A COMPREHENSIVE PURVIEW OF DIFFERENT CONCEPTS OF NUMBER THEORY IN CRYPTOGRAPHY

Dissertation submitted to the Department of Mathematics in partial fulfillment of the requirements for the award of the degree of Master of Science in Mathematics

MAHAPURUSHA SRIMANTA SANKARADEVA VISWAVIDYALAYA NAGAON, ASSAM

Submitted by

Deepanjal Ghosh

Roll No : MAT-15/23

Registration No: MSSV-0023-101-000374

M.Sc. 4th Semester

Session : 2023-2025

Under the guidance of

Dr. Maitrayee Chowdhury (Assistant Professor)

Department of Mathematics, MSSV

Nagaon, Assam

Certificate

This is to certify that **DEEPANJAL GHOSH** bearing **Roll No MAT-15/23** and **Regd. No. Mssv-0023-101-000374** has prepared his dissertation entitled "**A COMPREHENSIVE PURVIEW OF DIFFERENT CONCEPTS OF NUMBER THEORY IN CRYPTOGRAPHY**" submitted to the Department of Mathematics, **MAHAPURUSHA SRIMANTA SANKARADEVA VISWAVIDYALAYA**, Nagaon, for fulfilment of M.Sc. degree, under guidance of me and neither the dissertation nor any part thereof has submitted to this or any other university for a research degree or diploma.

He/She fulfilled all the requirements prescribed by the department of Mathematics.

Supervisor

(DR. MAITRAYEE CHOWDHURY)

Assistant Professor

Department of Mathematics

MSSV, Nagaon (Assam)

E-mail: maitrayee321@gmail.com

DECLARATION

I, Deepanjal Ghosh bearing the Roll No – MAT- 15/23, hereby declare that this dissertation entitled, "A COMPREHENSIVE PURVIEW OF DIFFERENT CONCEPTS OF NUMBER THEORY IN CRYPTOGRAPHY" was carried out by me under the supervision of my guide Dr. Maitrayee Chowdhury Ma'am, Assistant Professor of the Department of Mathematics, Mahapurusha Srimanta Sankaradeva Viswavidyalaya, Nagaon. The study and recommendation drawn are original. The data and facts started in this survey are correct to the best of my knowledge.

Date: Deepanjal Ghosh

Place: M.Sc. 4th Semester

Roll No: MAT-15/23

ACKNOWLEDGMENT

With great pleasure I would like to express my heartiest gratitude, cordial thanks, deepest sense of respect and appreciation to my reverend teacher and my dissertation supervisor Dr. Maitrayee Chowdhury, Assistant Professor, Department of Mathematics, Mahapurusha Srimanta Sankaradeva Viswavidyalaya, Nagaon for her indispensable guidance, sympathetic encouragement, valuable suggestions and generous help during the course of study and the progress of this dissertation work.

I would also like to extend my heartfelt thanks to all the faculty members and staff of Mathematics Department, Mahapurusha Srimanta Sankaradeva Viswavidyalaya, for providing a stimulating academic environment and the necessary resources to carry out this work.

A special thanks to my classmates for their constant motivation, constructive discussions, and moral support during the study time.

I am deeply grateful to my family for their unconditional love, sacrifices, and encouragement throughout my academic journey. Their faith in me has been my greatest source of strength.

Finally, I would like to acknowledge everyone who has directly or indirectly contributed to the completion of this dissertation. Your support and assistance have been invaluable, and I am truly thankful.

DEEPANJAL GHOSH

NAGAON

July 2025

Table of Contents

ABSTRACT

As we know in abstract algebra, the topic consists of some concepts such as groups, rings, fields etc. which form the basic foundation of modern theoretic mathematics. One of the important concepts that connects the abstract algebra and number theory is modular arithmetic. It can be defined as–

In mathematics, modular arithmetic is a branch of arithmetic that deals with integers, excluding the usual operations of elementary arithmetic, where numbers “wrap around” when reaching a specific value known as modulus. Carl Friedrich Gauss, in his book *Disquisitiones Arithmeticae* published in 1801, introduced the modern approach to modular arithmetic. For a positive integer n, two integers a and b are said to be congruent modulo n if their difference is divisible by n i.e.

$a \equiv b(mod\, n)\ iff\ \ n/a - b$

Arithmetic functions play a crucial role in number theory, acting as mappings from the set of positive numbers to the real or complex numbers. They are significant in various mathematical areas such as game theory. There are different types of arithmetic functions such as Euler’s totient function (ϕ(n)), Mobius function μ(n) etc.

Partition theory, an important field within number theory, examines ways to express integers as the sum of smaller integers. For instance, the number 4 can be split into five different forms: 4, 3+1, 2+2, 2+1+1, 1+1+1+1.

Cryptography is the branch of mathematics and also of computer science concerned with data protection and techniques for secure communication. It designs as well as analyzes algorithms that transform data so that unauthorized parties cannot interpret it, yet the intended recipients can successfully decode it.

Number theory plays a significant role in cryptography since it provides the mathematical base for many encryption algorithms and security protocols. Its applications help ensure private communication and data safety. They also maintain the integrity of digital transactions. Public-key cryptography, digital signatures, and secure communication

protocols make extensive use of number theory; they depend on number-theoretic concepts like prime numbers, modular arithmetic, and discrete logarithms. Data accuracy, secrecy, and verification within modern information systems rely on these mathematical principles to create robust encryption methods.

Cryptographic algorithms often utilize the properties of prime numbers, Euler's totient function $\phi(n)$, and the complexity of resolving specific problems in number theory, such as integer factorization and the discrete logarithm problem. These difficult mathematical problems ensure the strength of encryption systems, as they are nearly impossible to reverse without the correct cryptographic key.

Number theory acts as the theoretical core of cryptography, supporting the development of practical cryptographic protocols that uphold the confidentiality, consistency, and authenticity of digital information in today’s era.

Although number theory plays a vital role in cryptography, it is important to recognize the challenges it faces, including the potential of quantum computing to break current cryptographic techniques. This calls for ongoing research and innovation in quantum-resistant algorithms to secure future digital communications.

1. Introduction

As we know in abstract algebra, the topic consist of some concepts such as groups, rings, fields etc. which form the basic foundation of modern theoretic mathematics. One of the important concepts that connects the Abstract algebra and number theory is Modular arithmetic. It can be defined as-

In mathematics, modular arithmetic is a branch of arithmetic that deals with integers, excluding the usual operations of elementary arithmetic, where numbers "wrap around" when reaching a specific value known as Modulus. Carl Friedrich Gauss, in his book "Disquisitiones Arithmeticae" published in 1801, introduced the modern approach to modular arithmetic. For a positive integer n, two integers $a\ and\ b$ are said to be congruent modulo n if their difference is divisible by n i.e.

$$a \equiv b(mod\ n)\ iff\ \ n/a - b$$

Arithmetic function play a crucial role in number theory acting as mappings from the set of positive numbers to the real or complex numbers. They play a vital role in various mathematical content such as Game theory. There are some type of arithmetic function such as Euler's totient function $\big(\phi(n)\big)$, Mobius function $\mu(n)$ etc.(1)

Partition theory, a crucial field within number theory, investigates ways to represent integers as the sum of smaller integers. For instance, the number 4 can be divided into five different ways: $4, 3 + 1, 2 + 2, 2 + 1 + 1, 1 + 1 + 1 + 1$

Cryptography is the branch of mathematics and also branch of computer science dealing with the data protection and with techniques for secure communication. It creates as well as analyzes algorithm. Those algorithm transform so that forbidden parties cannot read it., yet intended recipients can decode it.

Number theory plays a major role within cryptography since it serves as the mathematical backbone for many cryptographic algorithms and for protocols. Its applications ensure secure communication as well as data protection. They also maintain throughout the integrity of digital transactions. Public-key cryptography, digital signatures, and secure communication protocols see number theory in cryptography's use; it relies on number-theoretic concepts like prime numbers, modular arithmetic, and discrete logarithms. Data integrity, confidentiality, and authenticity inside modern information systems depend on these mathematical principles to develop strong encryption techniques.

Cryptographic algorithms frequently leverage properties of prime numbers, Euler's totient function $\phi(n)$, and the complexity of solving specific problems in number theory, such as integer factorization and the discrete logarithm problem. These complex mathematical problems guarantee the safety of encryption systems, as they are practically impossible to solve without the proper cryptographic key.

Number theory serves as the theoretical basis for cryptography, allowing the development of practical cryptographic protocols that safeguard the confidentiality, integrity, and authenticity of digital data in the modern era.

Although number theory plays a crucial role in cryptography, it is essential to acknowledge the challenges it encounters, including the possibility of quantum computing undermining existing cryptographic systems. This necessitates continuous research and development of quantum-resistant algorithms to guarantee future data security.

1.1 Historical Backgrounds:

Number theory is a branch of mathematics that's all about exploring whole numbers and the unique ways they behave and relate to each other. While it's closely tied to arithmetic, which most people think of as basic math operations like addition and multiplication, number theory dives deeper—focusing specifically on the fascinating world of integers. In fact, it's sometimes called "higher arithmetic" because it goes beyond everyday calculations to uncover hidden patterns and relationships among numbers.

By the early 1900s, "number theory" had become the standard term for this field. When mathematicians talk about "numbers" here, they usually mean whole numbers—either natural numbers $(like\ 1,2,3,\ldots)$ or integers (which also include negative numbers and zero). In short, number theory is where math meets the mysteries and magic of whole numbers.

Ancient Civilizations:

Traces of number theory can be found in the earliest records of human civilization. Societies in Mesopotamia, Egypt, China, and India demonstrated advanced understanding of numbers and numerical patterns. A notable artifact is the Babylonian Plimpton 322 tablet (circa 1800 BC), which lists Pythagorean triples—integer solutions to the equation $a^2 + b^2 = c^2$ The systematic nature of these entries suggests a deliberate mathematical approach rather than random discovery.

Greek Contributions:

The Greeks made profound advances in the theoretical aspects of numbers, referring to the study as arithmētikḗ. The Pythagoreans, in particular, attributed mystical significance to numbers, exploring concepts such as perfect, amicable, and polygonal numbers. Euclid (around 300 BCE) compiled foundational number theory results in his treatise Elements, introducing the Euclidean algorithm for computing the greatest common divisor and proving the infinitude of prime numbers. Later, Diophantus of Alexandria (3rd century AD) pushed the field forward with Arithmetica, which presented methods for finding rational solutions to algebraic equations—paving the way for the study of Diophantine equations.

Indian Contributions:

With the decline of Roman influence, mathematical innovation shifted eastward. Indian mathematicians made significant strides in number theory:

- Āryabhaṭa (476–550 AD) contributed to modular arithmetic and devised the kuṭṭaka (pulverizer) method for solving simultaneous congruences, akin to the Euclidean algorithm.
- Brahmagupta (628 AD) was the first to systematically investigate indefinite quadratic equations, including early versions of what is now known as Pell's equation.
- Jayadeva and Bhāskara II (12th century) built on these foundations, offering comprehensive solutions to such equations.

Chinese Contributions:

The Chinese Remainder Theorem, which addresses the solution of simultaneous congruences, first appeared in the Sunzi Suanjing (3rd–5th centuries) and was elaborated upon in Qin Jiushao's Mathematical Treatise in Nine Sections (1247 AD). These early insights into modular arithmetic foreshadowed techniques that are essential to modern cryptography.

European Renaissance and Modern Foundations

The 17th century saw a resurgence of interest in number theory in Europe, led by Pierre de Fermat (1607–1665). Though he published little, Fermat's letters and notes introduced pivotal ideas, including:

- Fermat's Little Theorem (a cornerstone of modular arithmetic)
- Fermat's Last Theorem
- Investigations into prime numbers, Pell's equations, and representations as sums of squares

Building on Fermat's legacy, Leonhard Euler (1707–1783) proved many of his conjectures and formalized concepts such as the Euler's Totient Function ϕ(n)$\phi(n)$. Euler also contributed to the study of continued fractions, Diophantine equations, and the sum of four squares, laying the groundwork for analytic number theory and revitalizing interest in the subject.(2)

Prior to the modern era, the main goal of cryptography was to keep messages secret. This focused on encryption-converting readable messages into scramble code so that only a person with the right key could understand them. This was important for protecting sensitive information, especially in areas such as military communication, diplomacy where privacy was everything. Over the past few decades, however, cryptography has grown far beyond just hiding information. Today, it also plays a key role in verifying that messages haven't been tampered with, confirming the identity of the people involved in a communication, creating digital signatures, and even enabling secure methods for sharing information without revealing everything—such as in interactive proofs and secure computations.

Classical Cryptography:

In ancient times, cryptography mainly involved simple methods like substituting or rearranging letters in a message. Civilizations such as the Egyptians, Greeks, Indians, Persians, and Arabs all devised their own ciphers and ways to break them. The discovery of frequency analysis by Arab mathematicians made most of these early codes easy to crack. Later, more complex systems like the Vigenère cipher were introduced, but even these were eventually deciphered. By the end of the 19th century, it was recognized that a cipher's security should rely on keeping the key secret, not the method itself

Early Computer-Era Cryptography:

With the 20th century came mechanical encryption devices, such as the Enigma machine, which made codes more complicated. World War II spurred advances in codebreaking, including the use of early computers like Colossus. In the 1970s, cryptography became more widely studied, leading to the creation of the Data Encryption Standard (DES) by IBM and the invention of public-key cryptography, including the Diffie–Hellman key exchange and RSA algorithm. These innovations paved the way for secure digital communication.

Modern Cryptography:

Today, cryptography is based on advanced mathematics and computer science. Modern systems use algorithms that are secure because they are hard to solve with current technology. There are two main types: symmetric (the same key is used for both encryption and decryption, as in AES) and asymmetric (different keys for encryption and decryption, as in RSA and ECC). Modern cryptography not only protects privacy but also ensures data integrity, authentication, and non-repudiation, making it essential for secure digital interactions.(3)

Number theory - Sometimes known as "high arithmetic" - is a special area of mathematics that is about understanding the entire number and which ticks them. While most people think of arithmetic as simple calculations such as adding or multiplying, the number theory becomes very darker. It examines the hidden patterns, relationships and unique qualities of the integer. The region has an attractive history, which is spread in all ways from ancient civilizations to our modern digital world, where it now plays an important role in things like keeping our online information through cryptography

The history of number theory and cryptography reveals a fascinating journey—from philosophical curiosity about numbers to their critical role in securing global digital infrastructure. Each milestone not only enriched theoretical mathematics but also brought forward tools that empower the world's most secure communication systems today. The continued interplay between theoretical insights and technological advancements ensures that number theory will remain central to cryptography for the foreseeable future.

2. Literature Review

Fernando Peralta Castro in his work "The Evolution of cryptography through Number Theory" has given- Cryptography, originating from the term meaning "hidden writing," has transformed into a vital tool for securing digital information through mathematical principles. While its formal study began just a century ago, the discipline has rapidly advanced with the emergence of the digital era. What started as simple techniques for concealing messages has grown into complex cryptographic systems that rely heavily on concepts from number theory, including modular arithmetic, the Euclidean algorithm, and Euler's totient function. This literature review traces the historical development of cryptography and highlights how foundational mathematical ideas have shaped modern encryption methods. By examining both classical and contemporary approaches, it underscores the ongoing importance of cryptography in protecting data in an increasingly interconnected world.(2)

Wenchao Shang in his/her work "Development of Number theory and the application in cryptography" has given-Number theory, a foundational branch of mathematics, focuses on the properties and behavior of integers. Its deep connection with cryptography has significantly shaped modern methods of secure communication. This paper reviews the historical evolution of number theory and highlights its critical role in the development of cryptographic techniques. Through a literature-based approach, the study explores how number theory advanced across different eras—flourishing notably in the East by the 1930s and experiencing major growth in the West from the 15th to 19th centuries. The ongoing progress in the field is evident in recent discoveries, such as the identification of the largest known prime number by Curtis Cooper. Applications of number theory, particularly in algorithms like RSA and digital signatures, demonstrate its importance in the design and implementation of modern cryptographic systems. (3)

Dawson Shores in his work “The Evolution of cryptography through Number theory” has given-Cryptography, the art and science of concealing information to ensure secure communication, has a rich history spanning thousands of years. Its counterpart, cryptanalysis—the practice of breaking encrypted messages without the key—has played an equally pivotal role. From basic ancient methods like wrapping messages around sticks to today’s advanced internet encryption, the field has undergone tremendous evolution. As older ciphers were broken, more sophisticated systems had to be developed, leading to the dynamic and ever-changing nature of cryptography. A major driving force behind this evolution is the increasing use of mathematics. What began with simple operations like addition and multiplication has grown to include complex tools such as modular arithmetic, matrix operations, and discrete logarithms. Central to many modern encryption methods is number theory, especially in the design of public key cryptosystems. This paper explores early ciphers based on number theory and highlights the significance of public key systems—such as RSA and the Diffie-Hellman Key Exchange—in securing modern digital communication, including internet transactions and data protection.(6)

A Parthiban in his work “Number Theory: Cryptography and Security” has given-Number theory forms a critical foundation for modern cryptography and digital security, offering essential tools for protecting sensitive information in today’s interconnected world. This paper explores the deep relationship between number theory and cryptographic systems, focusing on key concepts such as prime numbers, modular arithmetic, and discrete logarithms, which underpin many encryption algorithms. By examining widely used schemes like RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), the study illustrates how number-theoretic principles enable secure data transmission, ensuring integrity, confidentiality, and authenticity. In addition, the paper addresses current trends and challenges in cryptographic protocols, highlighting how evolving number theory continues to adapt to emerging cyber threats. By combining theoretical analysis with practical application, this research emphasizes the indispensable role of number theory in shaping secure digital communication and building trust in the digital era.(7)

Mukesh Punia in his work “Number Theory & Application in Cryptography” has given-The number theory, traditionally a branch of pure mathematics, has become the foundation of modern cryptographic systems. This letter presents a detailed observation of fundamental number-synagogue concepts and their important applications in securing digital communication. The strength of encryption and decryption techniques used to protect sensitive information in today's digital world depends a lot on the properties obtained from the principle. The main views such as prime numbers, modular arithmetic, and discontinued logarithm problems form the backbone of many cryptographic algorithms. The paper specifically highlights the role of the major factor in public key cryptography, which depends on the computational difficulty of factoring large semipream numbers. It also discusses the practical use of elliptical curve cryptography (ECC), which is known to offer high security with low key sizes - makes it ideal for use in devices with limited resources. By discovering both the theoretical foundations and the implementation of the real world, this research emphasizes the important role of the number theory in developing communication, financial data and secure cryptographic protocols that protect personal privacy in the digital age.(8)

3. Preliminaries

Definition 3.1: Divisibility and Prime Numbers:

Prime numbers are defined as having only two elements. Prime numbers include, for example two, three, five, seven, eleven, thirteen, and so forth. There are two components to these numbers: the number itself and one. An integer b is said to be divided by a $(denoted\ \ a|b)$ if there exist an integer k such that $b = a.k$ i.e. The ability of a number to be divided by another number without producing a remainder is known as divisibility. For Example, $12\ is\ divisible\ by\ 3\ because\ 12/4 = 3(no\ remainder)$. We say that 3 is a divisor of 12. According to the Fundamental Theorem of Arithmetic, which states that every integer larger than one can be factored into a prime in a unique way, primes are the building blocks of integers. The distribution and unpredictability of prime numbers are crucial to cryptography methods like RSA, which use big primes to provide strong encryption keys.

Definition 3.2: Congruence modulo:

In mathematics, modular arithmetic is a branch of arithmetic that deals with integers, excluding the usual operations of elementary arithmetic, where numbers "wrap around" when reaching a specific value known as Modulus. For a positive integer n, two integers $a\ and\ b$ are said to be congruent modulo n if their difference is divisible by n i.e

$$a \equiv b(mod\ n)\ iff\ \ n/a - b$$

Numerous cryptographic algorithms are based on this idea, which uses operations like modular addition, multiplication, and exponentiation to guarantee the security and integrity of data. Particularly in public-key cryptography like RSA, modular congruence makes complicated calculations easier and gives encryption systems the mathematical structure they require.

Definition 3.3: Arithmetic function:

An arithmetic function is a mathematical function that operates on the set of positive whole numbers and can have real or complex values, frequently employed to investigate characteristics of integers. Examples of these functions include the Euler's totient function, divisor function, sum of divisors function, and mobius function. These functions are essential to many applications in cryptography as well as pure number theory. They are especially helpful in algorithms that depend on characteristics that are fundamental to contemporary cryptosystems like RSA, such as multiplicative behavior, prime factorization, or coprimality.

Definition 3.4: Partition theory: Partition theory, a crucial field within number theory, investigates ways to represent integers as the sum of smaller integers. For example the number 4 can be 4 can be partitioned in 5 different ways, viz. $4, 3+1, 2+2, 2+1+1, 1+1+1+1$.

Definition 3.5: Cryptography:

Cryptography is the field of study that focuses on encrypting and decrypting information to ensure its confidentiality and integrity. It guarantees the protection of privacy, the preservation of data accuracy, the verification of data origin, and the prevention of data denial. It heavily relies on mathematical concepts, particularly those from number theory. These number-theoretic concepts provide the foundation for designing secure algorithms that protect sensitive data in modern digital systems.

Definition 3.6: Public Key Cryptography:

In a cryptographic system, each user possesses a pair of keys: a public key that is openly shared and a private key that is kept confidential. Examples include RSA, Diffie-Hellman, and ECC. These systems are constructed on challenges such as integer factorization and discrete logarithms, which are difficult to crack. The foundation of contemporary digital security is this asymmetry in key usage, which permits secure communication even over untrusted networks. Confidentiality, authenticity are guaranteed by public key cryptography. Attackers cannot compute the private key from the public key due to the mathematical difficulty of the underlying number-theoretic difficulties.

Definition 3.7: RSA algorithm:

RSA is a pioneering public key encryption system. It employs modular exponentiation, utilizing a modulus that is formed by combining two large prime numbers. The security of the system relies on the complexity of factoring large composite numbers.

As an asymmetric or public-key cryptography technique, the Rivest-Shamir-Adleman (RSA) algorithm operates on two distinct keys- the public key and the private key. While the Private key is used for decryption and needs to be kept confidential by the recipient, the Public key is used for encryption and is known to everybody. It is named after Ron Rivest, Adi Shamir and Leonard Adleman, who published the algorithm in 1977.

Definition 3.8: Elliptic Curve Cryptography (ECC):

ECC is a mathematical concept that is based on the structure of elliptic curves over finite fields. It offers the same level of security as RSA but with smaller key sizes, making it efficient and secure. It is especially well-suited for usage in smart cards, mobile devices, and Internet of Things (IoT) applications because of its key size efficiency, which results in quicker computations, less storage needs, and lower power consumption.

Definition 3.9: Fundamental theorem of arithmetic:

Every integer greater than one is prime or may be uniquely represented as a product of prime numbers, according to the order of the factors, according to the fundamental theorem of arithmetic in mathematics, also known as the unique factorization theorem or prime factorization theorem.

Definition 3.10: Fermat's Little Theorem:

This theorem is a fundamental theorem of Number theory with various application in Cryptography. It states that if p is a prime number, then for any integer a , the number $a^p - a$ is an integer multiple of a

Here if p is a prime number then,

$$a^p \equiv a(mod\, p)$$

It has a special case i.e. if a is not divisible by p, then Fermat's Little theorem can be defined as - $a^{p-1} - 1$ is an integer multiple of p. Mathematically it can be termed as

$$a^{p-1} \equiv 1(mod\, p)$$

Definition 3.11: Chinese remainder theorem:

Chinese remainder theorem is a important mathematical principle which solves systems of systems of modular equations by identifying a unique solution from the remainder of the division. It is a very important principle which is being used in cryptography.

Mathematically it can be written as

If $M = m_1, m_2, \dots, m_r$ is a set of pairwise relatively prime non-zero integers such that the greatest common divisor of each pair is 1 and $a_1, a_2, \dots, a_r \in \mathbb{Z}$, then

The system of congruences

$x \equiv a_1(mod\, m_1)$,

$x \equiv a_2 (mod\ m_2)$,

$\ldots$,

$x \equiv a_r (mod\ m_r)$

Has a unique solution in modulo M for all $1 \leq i \leq r$

4. Use of Number Theory in various Cryptographic algorithms

We could observe that in the world of cryptographic language, number theory plays an integral part. It is evident in various cryptographic algorithms. Whether it is modular arithmetic or any other concept surely there remains a part of number theoretic concept in making or building a cryptographic code or algorithm. Also there lies different other concepts from the branch of Graph theory, Linear Algebra, Abstract algebra etc. Herein our study, we are interested in the number theoretic aspect that is present in any cryptographic algorithm.

The study of integers, known as number theory, has played a significant role in the advancement of cryptography. Over the years, mathematical concepts such as modular arithmetic, the Euclidean algorithm, and Euler's totient function have been employed to develop robust encryption techniques. Cryptography, which originally referred to concealed writing, has evolved from basic methods to intricate systems that employ number theory to safeguard digital information.

Early cryptographic techniques, such as basic letter substitutions, laid the groundwork for contemporary algorithms like RSA and digital signatures. The ongoing advancements in number theory, exemplified by the discovery of the largest known prime number by Curtis Cooper, highlight the intricate relationship between these two disciplines. In the modern era, number theory plays a crucial role in the development of secure cryptographic systems, safeguarding sensitive data in the digital realm

Number theory plays a pivotal role in the security of today’s digital communication systems. Technologies such as Public Key Infrastructure (PKI), cryptocurrencies like Bitcoin, and secure protocols including HTTPS and SSH are all built upon number-theoretic foundations. These applications safeguard transactions, ensure user privacy, and provide reliable authentication by leveraging mathematical problems that are extremely hard to solve computationally. The strength of these cryptographic methods is rooted in the complexity of challenges such as integer factorization, discrete logarithms, and the elliptic curve discrete logarithm problem

Some Cryptographic algorithms based on Number theory-

Cryptography has developed considerably over time, highly secure from simple replacement methods, infection in number-based encryption techniques. In this section, we will discuss three cryptographic algorithms of different complexity: Caesar Cipher, Vigenère Cipher and Elgamal algorithm. They represent a spectrum of cryptographic approaches - from classical to modern - each reflect the growing mathematical sophistication in getting information to each.

4.1 Caesar Cipher: The Caesar Cipher is the first and one of the simplest encryption techniques, dating back in ancient Rome and named after Julius Caesar, who allegedly used it for the protection of military messages. It is a type of replacement cipher where each letter is transferred by a certain number of positions in the alphabet in the plaintext. The mathematical foundation of Caesar cipher is modular arithmetic, which is a major concept in the number theory.

Each letter P in the plaintext is replaced by a letter C such that,

$$C = (P + k) mod 26$$

Where

P =The position of the letter in the alphabet$(A = 0, B = 1, \dots, Z = 25)$

k =The encryption key(a positive integer)

C =The resulting ciphertext letter.

Decryption is done using the inverse operation-

$$P = (C - k) mod 26$$

Now we will see an example of Caesar cipher to get a broader under understanding of the topic-

Let the plaintext be HELLO, and the key $k = 3$

Convert each letter to its position:

$H(7), E(4), L(11), L(11), O(14).$

Now, we will apply the Caesar cipher formula:

$$H(7) \rightarrow K(10)$$

$$E(4) \rightarrow H(7)$$

$$L(11) \rightarrow O(14)$$

$$L(11) \rightarrow O(14)$$

$$O(14) \rightarrow R(17)$$

So here, the encrypted message is KHOOR.

To decrypt this message, one must shifted back the letter by 3, this will ultimately leads to original message.

To decrypt:

$$K \rightarrow (10 - 3) mod\ 26 = 7 \rightarrow H$$

$$H \rightarrow (7 - 3) mod\ 26 = 4 \rightarrow E$$

$$O \rightarrow (14 - 3) mod\ 26 = 11 \rightarrow L$$

$$O \rightarrow (14 - 3) mod\ 26 = 11 \rightarrow L$$

$$R \rightarrow (17 - 3) mod\ 26 = 14 \rightarrow O$$

This cipher is easy to understand and applied, but is unsafe for brut-form attacks, as there are only 25 potential keys. Despite its simplicity, Caesar serves as an excellent introduction to the concept of cipher encryption

The Caesar cipher's reliance on modular arithmetic ($mod 26$) is a fundamental number-theoretic operation, illustrating how simple congruence relations can be used for basic encryption.

Caesar cipher may be simple, but it represents a fundamental concept in the field of cryptography. It highlights the principles of replacement, key-based encryption and modular arithmetic, which are all important in more advanced encryption systems. Despite being obsolete for real -world encryption, it remains an important educational equipment and a window in the early history of safe communication. (8)

4.2 Hill Cipher: The Hill cipher is a classical symmetric key cipher which was introduced by Lester S. Hill in 1929. It is a type of substitution cipher that encrypts blocks of plaintext letters using matrix multiplication over modulo 26. Here in this method, letters are converted into numbers such that (A = 0, B = 1, ..., Z = 25), then multiplied by an invertible square matrix (key matrix) modulo 26.

The result is then converted back into letters to obtain the ciphertext using the inverse of the key matrix.

Example: Encrypting 'Hide and Run' (using a 2x2 invertible matrix)

First, we remove spaces and convert the plaintext to uppercase, for example- ‘Hide and Run’ to ‘HIDEANDRUN’

Now we convert each letter to its number equivalent using A = 0, B = 1, ..., Z = 25.

So, the alphabets converted to numbers give: H = 7, I = 8, D = 3, E = 4, A = 0, N = 13, D = 3, R = 17, U = 20, N = 13

We group them into 2-letter blocks as required by any 2×2 matrix: (7,8), (3,4), (0,13), (3,17), (20,13)

Now, let’s take any square matrix, which is invertible. For example, let's use the key matrix $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ (It is invertible, because $3.5 - 2.3 \neq 0$)

Encrypt each block with matrix multiplication (mod 26).

a) (7,8):

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 45 \\ 54 \end{pmatrix} \ (mod\ 26) = \begin{pmatrix} 19 \\ 2 \end{pmatrix} \rightarrow \{T, C\}$$

b) (3,4):

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 21 \\ 26 \end{pmatrix} \ (mod\ 26) = \begin{pmatrix} 21 \\ 0 \end{pmatrix} \rightarrow \{V, A\}$$

c) (0,13):

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 0 \\ 13 \end{pmatrix} = \begin{pmatrix} 39 \\ 65 \end{pmatrix} \ (mod\ 26) = \begin{pmatrix} 13 \\ 13 \end{pmatrix} \rightarrow \{N, N\}$$

d) (3,17):

$$\begin{pmatrix}3 & 3\\2 & 5\end{pmatrix}\begin{pmatrix}3\\17\end{pmatrix}=\begin{pmatrix}60\\91\end{pmatrix}\ (mod\ 26)=\begin{pmatrix}8\\13\end{pmatrix}\rightarrow\{I,N\}$$

e) (20,13):

$$\begin{pmatrix}3 & 3\\2 & 5\end{pmatrix}\begin{pmatrix}20\\13\end{pmatrix}=\begin{pmatrix}99\\105\end{pmatrix}\ (mod\ 26)=\begin{pmatrix}21\\1\end{pmatrix}\rightarrow\{V,B\}$$

So, the Encrypted ciphertext is: TCVANNINVB

Now, let's find out the inverse of the key matrix, that is, the decryption key matrix:

The original encryption matrix was: $\begin{pmatrix}3 & 3\\2 & 5\end{pmatrix}$

Its determinant is: $3.5-2.3=9$

The inverse of 9 modulo 26 is: 9^{-1}(mod 26), that is, $9x\equiv 1\ (mod\ 26)\Rightarrow 9x\equiv 27(mod\ 26)\Rightarrow x\equiv 3(mod\ 26)$.

Thus, the inverse matrix modulo 26 is: $3.\begin{pmatrix}5 & -3\\-2 & 3\end{pmatrix}=\begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}$

Now, decrypting the ciphertext using the inverse of the key matrix which is $\begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}$, we get:

a) (19,2):

$$\begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}\begin{pmatrix}19\\2\end{pmatrix}=\begin{pmatrix}319\\398\end{pmatrix}\ (mod\ 26)=\begin{pmatrix}7\\8\end{pmatrix}\rightarrow\{H,I\}$$

b) (21,0):

$$\begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}\begin{pmatrix}21\\0\end{pmatrix}=\begin{pmatrix}315\\420\end{pmatrix}\ (mod\ 26)=\begin{pmatrix}3\\4\end{pmatrix}\rightarrow\{D,E\}$$

c) (13,3):

$$\begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}\begin{pmatrix}13\\3\end{pmatrix}=\begin{pmatrix}0\\13\end{pmatrix}\rightarrow\{A,N\}$$

d) (8,13):

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 8 \\ 13 \end{pmatrix} = \begin{pmatrix} 3 \\ 17 \end{pmatrix} \rightarrow \{D, R\}$$

e) (21,1):

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 21 \\ 1 \end{pmatrix} = \begin{pmatrix} 20 \\ 13 \end{pmatrix} \rightarrow \{U, N\}$$

So, the final recovered plaintext: HIDEANDRUN.

Note: There were originally 10 letters, here instead of taking a 2x2 matrix, we can take 2 , 3-rowed square matrices and two 2x2 matrices (all these matrices need to be invertible) and it will not affect the encryption or decryption.

4.3 Vigenère Cipher: Vigenère Cipher is a classical method of cipher encryption that greatly improves the simple cipher like Caesar cipher. In the name of French cryptographer Blaise de Vigenère, it is a polyalphabetic replacement cipher, which means that it uses several Caesar ciphers with different innings based on a repeated keywords. This method makes frequency analysis much better than monoalphabetic ciphers and was considered unbreakable over many years.

Although it was usually attributed to Blaise de Vigenère (1523–1596), the cipher was actually developed by Giovan Battista Bellaso in the first 16th century. Vigenère later described a uniform, more secure cipher, which is why his name is often associated with it. For centuries, this cipher was known as "le chiffre indéchiffrable" - indecipherable cipher - due to resistance to early cryptanalytic techniques. However, it eventually broke in the 19th century using statistical methods.

Now we will see the working principle of this:

Vigenère Cipher employments a keyword to decide the sum of move for each letter in plaintext. Unlike Caesar Cipher, which uses a fixed shift, Vigenère applies variable shifts depending on the corresponding letters of the keyword.

Now we will see the step by step process:

1. First we will Choose a keyword (e.g., "LEMON").
2. Now we will Repeat the keyword so it matches the length of the plaintext.
3. Now we will Convert letters to numbers (A = 0, B = 1, ..., Z = 25).
4. Apply the encryption formula for each letter

   $$C_i = (P_i + K_i)\ mod\ 26$$

   Where

   P_i =i-th letter of plaintext (in number)

   K_i =i-th letter of repeated keyword (in number)

   C_i =resulting letter of ciphertext (in number)
5. Now we will convert the ciphertext numbers back to letters.

   The Decryption formulae is

$$P_i = (C_i - K_i + 26)\ mod\ 26$$

Plaintext(P)	Keyword(K)
A	L
T	E
T	M
A	O
C	N
K	L
A	E
T	M
D	O
A	N

W	L
N	E

Step 2:

Convert to numbers:

| Letter | A | T | T | A | C | K | A | T | D | A | W | N |

| Value (P) | 0 | 19| 19| 0 | 2 |10 | 0 |19 | 3 | 0 |22 |13 |

| Keyword (K) |11 | 4 |12 |14 |13 |11 | 4 |12 |14 |13 |11 | 4 |

Step 3:

Now we Apply encryption:

$$C_i = (P_i + K_i)\ mod\ 26$$

| Result (C) |11 |23 | 5 |14 |15 |21 | 4 | 5 |17 |13 | 7 |17 |

| Ciphertext | L | X | F | O | P | V | E | F | R | N | H | R |

Now we will see the Final Ciphertext: LXFOPVEFRNHR

Now we will see the Decryption Example:

To decrypt LXFOPVEFRNHR using the same keyword **LEMON**:

$$P_i = (C_i - K_i + 26)\ mod\ 26$$

Using the same steps in reverse, we will recover the original plaintext: ATTACKATDAWN.

The Vigenère cipher played a significant role in the development of encryption techniques. It marked a substantial advancement over basic substitution ciphers and remained effective for centuries. Though no longer utilized for secure communication, it established the groundwork for the concept of employing variable keys in encryption — a principle that remains fundamental to contemporary cryptographic systems.

5.Conclusion and Future Scope:

Conclusion:

In this dissertation, we have detected deep and developed relations between number theory and cryptography. Starting with basic mathematical concepts such as partition, prime number, modular arithmetic and greetings, we have discovered how these abstract ideas make the backbone of modern cryptographic systems. Traveling from ancient encryption methods such as Caesar and Vinner cipher to advanced algorithms such as Elgamal not only reveals the development of cryptography, but also reveals the increasing importance of mathematical rigor in ensuring digital safety.

Through detailed discussion and examples, it became clear that the number principle provides not only tools but also those challenges that make encryption possible. Concepts such as factoring large major numbers or the difficulty of solving discrete logarithm are not just mathematical curiosities - they are many obstacles that protect encrypted messages in today's world. Whether it is RSA, Diffie-Hellman, or ECC, all these public major cryptographic systems fundamentally depend on number-principles related problems that are difficult to reversed computably.

In addition, the study of historical ciphers such as Caesar and Viganere offered valuable insight into the roots of cryptography. Although these methods are no longer safe from modern standards, they help us understand how early thinkers tried to protect communication - and how far we have come in this discovery. Even more importantly, these methods also laid the basis for the development of strong, more complex algorithms.

One of this task is the major takeaways realizing that cryptography is not only about encoding-this is a dynamic interconnection between abstract mathematics, computer science and real-world applications. From securing online banking and confidential communication for safety of national security and personal privacy, cryptographic systems are now an integral part of the digital age.

Future Scope:

As we move forward in the era of digital connectivity and data-operated technologies, the need for strong, more efficient cryptographic system is only increasing. The future of number theory in cryptography has immense ability, especially in the following areas:

1. Better security for internet:
   Cryptography helps save our messages, passwords, bank details and more when we use the Internet. In the future, strong number-principle-based methods can help make online communication even more secure from hackers.
2. Secure Mobile and Smart Devices: Since more people use mobile phones, smartwatch and smart home devices, we will need encryption that also works well on small and low-power devices. Number theory-based systems such as ECC (elliptical curve cryptography) are great and will become even more useful.
3. Protecting Data from Future Computers: Scientists are building powerful quantum computers, which may be able to break some encryption methods today. Researchers are now working on new number theory techniques that can oppose these future computers and keep our data safe.
4. Blockchain and Cryptocurrencies: Technologies like Bitcoin and blockchain rely on number theory to keep records safe and secure. As these technologies grow, number theory will continue to be used in developing better systems for digital money and smart contracts.
5. Safer Sharing of Information: Whether he is sending personal messages, storing health data, or making digital payments, the need for safe communication will continue to increase. The number theory will help create new ways to safely share data in all these areas.

In short, the number theory will be an important part of our digital future. As new problems and technologies appear, the number theory will help solve them - by making our digital world more secure, private and reliable.

6.REFERENCES:

The books and articles for our work are listed below:

1. *Modular arithmetic*. (2025). https://en.wikipedia.org/wiki/Modular_arithmetic
2. Castro, F.P.(2024). The evolution of cryptography through number theory. arXiv.
3. Shang, W. (2023). Development of number theory and the application in cryptography. *Theoretical and Natural Science*,2023
4. Wikipedia contributors. (2025, June 28). *Number theory*. Wikipedia.

   https://en.wikipedia.org/wiki/Number_theory
5. Wikipedia contributors. (2001, November 12). *Cryptography*. Wikipedia.

   https://en.wikipedia.org/wiki/Cryptography
6. Shores, D. (2020, November 30). *The evolution of cryptography through number theory*
7. Parthiban, A. (2019). Number theory: Cryptography and security. *The Pharma Innovation Journal, 8*(2), 893–896
8. Punia, M. (2014). Number theory and applications in cryptography. *International Journal of Mathematics and Its Applications, 2*(4), 71–82.