracting the two congruences to eliminate b' , we obtain:

$$2a' \equiv -7 \pmod{37}, \quad \text{and} \quad a' \equiv (-7)2^{-1} \equiv 15 \pmod{37}.$$

Finally, we obtain b' by substituting this value for a' in one of the congruences:

$$b' \equiv 20 \pmod{37}.$$

Now, we can decipher the message by the formula $P \equiv 15C + 20 \pmod{26}$, which reads as follows: **AGENT_006_IS_DEAD__007**.

1.3 Some Examples of Secrecy Systems

1.3.1 Simple Substitution Cipher

In this cipher, each letter of the message is replaced by a fixed substitute, usually also a letter. Thus, the message, $M = m_1m_2m_3m_4 \dots$, where m_1, m_2, m_3, \dots are the successive letters, becomes:

$$E = e_1e_2e_3e_4 \dots = f(m_1)f(m_2)f(m_3)f(m_4) \dots$$

Where the function $f(m)$ is a function with an inverse. The key is a permutation of the alphabet (when the substitutes are letters). An example key is: **Plain alphabet:**

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher alphabet:

PHQGIUMEAYLNOFDXJKRCVSTZWB.

An example encryption using the above key:

Plaintext:

DEFEND THE EAST WALL OF THE CASTLE

Ciphertext:

GIUIFG CEI IPRC TPNN DU CEI QPRCNI.

1.3.2 Transposition (Fixed Period d)

The message is divided into groups of length d and a permutation applied to the first group, the same permutation to the second group, etc. The permutation is the key and can be represented by a permutation of the first d integers. Thus, for $d = 5$, we might have 2 3 1 5 4 as the permutation. This means that: $m_1m_2m_3m_4m_5m_6m_7m_8m_9m_{10} \dots$ becomes

$m_2m_3m_1m_5m_4m_7m_8m_6m_{10}m_9 \dots$ Sequential application of two or more transpositions will be called compound transposition. If the periods are d_1, d_2, \dots, d_n , then the result is a transposition of period d , where d is the least common multiple of d_1, d_2, \dots, d_n .

1.3.3 Vigenere Cipher

The most famous example of a polyalphabetic cipher (In a polyalphabetic cipher, a plaintext has more than one ciphertext equivalent) was published by the French cryptographer Blaise de Vigenere (1523-1596) in his *Traicté de Chiffres* of 1586.

To implement this system, the communicating parties agree on an easily remembered word or phrase. With the standard alphabet numbered from A=0 to Z=25, the digital equivalent of the keyword is repeated as many times as necessary beneath that of the plaintext message. The message is then enciphered by adding, modulo 26, each plaintext number to one immediately beneath it. The process may be illustrated with the keyword **READY**; whose numerical version is 17 04 00 03 24. Repetitions of this sequence are arranged below the numerical plaintext of the message

“ATTACK AT ONCE”

to produce the array

00	19	19	00	02	10	00	19	14	13	02	04
17	04	00	03	24	17	04	00	03	24	17	04

When the columns are added modulo 26, the plaintext message is encrypted as

17	23	19	03	00	01	04	19	17	11	19	08
----	----	----	----	----	----	----	----	----	----	----	----

or, converted to letters, “**RXTDAB ET RLTI**”. Notice that a given letter of plaintext is represented by different letters in the ciphertext. The double “T” in the word “**ATTACK**” no longer appears as a double letter when ciphered, while the ciphertext “R” first corresponds to “A” and then to “O” in the original message.

In general, any sequence of n letters with numerical equivalents b_1, b_2, \dots, b_i ($0 \leq b_i \leq 25$) will serve as the keyword. The plaintext message is expressed as successive blocks $P_1P_2\dots P_n$ of n two-digit integers P_i , and then converted to ciphertext blocks $C_1C_2\dots C_n$ by means of the congruences:

$$C_i \equiv P_i + b_i \pmod{26}, \quad 1 \leq i \leq n.$$

Decryption is carried out by using the relations:

$$P_i \equiv C_i - b_i \pmod{26}, \quad 1 \leq i \leq n.$$

1.3.4 Autokey Cipher

A Vigenere type system in which either the message itself or the resulting cryptogram is used for the “key” is called an autokey cipher. The encipherment is started with a “priming key” (which is the entire key in our sense) and continued with the message or cryptogram displaced by the length of the priming key as indicated below, where the priming key is “COMET”. The message used as key:

Message: SENDSUPPLIES...

Key: COMETSENDSUP...

Cryptogram: USZHLMTCOAYH...

The cryptogram used as key:

Message: SENDSUPPLIES...

Key: COMETUSZHLMT...

Cryptogram: USZHLOHOSTSZ...

Chapter 2

Graph theory in Cryptography

2.1 Introduction

Graph theory is the study of graphs, which are mathematical structures used to model pairwise relationships between objects. An undirected graph $G(V, E)$ consists of:

- V : The set of vertices.
- E : The set of edges.

A walk in which vertices are not repeated is called a **path**. A **cycle** is a nonempty trail in which only the first and last vertices are equal. A graph is called **complete** when every single vertex is connected to every other vertex in the graph. A graph can be represented mainly in two ways, the adjacency list and adjacency matrices. The representation of graph consisting of array of V list, one for each vertex is called adjacency list. The adjacency list for vertex V contains all adjacent vertices to it. The adjacency matrix representation consists of matrix $V = [g_{ij}]$

where for an un-weighted graph,

$$g_{ij} = \begin{cases} 1, & \text{if } (i, j) \in E \\ 0, & \text{otherwise} \end{cases}$$

and for a weighted graph,

$$g_{ij} = \begin{cases} w_{ij}, & \text{if } (i, j) \in E \\ NIL, & \text{otherwise} \end{cases}$$

A connected sub-graph which consist all vertices with minimum weight of edges required is called a spanning tree. A minimum spanning tree is a special kind of tree that minimizes the length (or weights) of the edges of the tree.

2.2 Proposed Algorithm

In this algorithm, as first step we represent each character of the message to be encrypted as the vertices of the graph. We keep adding vertices until we form a cyclic graph. By using a keyword, whose length is longer than the message, we encoded the message in such a way that each letter of the message would be converted to the number of letters between it and the corresponding letters of the keyword using the encoding table. Then the weight of each edge is calculated as the distance between the encoded character of the adjacent edges as in the message. If we get the weight as zero we represent it as 27 (which is the last index in the encoding table). Then each vertex in the graph is joined by edges to make the graph a complete graph. For every newly added edge, it has a sequence weight, starting from last index (28, 29, 30, . . .) . Add special character A to the starting character. A is encoded as the difference between the corresponding indexes of the remnant character in the keyword and the special character. Adjacency-matrix is constructed from this complete graph. After that Minimum Spanning Tree (MST) is constructed and represented as adjacency-matrix. Then replace the zero diagonal entries by 0,1,2,. . . . Adjacency-matrix of the complete graph is multiplied to the adjacency-matrix of MST. The resultant matrix is multiplied to the key matrix which gives the final matrix which is to be sent to the recipient.

2.3 Encryption Algorithm

- Add vertex for each character in the plain text to the graph.
- Vertices of each sequential character are joined by edges until we form a cyclic graph.

- Weight of each edge is calculated as mentioned above.
- Add more edges to form a complete graph M_1 .
- Add special character A to the starting character. A is encoded as the difference between the corresponding indexes of the remnant character in the keyword and the special character A.
- Construct adjacency-matrix of M_1
- Then find the Minimum Spanning Tree and its adjacency-matrix M_2
- Then we replace the zero diagonal entries in M_2 matrix by 0,1,2.
- Then we multiply matrices M_1 by M_2 to get M_3 .
- After that the multiply M_3 by a predefined shared key K to form C, the cipher text.

2.3.1 Decryption Algorithm

- The receiver computes M_3 by using the inverse form of shared key K^{-1} .
- Then compute M_2 by using the inverse form of M_1 .
- Then we represent M_2 as a graph.
- Then compute the original text from the minimum spanning tree using the keyword.

2.4 Illustration

Lets see how graph is illustrated .

Let "COLD" be the message which has to be send to the receiver by sender. As the first step is to represent each character of the message to a vertex.

As shown in Fig. 2.

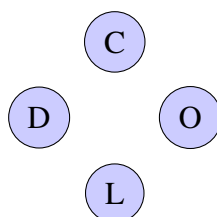


Fig.2 Represent each character as vertex

Then, connect pair of sequential characters by an edge to form a cyclic graph.

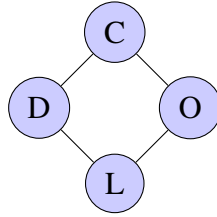


Fig. 3. Graphical representation of plain text to be encrypted

Then using a keyword and encoding table (Table 1) the given message is encoded as shown below.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Table 2.1: Encoding table

Let the keyword be SECRET Then each character in the message to be encrypted is converted to a number, which is the difference between the numbers representing the corresponding letters of the message to be encrypted and the keyword, from Table 1.

Message: C O L D Encoded message: 16 -10 -9 14 Then weight of each edge is calculated as the difference between the letters representing the end vertices of that edge. So, the edge connecting vertex C with vertex O has the weight as the distance between the two letters as follows:

$$\begin{aligned}
 \text{Distance} &= \text{code (O)} - \text{code (C)} \\
 &= 10 - 16 \\
 &= -6
 \end{aligned}$$

Proceeding as above, we get the graph as in Fig. 4.

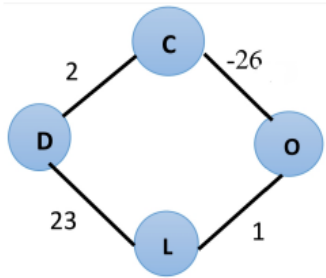


Fig. 4. Graphical representation of the message COLD

As next step, we add edges to fig 4 till we get a complete graph. Every newly added edge has a weight choosing from the sequence 28, 29, 30. . . .

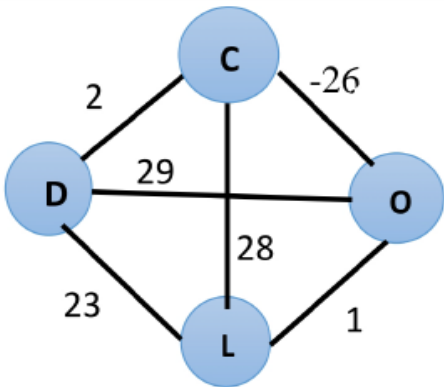


Fig. 5. Complete plain graph

Here we add a special character A before the character C to indicate that C is the first character of the message as shown in Fig .6.

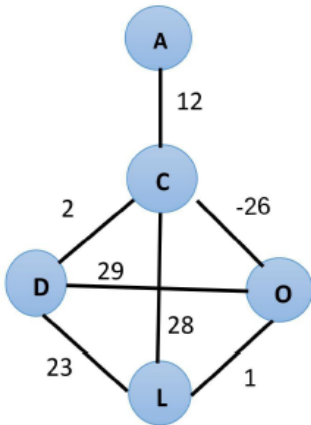


Fig. 6. Complete plain graph with a special character

The complete plain graph in Fig. 6. is represented as a matrix M_1 .

$$M_1 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 0 & -26 & 28 & 2 \\ 0 & -26 & 0 & 1 & 29 \\ 0 & 28 & 1 & 0 & 23 \\ 0 & 2 & 29 & 23 & 0 \end{bmatrix}$$

Then we find the minimum spanning tree (MST) as shown in Fig. 7.

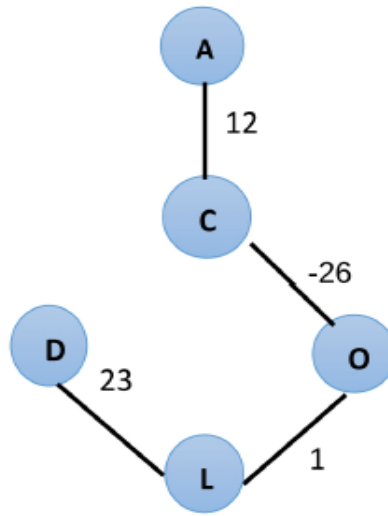


Fig. 7. Minimum Spanning Tree Graph

Adjacency-matrix M_2 of MST is determined, M_2 ,

$$M_2 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 0 & -26 & 0 & 0 \\ 0 & -26 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 23 \\ 0 & 0 & 0 & 23 & 4 \end{bmatrix}$$

Then we change the diagonal entries of M_2 by 0, 1, 2, 3, 4.

So, M_2 modified to M_2

$$= \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 1 & -26 & 0 & 0 \\ 0 & -26 & 2 & 1 & 0 \\ 0 & 0 & 1 & 3 & 23 \\ 0 & 0 & 0 & 23 & 4 \end{bmatrix}$$

After that, we multiply matrix M_1 by M_2 to form M_3 .

$$M_1 \times M_2 = M_3 = \begin{bmatrix} 144 & 12 & -312 & 0 & 0 \\ 0 & 820 & -24 & 104 & 652 \\ -312 & -26 & 677 & 670 & 139 \\ 336 & 2 & -726 & 530 & 92 \\ 24 & -752 & 29 & 98 & 529 \end{bmatrix}$$

Now, we use the shared-key K to encrypt M_3 .

Let $K =$

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

So, the cipher text $C = KM_5 =$

$$\begin{bmatrix} 192 & 56 & -356 & 1402 & 1412 \\ 48 & 44 & 44 & 1402 & 1412 \\ 48 & -776 & -20 & 1298 & 760 \\ 360 & -750 & -697 & 628 & 621 \\ 24 & -752 & 29 & 98 & 529 \end{bmatrix}$$

Now the data to be sent is C and M_1 .

In the receiver side, we get M_3 by multiplying the cipher text with the inverse of the shared key K^{-1} .

Then M_2 is calculated by multiplying M_3 by M_1^{-1} .

$$M_2 = M_3 M_1^{-1} = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 1 & -26 & 0 & 0 \\ 0 & -26 & 2 & 1 & 0 \\ 0 & 0 & 1 & 3 & 23 \\ 0 & 0 & 0 & 23 & 4 \end{bmatrix}$$

Then, M_2 represented as the following final graph (Fig. 8) (discard the diagonal):

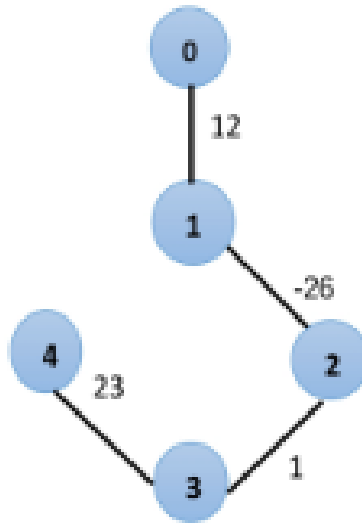


Fig. 8. Final Graph

We use this graph to retrieve the original message as follows : Let the node 0 be A, so by using the keyword and encoding table,

$$\text{node 1} = \text{code (A)} + 12$$

$$\text{code (A)} = E - A = 5 - 1 = 4 \text{ (using the keyword)}$$

$$\text{therefore, node 1} = \text{code A} + 12 = 4 + 12 = 16$$

$$S - 16 = 19 - 16 = 3, \text{ where 3 represents C (from the encoding table)}$$

$$\text{And node 2} = \text{code (C)} - 26$$

$$\text{Code (C)} = S - C = 19 - 3 = 16$$

$$\text{therefore, node 2} = \text{code (C)} - 26 = 16 - 26 = -10$$

$$E - (-10) = 5 - (-10) = 15, \text{ where 15 represents O}$$

Similarly proceeding, we get the original text COLD.

Chapter 3

Cryptography in Daily Life

3.1 WhatsApp Encryption

Cryptography plays a crucial role in securing communication across various platforms, and one of the most widely used applications of cryptography in daily life is **WhatsApp**. WhatsApp employs **end-to-end encryption (E2EE)** to ensure that messages, calls, and media shared between users remain private and secure from third parties, including hackers, governments, and even WhatsApp itself.

3.1.1 How WhatsApp Uses Cryptography

1. End-to-End Encryption (E2EE)

WhatsApp's encryption is based on the **Signal Protocol**, which uses a combination of **asymmetric and symmetric encryption** to protect messages. When a user sends a message, it is **encrypted on their device** and only **decrypted on the recipient's device**, preventing any interception in between.

2. Public and Private Key Pair

- Each user has a **unique pair of cryptographic keys**: a **public key** and a **private key**.
- The public key is shared with contacts, while the private key remains securely stored on the user's device.

- When a message is sent, it is encrypted using the recipient's public key, and only their private key can decrypt it.

3. Session Keys for Secure Communication

- Each conversation session generates a unique **session key**, ensuring that even if one message is compromised, previous and future messages remain secure.
- The session keys are regularly updated to enhance security.

4. Forward Secrecy

WhatsApp employs **forward secrecy**, meaning that even if a session key is exposed, past communications remain protected. This ensures that an attacker cannot decrypt old messages even if they somehow access the encryption keys.

5. Verifying Encryption

Users can verify their encryption by **scanning a security code** in their contact's chat settings, ensuring that their conversation remains private and uncompromised.

3.1.2 Importance of WhatsApp Encryption

- **Privacy Protection:** Prevents third parties from reading private conversations.
- **Secure Calls and Media Sharing:** Encrypts voice/video calls, documents, images, and videos.
- **Prevents Government and Corporate Surveillance:** Even WhatsApp itself cannot access user messages.
- **Defends Against Hackers:** Ensures that data remains protected from cyberattacks and breaches.

WhatsApp's cryptographic framework is an excellent example of how encryption safeguards digital communication, ensuring privacy in our daily interactions. However, as technology evolves, new cryptographic methods will be needed to counter emerging security threats, making continuous improvements in encryption essential.

3.2 Network Security Using Graph Theory in Cryptography

Graph theory plays a key role in securing networks by detecting cyber threats, ensuring safe data transfer, and managing encryption keys. It helps in analyzing attack patterns, optimizing secure routes, and strengthening cryptographic protocols.

3.2.1 How does graphs used in cryptography

They provide a mathematical structure that allows complex problems to be represented visually and computationally. For example, in blockchain technology, Merkle Trees— which are a type of graph—are used to ensure data integrity by securely linking blocks of information. Graph-based problems, such as finding the shortest or most complex paths, are also used in encryption methods to make breaking the security system extremely difficult. Additionally, cryptographic protocols use graphs to securely exchange keys and protect communications.

3.2.2 Attack Graphs for Threat Analysis

Attack graphs represent possible ways an attacker can exploit vulnerabilities in a network. By analyzing these graphs, security experts can identify weak points and implement measures to prevent attacks. These graphs are widely used in penetration testing to simulate cyberattacks and improve defense strategies.

3.2.3 Intrusion Detection Systems (IDS)

Graph-based **Intrusion Detection Systems (IDS)** monitor network traffic and detect unusual patterns that may indicate a cyberattack. Graph models help in identifying anomalies, recognizing known attack signatures, and grouping suspicious activities. This enhances network security by alerting administrators to potential threats.

3.2.4 Secure Routing in Networks

Graph algorithms ensure data is transmitted securely and efficiently.

- **Shortest Path Algorithms (Dijkstra's, Bellman-Ford)** help find the safest and fastest routes for data.
- **Minimum Spanning Tree (MST)** is used in network design to connect all nodes securely with minimal risk and cost.
- **Resilient Routing** prevents attacks like *Man-in-the-Middle (MitM)* and *Denial of Service (DoS)* by choosing alternative secure paths.

3.2.5 Cryptographic Key Management

Encryption keys are essential for protecting network communication. Graph-based key management methods ensure secure key exchange.

- **Graph-Based Key Exchange** improves security by distributing encryption keys across a network.
- **Threshold Cryptography** splits a key into multiple parts, making it harder for hackers to steal or misuse it.

Graph theory strengthens network security by detecting threats, securing data transmission, and managing encryption keys. As cyber threats continue to evolve, graph-based cryptographic techniques will play a crucial role in protecting digital communication and online transactions.

3.3 Other Applications

3.3.1 Cryptography and Emails

Email cryptography is used to keep emails safe and private. It scrambles (encrypts) the message so only the intended person can read it. It also adds digital signatures to prove the email is real and hasn't been changed. Security tools like SPF, DKIM, and DMARC help stop fake emails and prevent scams. TLS encryption protects emails while they travel across the internet. All these methods work together to keep emails safe from hackers and fraud.

Conclusion

Cryptography as explored in this project, plays a crucial role in securing communication by using mathematical techniques to encrypt and decrypt data. The study began with an introduction to cryptography, covering its historical evolution from early ciphers like the Caesar cipher to modern encryption techniques. The field has grown from simple substitution methods to complex cryptographic systems used in various applications today.

In the second chapter, we examined different cryptosystems, including shift transformations, affine transformations, and digraph encryption. We also explored cryptanalysis techniques, demonstrating how encrypted messages can be deciphered using mathematical principles. This chapter emphasized how cryptographic strength depends on the complexity of the encryption method and the secrecy of the key.

The third chapter introduced the use of graph theory in cryptography, highlighting how mathematical structures such as graphs and spanning trees can enhance encryption algorithms. A proposed encryption algorithm was developed using graphs, demonstrating an innovative approach to secure communication. By constructing a minimum spanning tree and applying matrix operations, this method illustrated a novel way to encode and decode messages.

In the fourth chapter, we explored real-world applications of cryptography. Application of cryptography in whatsapp, network security and Emails.

Through this study, it is evident that cryptography has transitioned from being a military tool to an indispensable aspect of everyday life, ensuring confidentiality, integrity, authentication, and non-repudiation in digital communications. As cyber threats evolve, cryptographic techniques must also advance to counteract potential vulnerabilities. The future of cryptography lies in the development of quantum-resistant algorithms and post-quantum cryptography, ensuring that secure communication remains reliable in an increasingly digital world.

References

1. CRYPTOGRAPHY:THEORY AND PRACTICE by Douglas R.Stinson
2. CRYPTOGRAPHY:AN INTRODUCTION by VV. Yaschenko