Basic Terminologies

- **Plain Text :** Data that can be read and understand without any special measure(original message).
- **Cipher Text:** Data that is transformed or converted by Encryption algorithm(coded message).
- **Encryption:** Algorithm for transforming plain text to cipher text.
- **Decryption:** Algorithm for transforming cipher text to plain text.
- **Key:** It is used for encryption and decryption of message.
- **Cryptography:** It is the science of using mathematics to encrypt and decrypt data

Objectives of Cryptography

- Confidentiality
- Integrity
- Non repudiation
- Authentication

Cont….

- **Confidentiality**
  - The protection of data from unauthorized disclosure.
  - Confidentiality is the protection of transmitted data from passive attacks
- **Integrity**
  - The assurance that data received are exactly as sent by authorized entity
  - Data integrity is the protection of transmitted data from active attacks

Cont. …

- **Non-repudiation**
  - Non-repudiation prevents either sender or receiver from denying a transmitted message.
- **Authentication**
  - It is concerned with assuring that a communication is authentic, i.e. assure the recipient message is from the source that it claims to be.

Types of Cryptography

- **Followings are the Types of Cryptography:**
  - Symmetric cipher
  - Asymmetric cipher

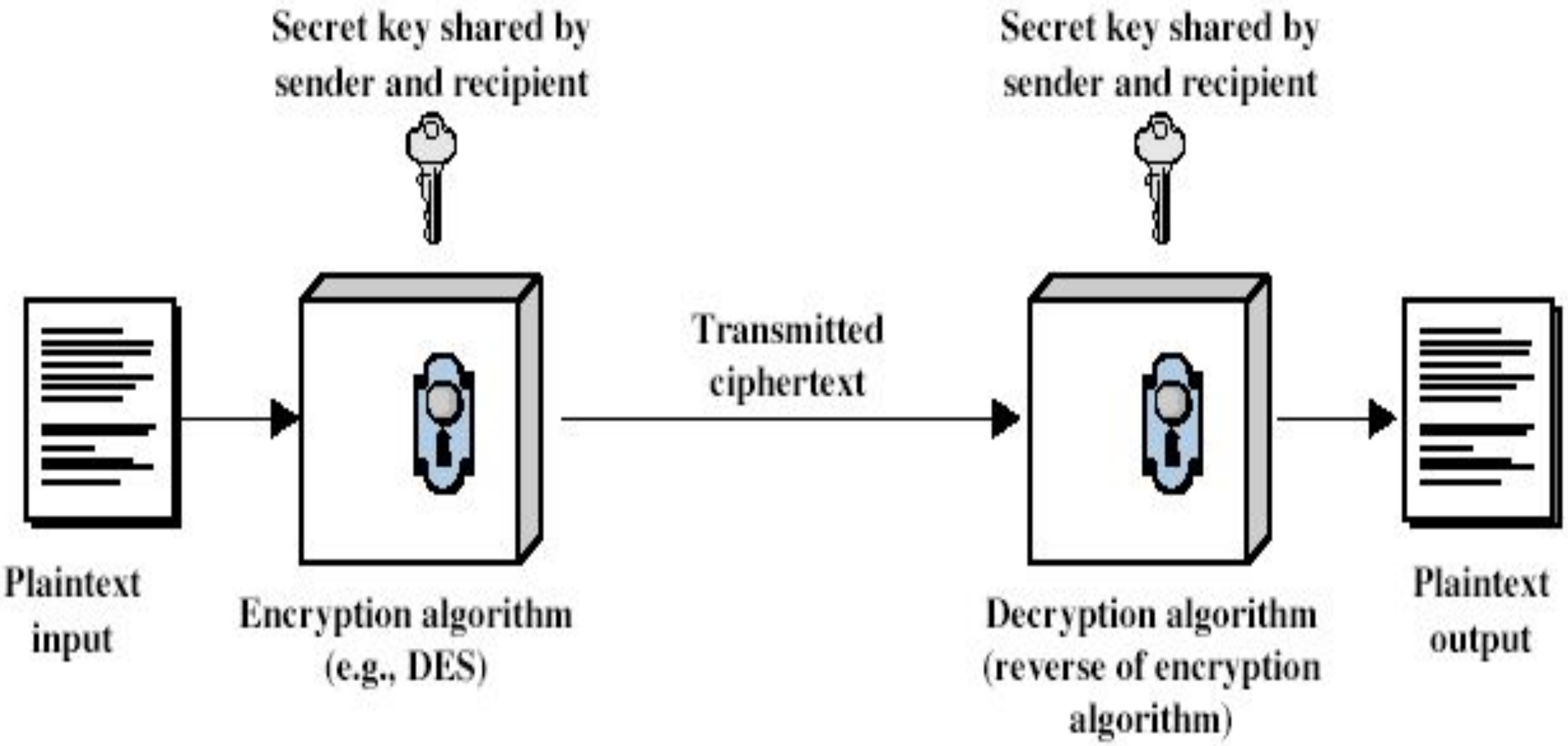
Cont.…

- **VIRUS:**
  - A computer virus is a malicious program that self-replicates via copying itself to another program. In different phrases, the computer
  - virus spreads with the aid of itself into other executable code or documents.
  - Almost all viruses are connected to an executable document, which means the virus may also exist on your pc but it surely cannot infect your computer unless you run or open the malicious program.
  - It is important to note that a virus cannot be spread without a human action(such as running an infected program).

Symmetric cipher

- Both sender and receiver use single same key for Encryption and Decryption
- It is also known as Conventional Cryptography/Secret Key /Private Key
- Example :DES

Symmetric Cipher Model

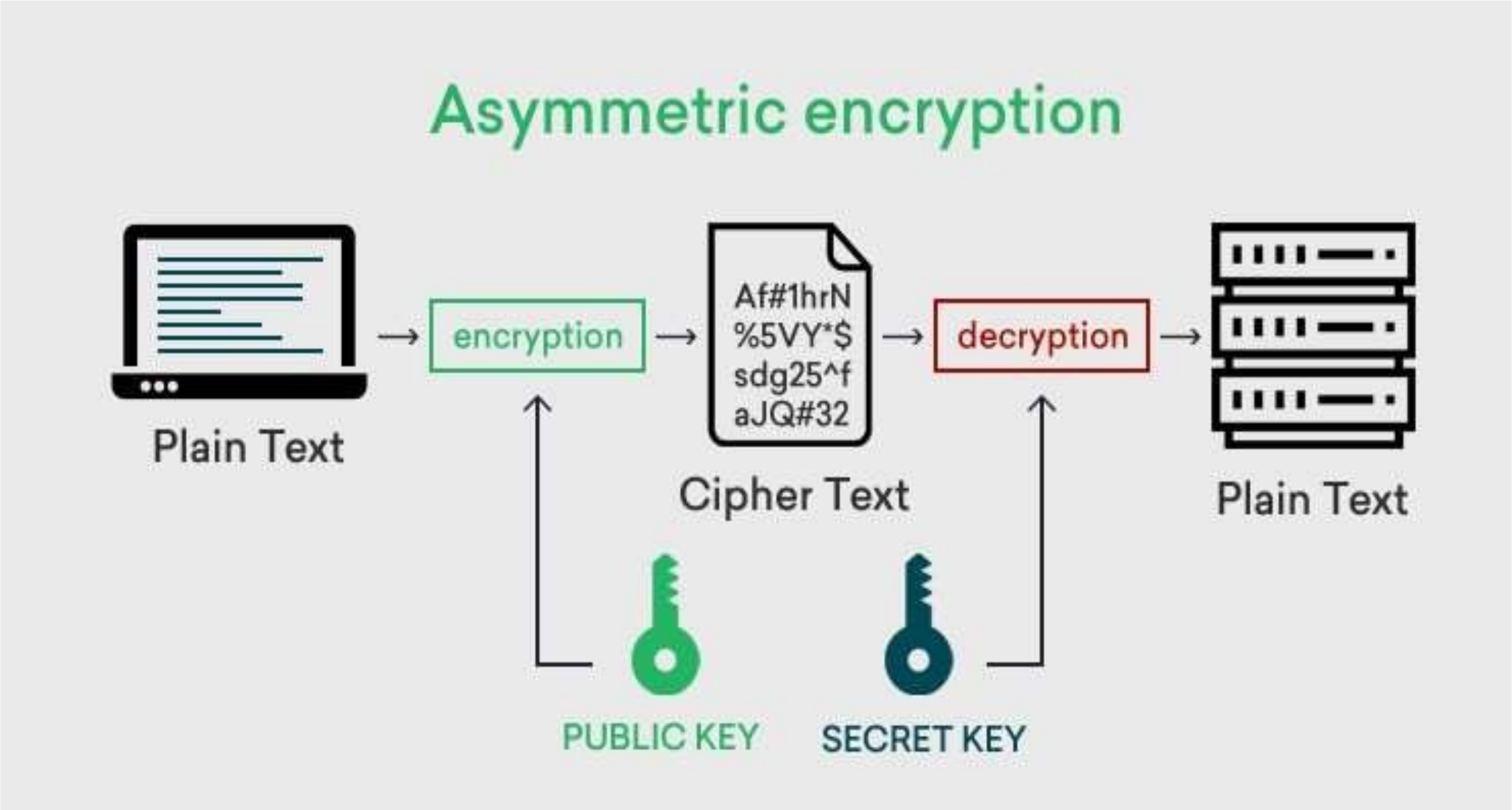


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Asymmetric Cipher Model

- **Asymmetric cryptography,** also known as public-key cryptography.
- It is a process that uses a pair of related keys one public key and one private key to encrypt and decrypt a message and protect it from unauthorized access or use.
- **A private key** also known as a secret key is shared only with key's initiator.
- **Example:** RSA algorithm

Asymmetric Cipher Model



Encryption Algorithm

- **Type of operation used**

  1. Substitution : Elements of plaintext are mapped into another element
  2. Transposition : Elements of plaintext are rearranged

- **Some of the Substitution Techniques are**

  - Caesar cipher
  - Playfair cipher
  - Hill cipher
  - Vigenere cipher (Auto-key system)
  - Vernam cipher or One time pad