Number Theory and Cryptography

By: Ceisly Andino

In our increasingly digital and interconnected world, the importance of cryptography cannot be overstated. It plays a vital role in securing sensitive information, protecting privacy, and ensuring the integrity of data. Today, we will delve into the fundamental concepts of number theory and understand how they underpin the foundations of modern cryptography. So, let's begin our journey into the realm of numbers and encryption.

In today's digital age, where vast amounts of information are transmitted and stored electronically, the need for secure communication and data protection has become paramount. Cryptography serves as the cornerstone of achieving these objectives. It provides a set of mathematical techniques and algorithms that enable us to transform information into an unintelligible form, ensuring that only authorized parties can access and understand it.

Number Theory - Basic Overview

Number theory is the branch of mathematics that deals with the properties and relationships of numbers. It is a field that has captivated mathematicians for centuries and has played a crucial role in the development of cryptography. Let's explore the historical significance of number theory and introduce some key concepts within this fascinating branch of mathematics.

- ❖ Key concepts in number theory:
    - Prime Numbers
    - Modular Arithmetic
    - Euler's Totient Function.

Modular Arithmetic

- Modular arithmetic is a system of arithmetic that introduces the concept of "wrapping around" or "clock arithmetic." It operates within a finite range, called the modulus, and has a significant role in encryption algorithms. Let's delve into modular arithmetic, exploring its operations and its relevance in encryption algorithms.

Modular Addition and Modular Subtraction

- Modular addition is the operation of adding numbers within a modulus. It can be defined as follows: given two numbers, a and b, and a modulus m, the modular sum of a and b, denoted as (a + b) mod m, is the remainder obtained when the sum of a and b is divided by m. In other words, it is the value that "wraps around" within the modulus range.

For example, let's consider modular addition with modulus 7:

➔ (3 + 5) mod 7 = 1, since 3 + 5 = 8, and 8 divided by 7 leaves a remainder of 1.

➔ (6 + 4) mod 7 = 3, as 6 + 4 = 10, and dividing 10 by 7 gives a remainder of 3.

Modular addition is a fundamental operation in encryption algorithms, allowing secure computations within a finite range.

- Modular subtraction operates similarly to modular addition. Given two numbers, a and b, and a modulus m, the modular difference of a and b, denoted as (a - b) mod m, is the remainder obtained when the subtraction of b from a is divided by m.

For example, let's consider modular subtraction with modulus 7:

➔ (9 - 4) mod 7 = 5, since 9 - 4 = 5, and dividing 5 by 7 leaves a remainder of 5.

➔ (2 - 6) mod 7 = 3, as 2 - 6 = -4, and dividing -4 by 7 results in a remainder of 3.

Modular subtraction allows for computations that "wrap around" within the modulus, ensuring values stay within the defined range.

Modular multiplication

Modular multiplication is the operation of multiplying numbers within a modulus. Given two numbers, a and b, and a modulus m, the modular product of a and b, denoted as (a * b) mod m, is the remainder obtained when the product of a and b is divided by m.
For example, let's consider modular multiplication with modulus 7:

➔ (3 * 4) mod 7 = 5, since 3 multiplied by 4 equals 12, and dividing 12 by 7 leaves a remainder of 5.

➔ (6 * 2) mod 7 = 5, as 6 multiplied by 2 is 12, and dividing 12 by 7 results in a remainder of 5.

Modular multiplication is a crucial operation in encryption algorithms, enabling secure computations within a limited range.

Cryptography - Introduction

Cryptography is the practice of securing communication from adversaries by converting information into an unintelligible form. It is an essential field that plays a critical role in ensuring the confidentiality, integrity, and authenticity of data. Let's explore the two main branches of cryptography and emphasize the importance of number theory in both branches.

➔ Symmetric key cryptography

  - Symmetric key cryptography, also known as secret key cryptography, is a cryptographic technique where the same key is used for both encryption and decryption. The key must be kept secret and shared between the communicating parties beforehand.

➔ Public Key Cryptography

  - Public key cryptography, also known as asymmetric key cryptography, employs a pair of distinct but mathematically related keys: a public key and a private key. The public key is freely available to anyone, while the private key remains secret and known only to the key owner.

By leveraging the principles of number theory, cryptographic algorithms can achieve the desired security properties necessary for protecting sensitive information and ensuring secure communication.

In conclusion, we have explored the fascinating world of number theory and its critical role in the field of cryptography. Here are the key points we discussed:

➔ Cryptography is the practice of securing communication by converting information into an unintelligible form.
➔ The two main branches of cryptography are symmetric key cryptography and public key cryptography.
➔ Symmetric key cryptography uses the same key for encryption and decryption, relying on number theory concepts for key generation and secure computations.
➔ Public key cryptography uses a pair of mathematically related keys (public and private keys) and leverages number theory for key pair generation and security properties.
➔ Number theory concepts, such as prime numbers, modular arithmetic, and Euler's totient function, are crucial in both symmetric key and public key cryptography.
➔ Prime numbers provide uniqueness and computational complexity, while modular arithmetic ensures secure computations within a finite range.
➔ Euler's totient function aids in generating secure key pairs, and number theory forms the basis of computational problems that are difficult to solve.

Overall, number theory provides a foundation for understanding the properties and relationships of numbers, and its concepts have numerous applications in various fields.