E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 06-05-2025
Accepted: 10-06-2025
Published: 15-07-2025

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 3; Issue 3; 2025; Page No. 344-348

Role of Elementary Number Theory in Modern Cryptographic Systems

[1]Tripti Gautam and [2]Dr. Narendra Bahadur Singh

[1]Research Scholar, Mahakaushal University, Jabalpur, Madhya Pradesh, India
[2]Professor, Mahakaushal University, Jabalpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18381105

Corresponding Author: Tripti Gautam

Abstract

The foundation of modern cryptography is number theory. It provides the mathematics required for safe message delivery and data protection. Common building blocks cryptography techniques, including RSA and Diffie If you ask Hellman include modular arithmetic and prime numbers. Progress in modern cryptographic algorithm development that guarantee safe communication and data privacy in many real-world applications depends heavily on the foundations of number theory. RSA and elliptic curve are two examples of number-theory-based cryptographic algorithms that are now in use and are used to secure digital signatures, restricted access systems, and monetary dealings conducted over the Internet. It is the fundamental goal of this study to investigate uses for number theory in Modern Cryptographic Systems. An explanation of the number theoretic techniques and the importance of these approaches in cryptography is provided in this paper.

Keywords: Cryptography, Number Theory, Internet, Techniques, Elementary

Introduction

Modern society relies heavily on cryptography as a security measure for its information infrastructure. As an example, cryptography has many applications in the field of network security, including protecting data from theft or tampering with communications over networks, encrypting card information, safeguarding transaction data, and preventing fraud in the financial sector, and protecting state secrets and personal privacy in government agencies. Throughout mathematics' long and illustrious history, number theory has evolved into a comprehensive framework. For cryptography involving complicated operational procedures, number theory-an important subfield of theoretical mathematics offers a secure and trustworthy encryption system. Using modern technology, a few decades ago, encryption began to use number theory, which greatly improved internet information security.

Thus, it is crucial for individuals in contemporary communities to understand how Cryptography evolved with the help of number theory. Two examples of cryptography methods are RSA and DH. techniques, along with the primary emphasis of this literature review is on the underlying number theory of these two elementary algorithms, drawing on a synthesis of previous research and studies in cryptography. Following the algorithms' presentation, we will discuss their security analysis and their applications. As a last point, this literature study will go over a few good ways to fix the current issues with RSA and DH algorithms. The purpose of this literature study is to educate readers about cryptography's foundational concepts and to examine the potential vulnerabilities in various algorithms.

For many generations, it has been essential to communicate covertly. If two people want to keep their conversation private, they need to write in a way that someone else the message, not even after reading it, could make sense of it. For instance, it would be disastrous for allied military commanders to risk their enemies eavesdropping on them while they deliberate crucial war strategies. The notion of encryption originated from this general concept. Encryption of communications necessitated the recruitment of individuals to design ciphers. The Caesar Cipher, an early kind of encryption that was Caesar's name is synonymous with a famous historical method. By rearranging a predetermined distance from each letter of the alphabet, we may form new words (for instance, "at" becomes "bu" when we reorder the letters by 1). The term for this kind of encryption is a shift cipher. Applying any number other than 26 to the English alphabet would obviously work (because that would result in a letter reverting to its original location).

Literature Review

K, Gavirangaiah. (2023) [1]. Numerology, a branch of mathematics, is foundational to security, since it provides the theoretical groundwork for many cryptographic methods and protocols. Diophantine equations, modular arithmetic, prime numbers, divisibility, and other features of integers are studied in this area. In order to safeguard information, prevent unauthorized access, and guarantee anonymity during online transactions, cryptographic systems use fundamental notions from number theory. Relying concerns certain problems in number theory and their mathematical complexity, It is public-key cryptography that stands out among the many cryptographic applications of number theory.

Peranginangin, Andreas. (2024) [2]. Our technological age has altered the way of life. Starting with the challenge of locating information, technology allows for easy and rapid searches of many kinds of information. On top of that, data storage in software or online is a breeze. On the other hand, you would prefer that no one who isn't interested in this data have it. Cryptography, a branch of computer science that draws on concepts from number theory, is therefore essential for protecting sensitive information.

Ethan, Amelia Konal. (2023) [3]. More secure means of data encryption and secret communication have been made possible by cryptography's heavy reliance on mathematical discipline known as number theory. Analyzing the theoretical foundations and practical applications of current cryptographic algorithms and protocols, this article explores how number theory has been applied to them. The study delves into the mathematical foundations of several number-theory based cryptographic primitives, including secure communication protocols, public-key cryptography, digital signatures.

Hou, Bo. (2024) [4]. The expansion of the Internet has been phenomenal in the 21st century. Keep up with the ever-changing digital world by learning cryptography, which safeguards number theory as an essential Internet guarantee, and update your algorithms accordingly. A lot of people are concerned about newly found security flaws in algorithms since the Internet is growing so quickly. Rivest-Shamir-Adleman algorithms, which are the focus of this literature study, include RSA and Diffie-Hellman, which integrates and summarizes prior research on their introductions. A brief overview of algorithms and number theory is provided in this literature review, along with examples of its use and any related security concerns.

Vladimirovich, V.S. *et al*. (2018) [5]. This article explains how current information security methods make use of some aspects of number theory. Some well-known examples of such protocols and algorithms are the RSA and El Gamal public key encryption methods, as well as the Diffie-Hellman Protocol, which generates keys in pairs. Among the many cryptographic uses of number theory, modified Euclid method stands out. Methods are provided the algorithms for RSA and El Gamal signatures are provided. The bilinear transformation-based electronic signature technique concludes by applying an explicit rule of reciprocity to a simplified pairing scenario.

Number Theory

Nowadays, cryptography-an application of mathematics-is ubiquitous. Mathematics includes the branch known as cryptography. Creating secure and effective codes is the focus of cryptography. Cryptosystems are a collection of techniques that it uses to transmit and receive encrypted messages. An ever-growing role of cryptography, which emerged in prehistoric societies, is evident in modern life. Every time you use a computer or swipe a credit card, a security mechanism built from a cryptosystem is implemented. Cyber and national security-related matters are where it really shines. Cryptography depends significantly on mathematics, namely the study of numbers, also referred to as number theory. The research primarily aims to will be on Number Theory applications that might have direct implications for cryptography.

The struggle to safeguard individuals' right to privacy in their online communications is a long-standing one. Modern cryptography has its roots in the use of methods like buried text, code pads, and disappearing inks. An ancient Greek term meaning "to hide," "kryptos" is where the English word "cryptography" gets its start. Central to cryptography it's the study of techniques that make it possible to encrypt communications or data in a manner that makes deciphering them very difficult without a particular key that can be used to reverse the encoding process. The field of research known as cryptography focuses on methods for encoding or hiding communications or data.

One kind of encryption scheme is the use of "one-time pads," also known as Vernam ciphers, which are very secure and involve nothing more complicated than changing letters for numbers. So yet, the only cryptography method that has shown to be impenetrable is one-time pad encryption. This is because keys and one-time pad codes are only valid for a single usage. However, because to the high number of codes and keys needed, one-time pads are not practical for widespread use. A large deal of wars and diplomatic negotiations have hinged on whether one side or another could decipher the so-called secret signals transmitted by the other side. For example, the Allies were able to gain crucial strategic and tactical advantages in WWII by intercepting and deciphering the Enigma code, which Nazi Germany had used to encrypt secret communications.

It was Nazi Germany that had sent these communications in code. U.S. troops gained the upper hand in their confrontation with Imperial Japanese forces when the creation of operation MAGIC hacked Japan's encryption system. The outcome was a resounding triumph for America because of this. as a result of the gradual replacement of paper and pencil by digital record keeping tools and the ongoing evolution of computer technology. The study of cryptography became more important midway through the 20th century.

Early Modern Number Theory

French mathematician Pierre de Fermat (1607–1665) kept his works under wraps, communicating only via letters and marginal notes. in The European community took a fresh interest in number theory after his work revived the discipline. In addition to proving Fermat's right triangle theorem, he postulated two foundational theorems of Fermat: modules in mathematics are derived from the Little Theorem and the Last Theorem. In addition, he researched Pell's equations, prime numbers, and the four-square

theorem.

A friend of Leonhard Euler's, the hobbyist Christian Goldbach, directed him to some of Fermat's writings on the topic in 1729, piquing his interest in number theory (1707–1783). Some have referred to this as the "rebirth" of contemporary number theory, as Fermat failed to pique the interest of his colleagues in the field. He established allegations put out by Fermat, such as began to demonstrate Fermat's Last Theorem, It asserts that all numbers, when squared, add up to their total, and the same holds true for Fermat's Little Theorem. The relationship between continuing fractions and Pell's equation was explained in depth by him. Analytical number theory may trace its roots back to his writings.

Three of their European contemporaries continued the effort in the area of elementary number theory. We gave complete demonstrations of Wilson's theorem and the four-square theorem. Joseph-Louis Lagrange (1736–1813) also established the theory that underlies Pell's equations. According to Adrien-Marie Legendre (1752–1833), quadratic reciprocity is stipulated by law. Additionally, he made assumptions about in the theory of prime numbers and arithmetic progressions, Dirichlet theorem applies. The equation was carefully considered by him. $ax^2 + by^2 + cz^2 = 0$. As he grew older, he successfully proven the last theorem of Fermat. In his 1801 work, Disquisitiones Arithmetician, Carl Friedrich Gauss (1777–1855) had a tremendous impact on number theory and shaped its trajectory throughout the nineteenth century. In this study, Gauss established quadratic form theory and proved the rule of quadratic reciprocity. In addition, he included a section on computational issues, including primality checks, and provided basic notation for congruences. He connected number theory with the roots of unity. This is one method in which Gauss may have indirectly explored algebraic number theory and the work of Évariste Galois.

When it comes to delving into the patterns and systems that govern our environment, modern mathematics offers a one-of-a-kind toolbox. Number theory, which investigates the connections and fundamental features of integers, is a prominent area in this regard. Renowned mathematicians like Hugo Riemann, Hermann Minkowski, Terence Tao, Pierre Fermat, Carl Friedrich Gauss, Leonhard Euler, and Pierre Fermat all played important roles in expanding the area of number theory by finding new laws and bridging the gap between it and other areas of mathematics. Within the realm of mathematical statistics, numbers and all the things they can do are the focus of attention. Organic arrays.

1, 2, 3, 4, 5,..., 99, 100, 101,...

Research into all natural numbers form a set that falls under the utmost importance. Research into natural numbers has its roots in Classical Greece. Both P. Fermat and L. Euler made significant advances to our understanding of natural numbers in the 17th and 18th centuries, respectively. Although Fermat did not provide proofs for many of his findings, Euler developed new methods and procedures and attached proofs to them. Mathematical number theory has been around for a long time. Numerous areas of mathematics may trace their roots back to these investigations; number theory, in turn, employs a wide variety of analytical, algebraic, geometric, and other techniques to address issues in number theory. A number of subfields of algebra emerged in response to efforts to resolve issues with topics such as Fermat's theorem and prime number distribution.

Elementary Number Point Number Theory

Mathematical inquiry into integers and all that they have to offer is known as elementary number theory. Number distribution, divisibility, prime numbers, and congruences are some of the basic ideas covered. By shedding light on the structures and patterns intrinsic to numbers, this area provides the framework for comprehending their interactions. Questions concerning the properties of whole numbers, such as their connections, divisors, and remainders, are fundamental to number theory. As an example, A linear Diophantine equation involving factors and multiples or the GCD of two integers may be solved with its assistance. Modular arithmetic, prime factorization, and theorems like the arithmetic fundamental theorem-that all positive integers may be uniquely factored into primes - are important subjects.

The notion of remainders when dividing by a number is a common representation of modular arithmetic, which is introduced in elementary number theory and includes arithmetic operations inside a given set of integers. The complexity of some number-theoretic issues provides the foundation for secure communication systems, which is only one example of how this field of research has real-world implications outside of pure mathematics. The breadth and depth of the subject make it an excellent research topic with ties to many branches of mathematics. Filling the gap between academic Using precision and practicality, the ideas presented here provide the basis of more complex subjects.

Prime numbers are crucial in several cryptographic contexts due to their exceptional mathematical properties. Their cryptographic uses and importance are summarized below:

RSA Algorithm

An essential component of contemporary cryptography, the RSA method-created by in particular, it is the responsibility of Adi Shamir, Leonard Adleman, and Ron Rivest to guarantee the security of data while it is being sent over the internet. Data is encrypted using a public key and decrypted using a private key, much as in other public-key cryptosystems.

How It Works

Key Generation

Producing two enormous prime numbers is the first stage of RSA. These secret primes are selected at random. A huge composite number is obtained by multiplying these two primes together. Any public or private key may make use of this composite number. Concurrently, a unique prime number, known as Euler's totient function, is computed. Finding out how public and private keys relate to one another is made easier using this function. Then, with regard to this totient function, certain criteria are used to choose an integer. This number is included in the key that is publicly available. Following that, the secret key, which is an additional integer, is computed. When used with the public key, this integer guarantees accurate data decryption.

Encryption and Decryption

Encryption and decryption may start after keys are produced. The message may be encrypted by the sender using a key. The public key may be accessed by anybody. The point is altered into a form that is both incomprehensible and seems arbitrary to everybody who hears about it. The message can be deciphered by the receiver if they have the secret key. The original format of the communication is restored via this decryption procedure. The difficulty in reducing the composite number to its prime components is the foundation of this method's security. Due to the computing the factorization problem's computational complexity, decrypting messages without the secret key is very difficult for unauthorized parties.

Binary Operations: Three binary operations on the set of integers are of relevance in cryptography. Two inputs are required for a binary operation to produce a single output. When working with numbers, the three most typical binary operations are adding, subtracting, and multiplying. In Figure 1 we can see that a and b are the inputs to these procedures, while c is the output. The collection of integers is used as both the input and the output. In this context, division does not belong as it produces two results instead of one, as we will see shortly.

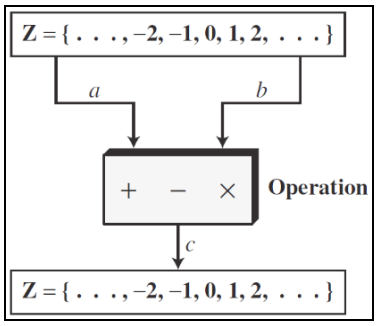

Fig 1: A collection of integers and three binary operations on it

Integer Division: In integer mathematics, we may get q and r by dividing a by n. It is possible to demonstrate the connection between these four numbers by $a = q \times n + r$ In this connection, the variables a, q, n, Dividend, quotient, divisor, and remainder are represented by r, correspondingly. Because two integers, q and r, are produced by dividing a by n, it is clear that this is not an operation. We may refer to it as the division relation.

Example 1.1: Picture a world where n= 11 and a= 255. Using the division process we learnt in math, we can determine q = 23 and r = 2, much as Figure 2 shows.

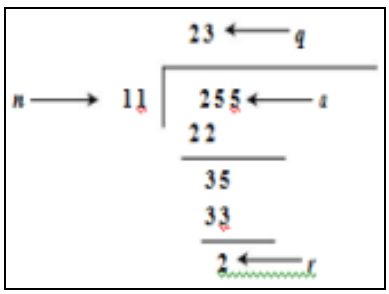

Fig 2: Calculating the product and its leftover

In the majority of computer languages, you may get the quotient and remainder by making use of operators that are particular to that language. The quotient and remainder may be obtained in C, for example, by using the / operator with the % operator.

Two Restrictions: There are two limitations that come with using the division connection mentioned above for cryptographic purposes. To begin, we need the divisor to be an integer (n=0) and positive. Secondly, the residual must be an integer that is not negative ($r \geq 0$).

Example 1.2: As soon as we plug in our calculators or computers, *r* and *q* have a negative impact given that an is negative. Is there a concrete method to make sure that r is always positive? We increase the value of n to r and add a negative integer to the value of q by 1, turning it into a positive integer. For example, −255 equals (−23 × 11) plus (-2) and (−24 × 11) plus 9.

We have reduced -23% to -24% and increased 11 to -23% to get 9 by adding 11. Maintaining the preceding relation's validity.

Cryptography

The Caesar encryption was the first encryption used in cryptography. Both ciphers and contemporary cryptographic techniques used keys and plaintext, but ciphers were much simpler to decipher. Despite their simplicity, ancient ciphers were the first methods of encryption. The algorithms and cryptosystems used today are state-of-the-art. For the utmost security during transmission and storage, they use several rounds of ciphers and encrypt messages' ciphertext. Nowadays, there are cryptographic techniques that cannot be reversed, guaranteeing that the communication will remain secure indefinitely.

Data security is becoming more and more of a priority, which caused cryptography methods to advance in sophistication. The majority of the algorithms and ciphers used in the first stages of cryptography have been cracked, rendering them ineffective in safeguarding data. Although modern algorithms can be cracked, it would take a very long time-sometimes decades-to figure out what a single message meant. So, the pursuit of ever-more-advanced cryptographic methods is far from over.

The field of computer science known as cryptography focuses on making plain text unintelligible. Confidentiality, authentication, data integrity, and other forms of information security are the focus of cryptography, the study of mathematical formulae and methods. "Cryptography" descended that derive from the Greek terms "kryptos" (meaning "Secret") and "graphein" (meaning "Writing"), by which the English word "the art or science of secret writing" was borrowed. Ancient peoples used hidden writing on stones as a foundation for cryptography Egyptians used as early as 1900 B.C.

Uses of Number Theory in Real Life in Cryptography

The field including the study and application of encrypting messages in order to prevent their decipherment or alteration by unauthorized parties. Secure communications, online privacy, and digital transactions are just a few of the many sectors where it has become an essential component.

Types of Cryptography

Symmetric key cryptography

When encrypting and decrypting, use the same keys. Private keys, secret keys, and other similar terms, as well as single-key encryption, are all features of synthetic key cryptography. In these kinds of systems, the private key is something that every user needs.

Asymmetric key cryptography

Using public and secret keys is one use case for asymmetric encryption. For this reason, they are also known as algorithms that use public keys. Even if a single key is known to everybody, an encrypted message employing a public key can only be deciphered with the recipient's private key. cryptography. Making it more secure than symmetric encryption methods.

One-way hash algorithms

Cryptographic hash algorithms, often called digests, accept strings of varying lengths as input and produce strings of set lengths as output. The cipher is a function that generates an output hash that deciphers the input data.

Conclusion

With its deep roots in ancient mathematics and its continued relevance in contemporary applications, elementary number theory is still a vital and important area of study. Its core ideas, which range from divisibility and prime number qualities to congruences and Diophantine equations, offer a strong basis for comprehending complex integer connections. With its vital role in computer science, coding theory, and cryptography, the field's importance goes well beyond pure mathematics. Elementary number theory's applications in these fields show how useful it is in our increasingly digitized society. In coding theory, number-theoretic concepts facilitate the creation of error-correcting codes that guarantee data integrity, while in cryptography, they provide secure communication networks. Number theory influences algorithm design and analysis in computer science, which advances computational efficiency and problem-solving skills. Elementary number theory research keeps resolving long-standing issues and revealing new information. The discipline appeals to both experienced researchers and beginning mathematicians due to its combination of profound intricacy and accessibility. Going forward, elementary number theory is expected to continue to be at the forefront of mathematical research, propelling technological advancements and expanding our comprehension of the basic properties of numbers. Elementary number theory continues to influence our comprehension of mathematics and its practical ramifications in the contemporary world because of its persistent relevance and extensive applicability.

References

1. Gavirangaiah K. Applications of number theory in cryptography. Shodhkosh: Journal of Visual and Performing Arts. 2023;4. doi:10.29121/shodhkosh.v4.i2.2023.4021.
2. Peranginangin A. Application of number theory in cryptography. International Journal of Educational Research Excellence (IJERE). 2024;3(1):67–76. doi:10.55299/ijere.v3i1.733.
3. Ethan A, Khan K. Exploring the use of number theory in modern cryptography: advancements and applications; c2023.
4. Hou B. Number theory based modern cryptography: RSA and Diffie–Hellman algorithms. Theoretical and Natural Science. 2024;51:107–113. doi:10.54254/2753-8818/51/2024CH0180.
5. Vladimirovich VS, Vostokova RP, Borisov S. Number theory and applications in cryptography. Chebyshevskii Sbornik. 2018;19(3):61–73. doi:10.22405/2226-8383-2018-19-3-61-73.
6. Shang W. Development of number theory and the application in cryptography. Theoretical and Natural Science. 2023;2:188–193. doi:10.54254/2753-8818/2/20220139.
7. Castro F. The evolution of cryptography through number theory. arXiv. 2024. doi:10.48550/arxiv.2411.14451.
8. Yaqoob A. Number theory and cryptography: unraveling the foundations of data security. 2022.
9. Salunkhe H, Karande S. Applications of number theory in asymmetric cryptography. 2023;43:59–66.

Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.