Use of Modular Arithmetic in Cryptography

G11 – SY IT A2
Hiral Patel – 16010421071
Karan Patel – 16010421072
Keyur Patel - 16010421073

Cryptography is the practice of secure communication in the presence of third parties or adversaries. It involves using mathematical techniques and algorithms to encrypt and decrypt messages, ensuring that they can only be read by the intended recipients.

Modular arithmetic is a branch of mathematics that deals with operations on integers, where the result of the operation is restricted to a certain range. This property of modular arithmetic makes it useful in cryptography, where secure communication is important.

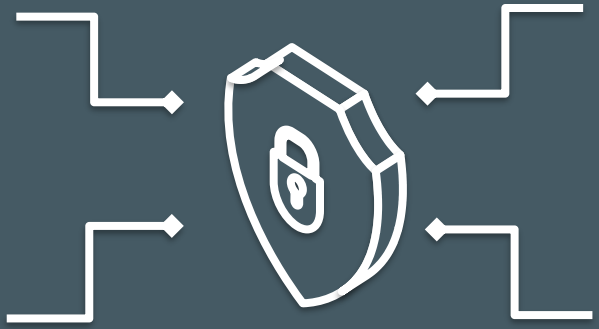
Modular arithmetic has several important properties that make it useful in cryptography, including:

- It is reversible, meaning that given the result of an operation and one of the operands, it is possible to find the other operand.
- It is easy to compute using modern computing technology.
- It is difficult to compute the original operands given only the result of an operation.

- Public Key Cryptography: This involves using two related keys, one for encryption and one for decryption, where the keys are based on the properties of modular arithmetic.
- Hash Functions: These are used to generate fixed-length values from variable-length input data, and are based on modular arithmetic operations.
- Digital Signatures: These are used to verify the authenticity of digital documents and are based on modular arithmetic operations.

Use of Modular Arithmetic in Cryptography

A key is a value that is used to encrypt and decrypt messages. In public key cryptography, two related keys are used a public key for encryption and a private key for decryption. Key exchange protocols allow two parties to agree on a shared secret key that can be used for encryption and decryption of messages. Modular arithmetic is used in key exchange protocols to ensure that the shared secret key is secure and cannot be easily guessed by an attacker. A common protocol is the Diffie-Hellman key exchange.



When data is transmitted over a network or stored on a disk, errors can occur due to noise or other factors. Error detection and correction algorithms are used to ensure that the data is received or stored correctly. Modular arithmetic is used in error detection and correction algorithms to generate check codes that can be used to detect errors and correct them if they occur. One commonly used algorithm that uses modular arithmetic for error detection and correction is the cyclic redundancy check (CRC).

Random numbers are often used in cryptography to generate keys or as inputs to cryptographic algorithms. However, generating truly random numbers is difficult, so cryptographers often use pseudorandom number generators (PRNGs) to generate sequences of numbers that appear random. Modular arithmetic is used in the calculation of PRNGs to ensure that the generated numbers are uniformly distributed and unpredictable. One commonly used PRNG that uses modular arithmetic is the linear congruential generator (LCG).

Cryptographic hash functions are used to create fixed-length outputs from variable-length inputs. They are often used in digital signatures and data integrity checks. Cryptographic hash functions use modular arithmetic operations to compute a hash value from the input data. A hash function is difficult to find two inputs that produce the same hash value and it is difficult to find an input that produces a given hash value. One commonly used cryptographic hash function that uses modular arithmetic is the Secure Hash Algorithm (SHA).