CSS2C08

COMPUTER NETWORKS

MODULE 5
Security in Networks

1. **Principles of cryptography**
2. Authentication
3. Integrity
4. Key distribution and certification
5. Firewalls
6. Attacks and counter measures

Security in Networks

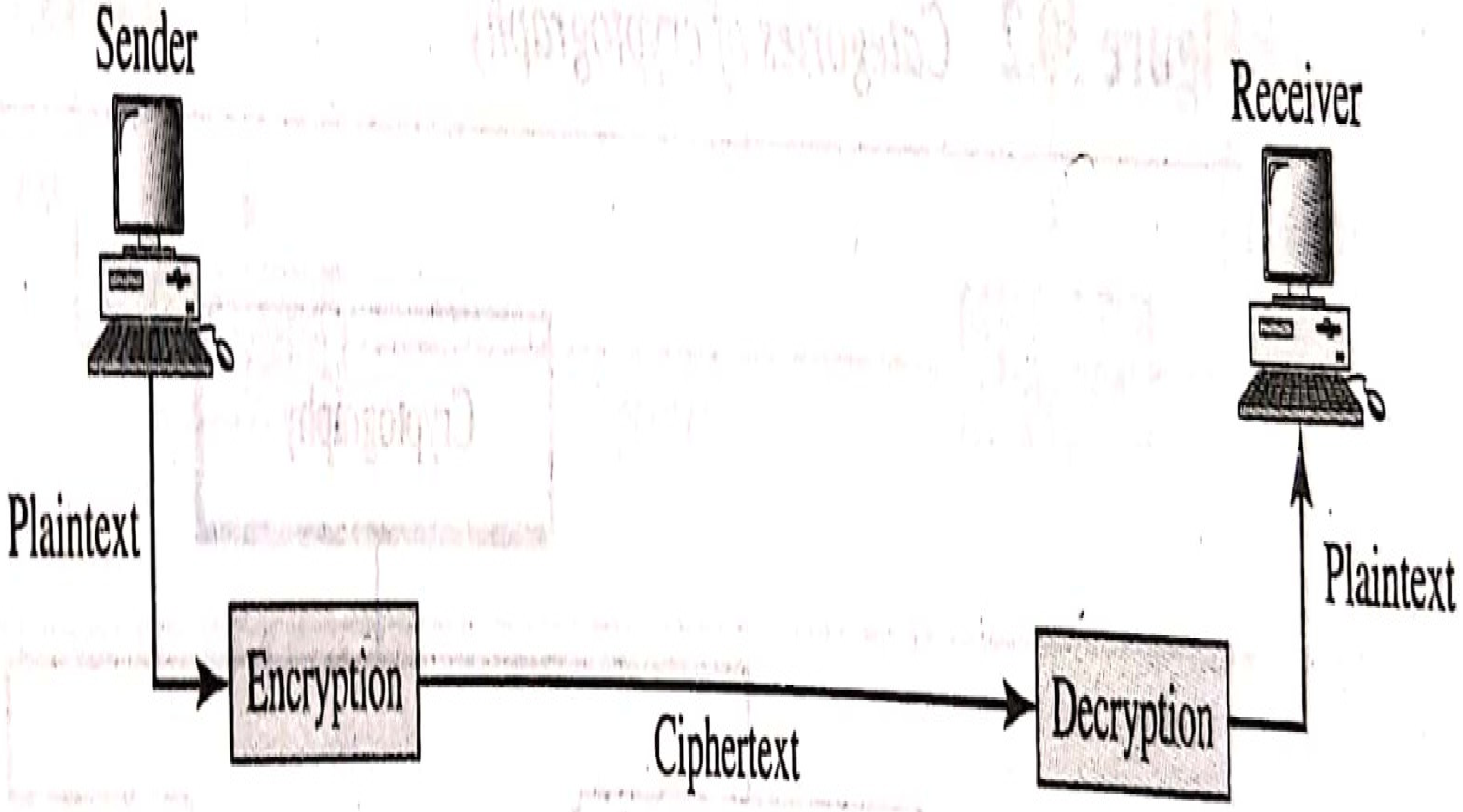
- **Network Security:**
  - It is measures to protect data during their transmission .
- **Cryptography:**
  - The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form is called cryptography.

Cryptography components:

Plaintext and Ciphertext:

- The original message, before being transformed, is called plaintext.
- After the message is transformed, it is called ciphertext.
- An encryption algorithm transforms the plaintext into ciphertext;
- A decryption algorithm transforms the ciphertext back into plaintext.
- The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

- **Cipher:**
  - We refer to encryption and decryption algorithms as ciphers.
  - The term cipher is also used to refer to different categories of algorithms in cryptography.
- **Key:**
  - A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on.
  - To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext. These create the ciphertext.
  - To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

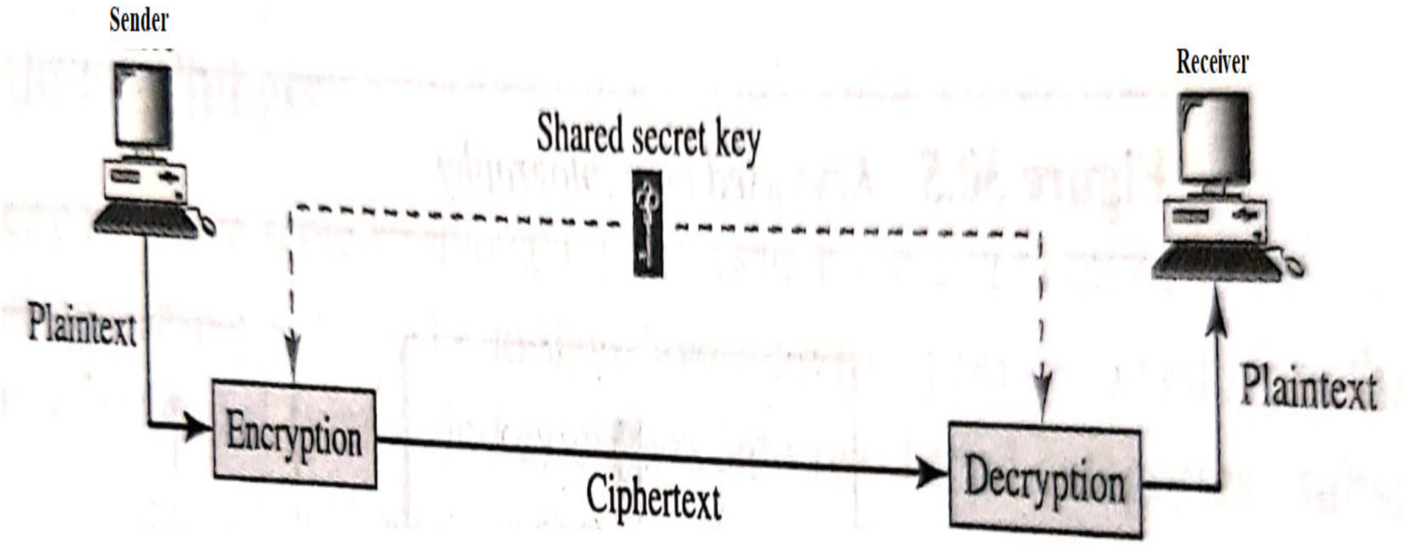

Sender
Receiver
Plaintext
Encryption
Ciphertext
Decryption
Plaintext

- We can divide all the cryptography algorithms (ciphers) into two groups:

  1. Symmetric key (also called secret-key) cryptography algorithms
  2. Asymmetric (also called public-key) cryptography algorithms.

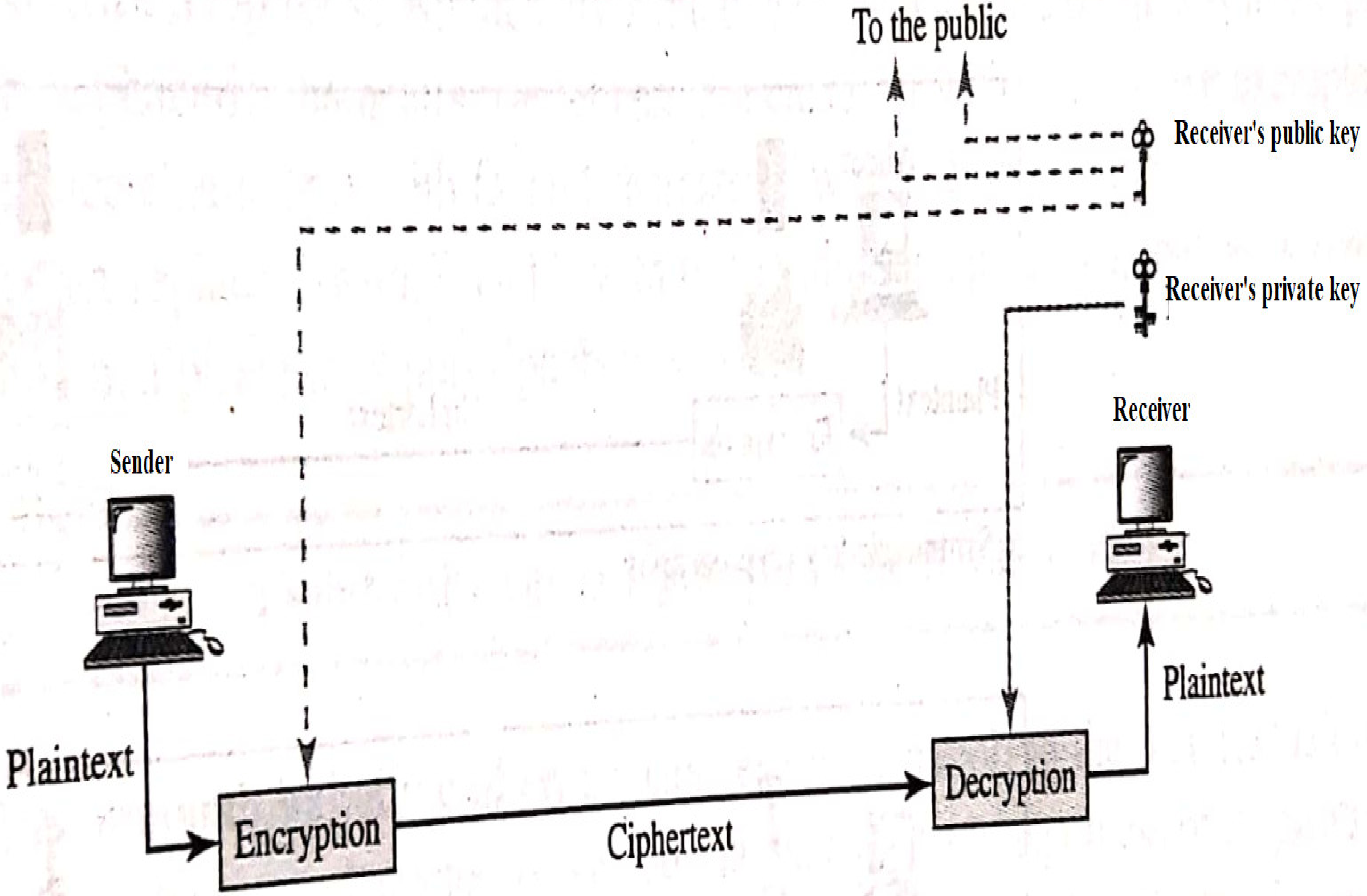
1. Symmetric Key Cryptography:

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data .



2. Asymmetric-Key Cryptography

- ❖In asymmetric or public-key cryptography, there are two keys: a private key and a public key.
- ❖The private key is kept by the receiver.
- ❖The public key is announced to the public.
- ❖In public-key encryption/decryption:
    - ❖ the public key that is used for encryption
    - ❖ the private key that is used for decryption.
- ❖The public key is available to the public;
- ❖the private key is available only to an individual.


To the public
Receiver's public key
Receiver's private key
Receiver
Sender
Plaintext
Encryption
Ciphertext
Decryption
Plaintext