# Cryptography

# Cryptography

- Cryptography is a technique
  - of securing information and communications using codes
  - to ensure confidentiality, integrity and authentication.

- preventing unauthorized access to information

- prefix "crypt" means "hidden" and
- suffix "graphy" means "writing"

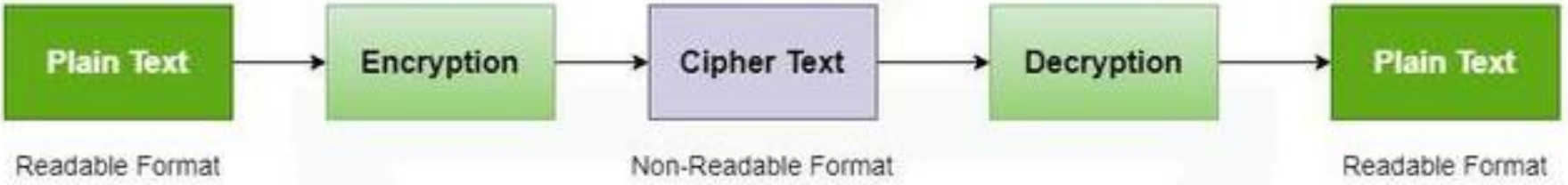
# Cryptography

- the techniques that are used
  - to protect information are obtained from mathematical concepts and
  - a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode them.

# Cryptography

- These algorithms are used for
  - cryptographic key generation,
  - digital signing,
  - verification to protect data privacy,
  - web browsing on the internet and
  - to protect confidential transactions such as credit card and debit card transactions

# Cryptography



# Features of Cryptography

- **Confidentiality:**
  - Information can only be accessed by the person for whom it is intended and
  - no other person except him can access it.

- **Integrity:**
  - Information cannot be modified in storage or transition between sender and
  - intended receiver without any addition to information being detected.

# Features of Cryptography

- **Non-repudiation**:
- The sender cannot deny his intention to send information at a later stage

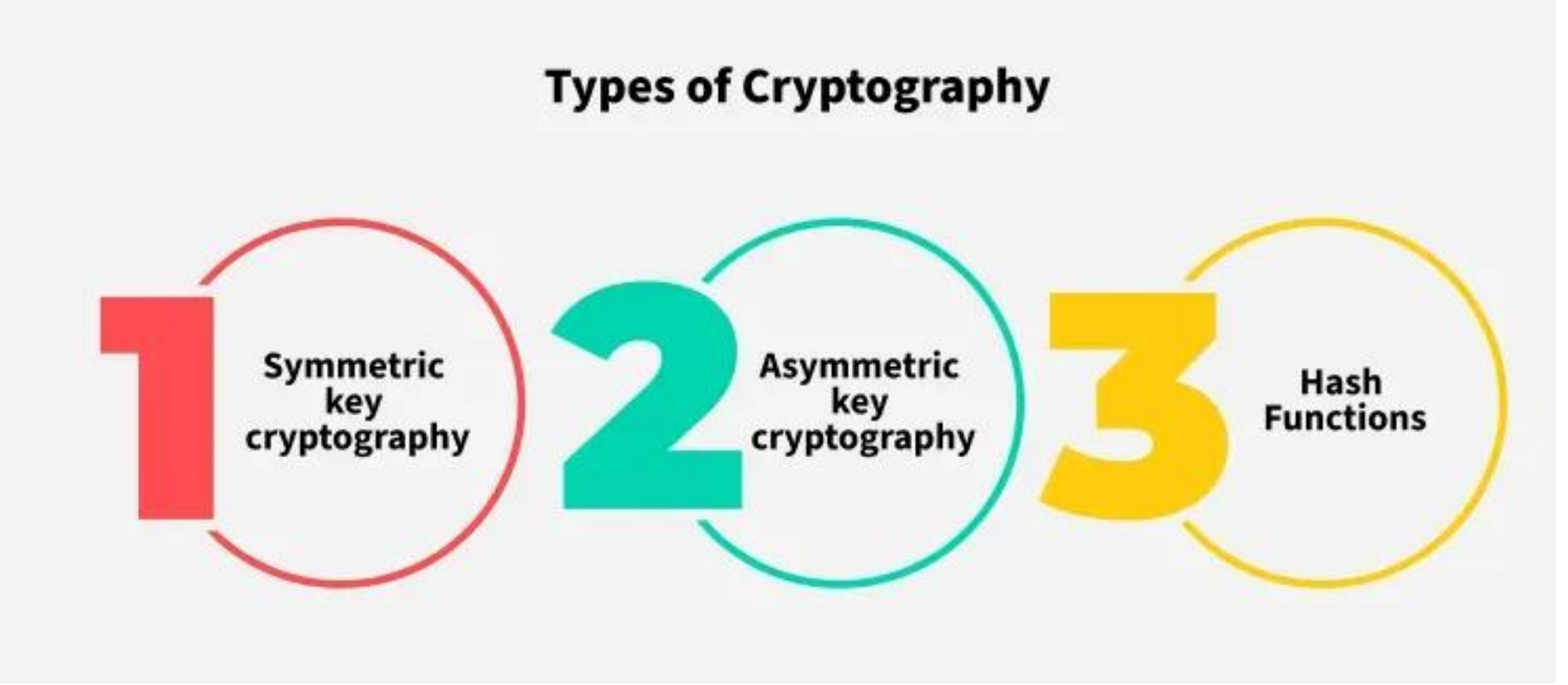
- **Authentication:**
- The identities of the sender and receiver are confirmed.
- As well destination/origin of the information is confirmed.

# Features of Cryptography

- **Interoperability:**
- Cryptography allows for secure communication between different systems and platforms

- **Adaptability:**
- Cryptography continuously evolves to stay ahead of security threats and technological advancements.

# Types of Cryptography



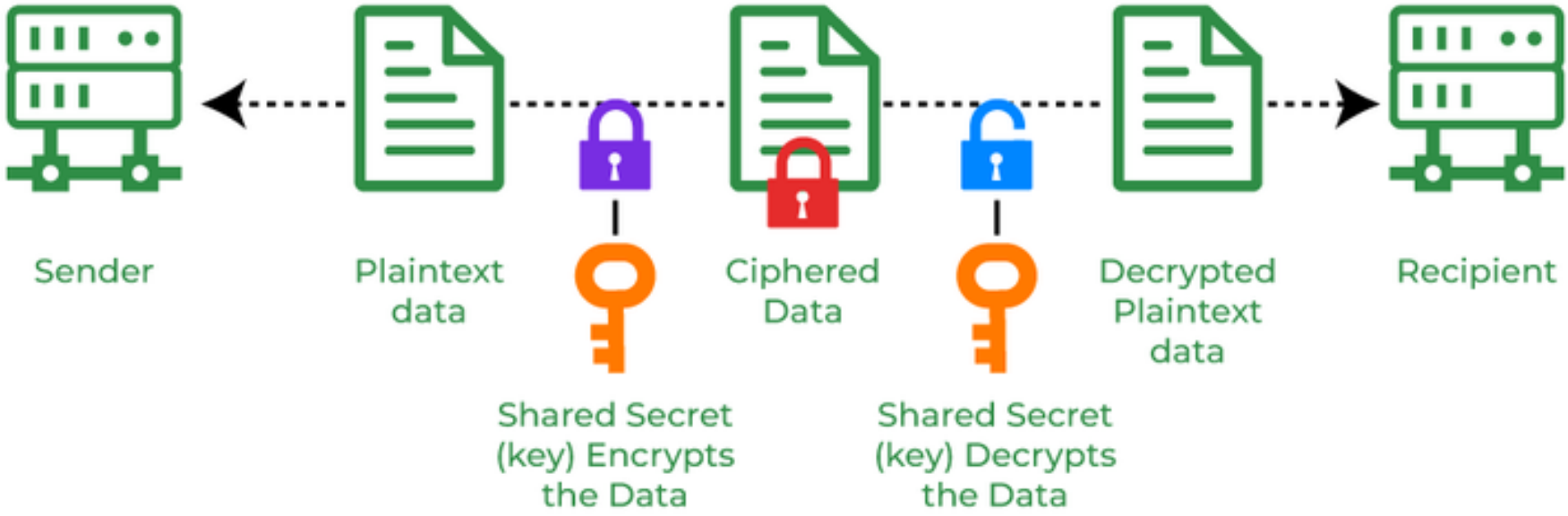
# 1. Symmetric Key Cryptography

- is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages.

- faster and simpler but the problem is that the sender and receiver have to somehow exchange keys securely

- The popular symmetric key cryptography systems are
  - Data Encryption Systems (DES) and
  - Advanced Encryption Systems (AES).

# 1. Symmetric Key Cryptography



# 2. Asymmetric Key Cryptography

- a pair of keys is used to encrypt and decrypt information.
- A sender's public key is used for encryption and a receiver's private key is used for decryption
- Public keys and Private keys are different.
- Even if the public key is known by everyone the intended receiver can only decode it because he holds his private key.

# 2. Asymmetric Key Cryptography

- The most popular asymmetric key cryptography algorithm is the RSA algorithm

# 3. Hash Functions

- There is no key required in hash function cryptography

- as it uses mathematical equations to genrate a hash message for nay arbitrary length of message, and the output will be of fixed length.

- Some of the famous hash function are:
- SHA-256
- MD5
- MD6

# Applications of Cryptography

- Cryptography has wide area of applications in the modern world, where the technology is rapidly evolving

- From authentication measures to cryptocurrencies, cryptography is here to stay, these are some of the most common applications of cryptography listed below:

# Computer passwords:

- When a user logs in, their password is hashed and compared to the hash that was previously stored

- Passwords are hashed and encrypted before being stored

- In this technique, the passwords are encrypted so that even if a hacker gains access to the password database, they cannot read the passwords.

# Digital Currencies:

- To protect transactions and prevent fraud, digital currencies like Bitcoin also use cryptography

- Complex algorithms and cryptographic keys are used
  - to safeguard transactions,
  - making it nearly hard to tamper with or forge the transactions.

# Secure web browsing:

- Online browsing security is provided by the use of cryptography,

- which shields users from eavesdropping and man-in-the-middle assaults.

- Public key cryptography is
  - by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
  - to encrypt data sent between the web server and the client, establishing a secure channel for communication

# Electronic Signatures:

- Electronic signatures serve as the digital equivalent of a handwritten signature and are used to sign documents

- Digital signatures are created using cryptography and can be validated using public key cryptography

- In many nations, electronic signatures are enforceable by law, and their use is expanding quickly.

# Authentication:

- Cryptography is used for authentication in many different situations, such as
  - when accessing a bank account,
  - logging into a computer, or
  - using a secure network

- Cryptographic methods are employed by authentication protocols to confirm the user's identity and confirm that they have the required access rights to the resource.

# Cryptocurrencies:

- Cryptography is
  - used by cryptocurrencies like Bitcoin and Ethereum
  - to protect transactions, thwart fraud, and maintain the network's integrity

- Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.

# End-to-end Internet Encryption:

- End-to-end encryption is used to protect two-way communications like video conversations, instant messages, and email.

- Even if the message is encrypted, it assures that only the intended receivers can read the message.

- End-to-end encryption is widely used in communication apps like WhatsApp and Signal, and it provides a high level of security and privacy for users.

# Types of Cryptography Algorithm

- Cryptography Algorithms can be classified into several categories based on
  - the way they utilize and
  - manage their keys,
  - their efficiency and workflow,

- here are the most common algorithms

# Advanced Encryption Standard (AES)

- AES is a popular encryption algorithm which uses the same key for encryption and decryption

- It is a symmetric block cipher algorithm with block size of 128 bits, 192 bits or 256 bits

- AES algorithm is widely regarded as the replacement of DES (Data encryption standard) algorithm.

# Data Encryption Standard (DES):

- DES is an older encryption algorithm that is used to convert 64-bit plaintext data into 48-bit encrypted ciphertext.

- It uses symmetric keys (which means same key for encryption and decryption)

- It is kind of old by today's standard but can be used as a basic building block for learning newer encryption algorithms

# RSA(Rivest-Shamir-Adleman)

- RSA is an basic asymmetric cryptographic algorithm which uses two different keys for encryption.

- The RSA algorithm works on a block cipher concept that converts plain text into cipher text and vice versa.

# Secure Hash Algorithm (SHA):

- SHA is used to generate unique fixed-length digital fingerprints of input data known as hashes
- SHA variations such as SHA-2 and SHA-3 are commonly used to ensure data integrity and authenticity
- The tiniest change in input data drastically modifies the hash output, indicating a loss of integrity
- Hashing is the process of storing key value pairs with the help of a hash function into a hash table.

# Advantages of Cryptography

- used for access control to ensure that only parties with the proper permissions have access to a resource.

- For secure online communication, it offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the Internet.

- It helps in the defense against various types of assaults including replay and man-in-the-middle attacks.

# Advantages of Cryptography

- It help firms in meeting a variety of legal requirements including data protection and privacy legislation.