INTRODUCTION

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of inter connected networks.

WHY WE NEED INFORMATION SECURITY?

Because there are threats

Threats: A threat is an object, person, or other entity that represents a constant danger to an asset.

Threat Categories

- Acts of human error or failure Compromises to intellectual property
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism deliberate acts of theft
- Deliberate software attack Forces of nature
- Deviations in quality of service Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolesce

Security Approaches:

Here are some common security approaches:

Symmetric-key cryptography: Using the same key for encryption and decryption (e.g., AES).

Asymmetric-key cryptography: Using a pair of keys: public for encryption and private for decryption (e.g., RSA).

Hash-based cryptography: Using one-way hash functions for data integrity and authenticity (e.g., SHA-256).

Digital signatures: Using asymmetric cryptography to authenticate and ensure non-repudiation.

Homomorphic encryption: Enabling computations on encrypted data without decrypting it first.

Principles of Security:

1. Defense in depth: Layering multiple security mechanisms to protect against various threats.
2. Least privilege: Granting only necessary access rights and permissions.
3. Segregation of duties: Dividing responsibilities to prevent single points of failure.
4. Secure communication protocols: Using protocols like TLS, IPsec, and SSH to protect data in transit.
5. Regular updates and patching: Keeping software and systems up-to-date to prevent exploitation of known vulnerabilities.
6. Monitoring and incident response: Detecting and responding to security incidents.
7. User education and awareness: Educating users about security best practices and threats.

NOTE:

1. TLS: Transport Layer Security, 2. IPsec: Internet Protocol Security, 3. SSH: Secure Shell

Types of Security Attacks: Security attacks are actions taken to compromise the integrity, confidentiality, or availability of computers, networks, or data. These attacks come in various types, each exploiting different vulnerabilities.

1. **Brute-force attacks**: Trying all possible keys or combinations to decrypt data.
2. **Side-channel attacks**: Exploiting implementation flaws or environmental factors (e.g., timing, power consumption).
3. **Differential cryptanalysis**: Analyzing differences in cipher text to deduce encryption keys.
4. **Linear cryptanalysis**: Using linear approximations to attack block ciphers.
5. **Man-in-the-middle (MITM) attacks**: Intercepting and altering encrypted communications.
6. **Replay attacks**: Reusing encrypted messages to gain unauthorized access.

7. **Key exhaustion attacks**: Forcing a system to generate new keys, potentially leading to weak keys.
8. **Quantum computer attacks**: Using quantum computers to break certain encryption algorithms.

ASPECTS OF SECURITY

There are 3 aspects of information security:

Security Attack
Security Mechanism
Security Service

Security Attacks, Services and Mechanisms: To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

SECURITY SERVICES: The classification of security services are as follows:

Confidentiality: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.

E.g. Printing, displaying and other forms of disclosure.

Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating anddelaying or replaying of transmittedmessages.

Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.
Availability: Requires that computer system assets be available to authorized parties when needed.

SECURITY MECHANISMS: One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are
Encipherment: It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used encryption keys.

Digital Signature: The appended data or a cryptographic transformation applied to any data unit allowing to prove the source and integrity of the data unit and protect against forgery.

Access Control: A variety of techniques used for enforcing access permissions to the system resources
Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
Routing Control: Enables selection of particular physically secure routes for certain data and allows routing changes once a breach of security is suspected.

Notarization: The use of a trusted third party to assure certain properties of a data exchange

Pervasive Security Mechanisms: These are not specific to any particular OSI security service or protocol layer.
Trusted Functionality: That which is perceived to be correct with respect to some criteria.

Security Level: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection: It is the process of detecting all the events related to network security.

Security Audit Trail: Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery: It deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

SECURITY ATTACKS: There are four general categories of attack which are listed below.

Normal flow: It is the foundation against which security teams detect, analyze, and respond to abnormal actions that may pose security threats.
Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.
Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a Computer .e.g., wiretapping to capture data in the network, illicit copying of files

Modification: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.

Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.

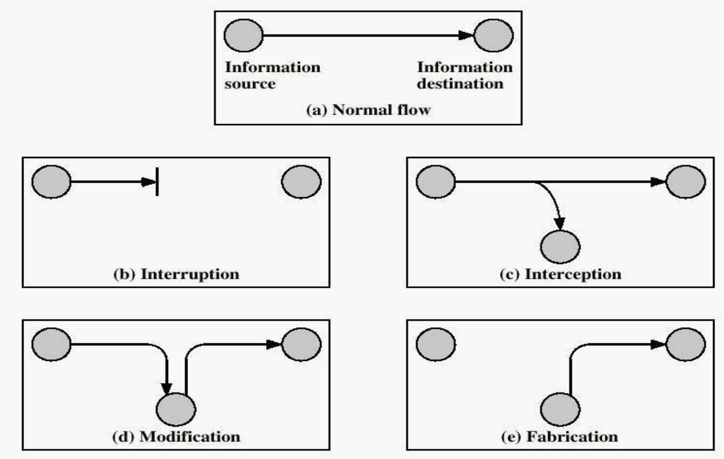


Figure 1.1 Security Threats

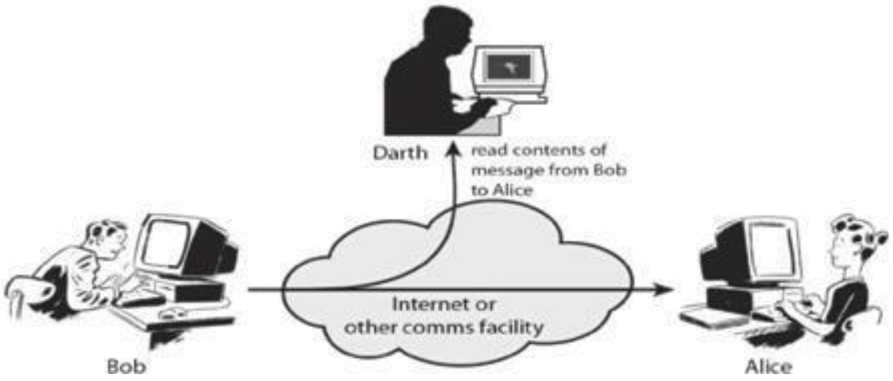
CRYPTOGRAPHIC ATTACKS

PASSIVE ATTACKS: Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

Release of message contents: A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

Traffic analysis: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

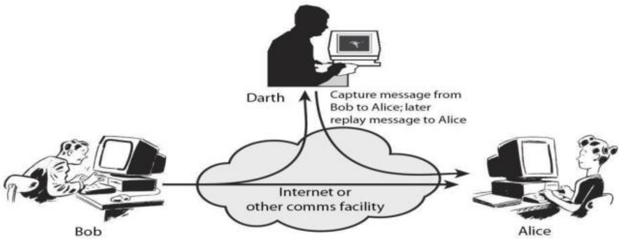
ACTIVE ATTACKS: These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

Masquerade – One entity pretends to be a different entity.

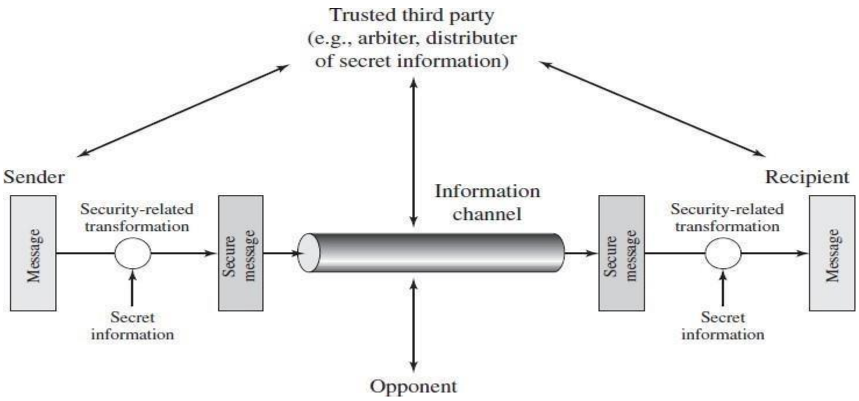
Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance. It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

MODEL FOR NETWORK SECURITY

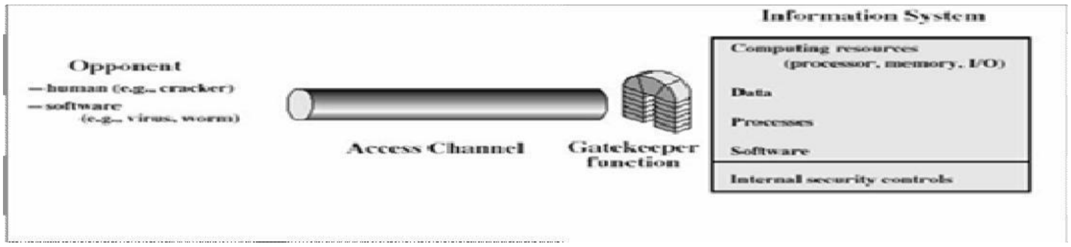


A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Using this model requires us to:

- Design a suitable algorithm for the security transformation.
- Generate the secret information (keys) used by the algorithm
- Develop methods to distribute and share the secret information
- Specify a protocol enabling the principals to use the transformation and secret information for a security service

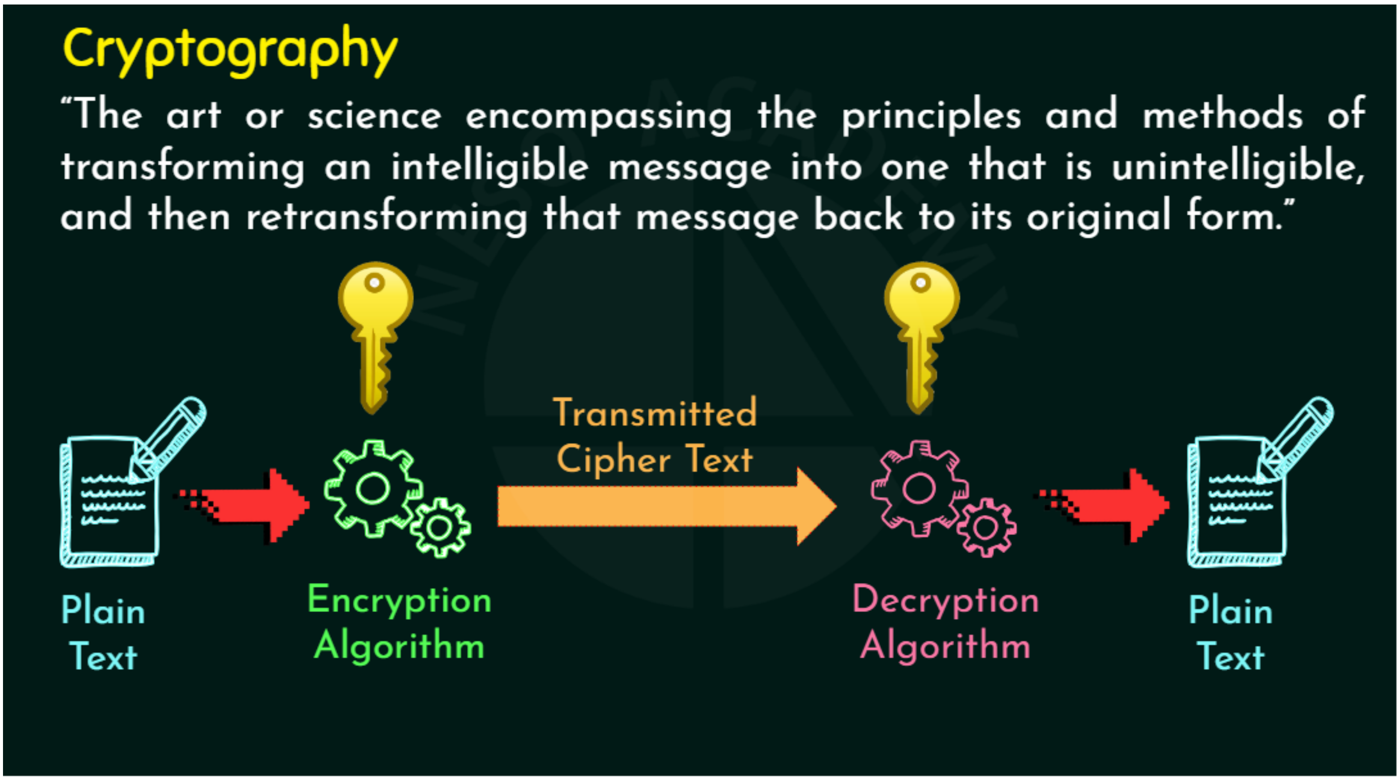
MODEL FOR NETWORK ACCESS SECURITY



Using this model requires us to:

- Select appropriate gatekeeper functions to identify users
- Implement security controls to ensure only authorized user’s access designated information or resources

Trusted computer systems can be used to implement this model



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."

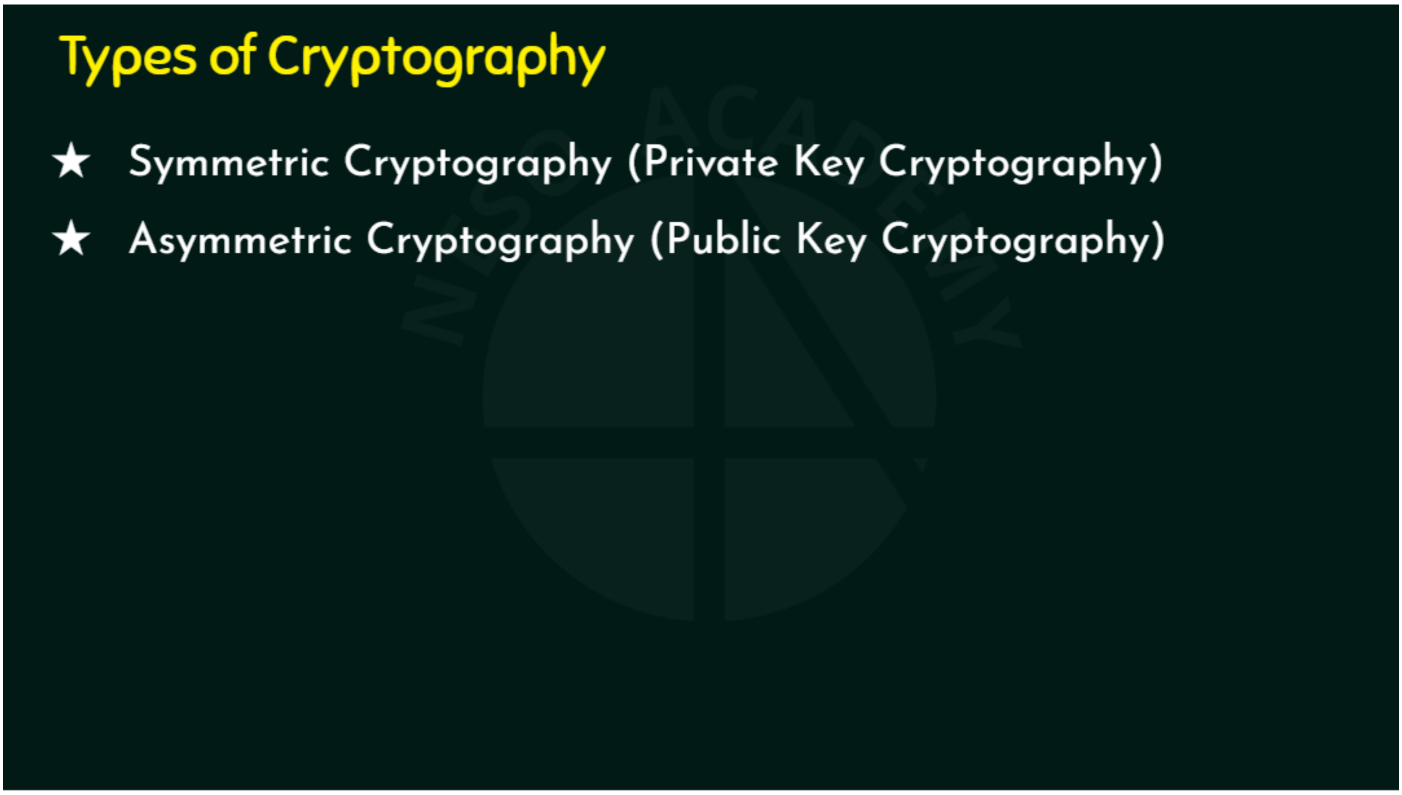
Plain Text

Encryption Algorithm

Transmitted Cipher Text

Decryption Algorithm

Plain Text



Types of Cryptography

★ Symmetric Cryptography (Private Key Cryptography)

★ Asymmetric Cryptography (Public Key Cryptography)

1. Symmetric Key Cryptography

✓ Definition

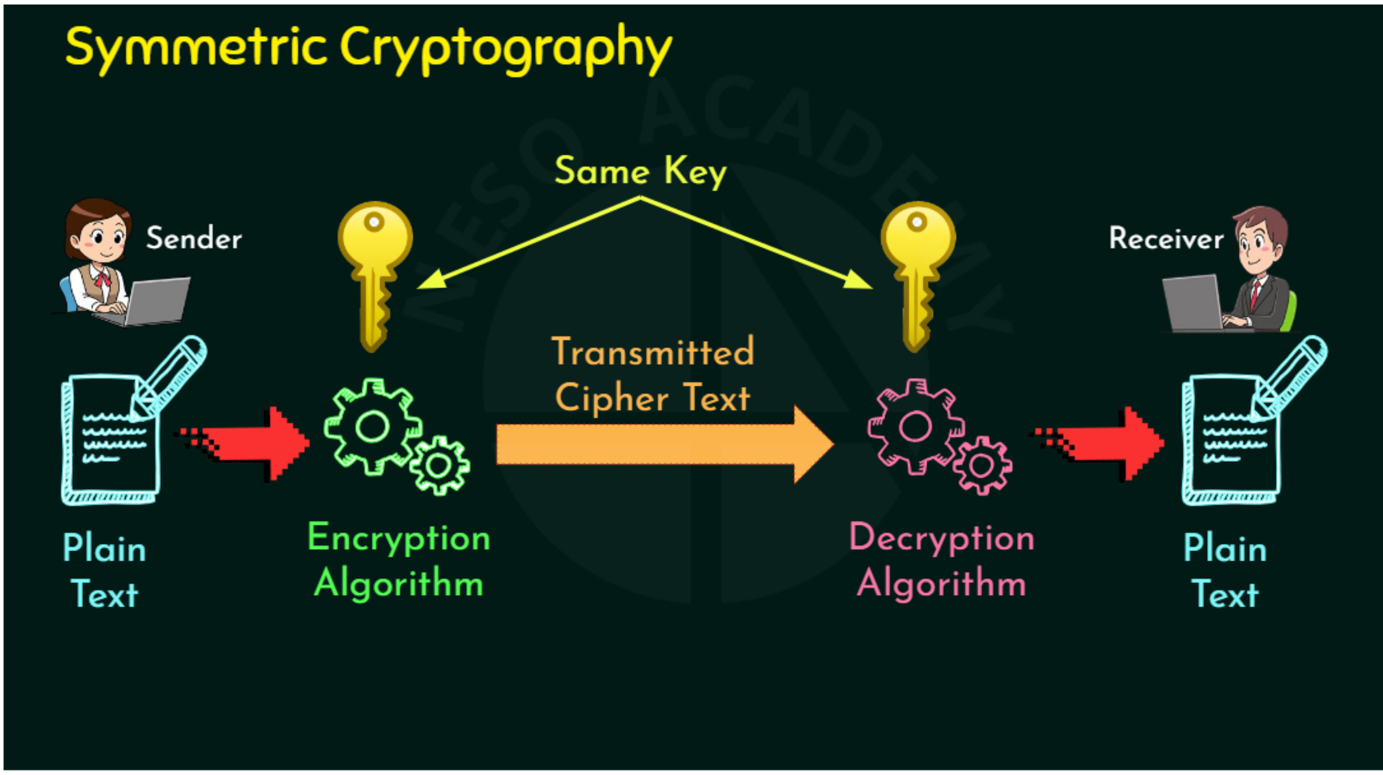
A cryptographic system where the same key is used for encryption and decryption.

✓ Key Idea

☞ One key shared between sender and receiver.

✓ Example

- **AES (Advanced Encryption Standard)**
- **DES (Data Encryption Standard)**
- **RC4, Blowfish**
- **Classical ciphers: Caesar cipher, Playfair, Rail Fence, Columnar, etc.**



-

✓ Advantages

- Very fast
- Suitable for large data
- Simple implementation

✓ Disadvantages

- Key distribution problem
  Both parties must share the key securely.
- Not suitable for open networks.

2. Asymmetric Key Cryptography

✓ Definition

A cryptographic system where two different keys are used:

- Public Key → Used for encryption
- Private Key → Used for decryption

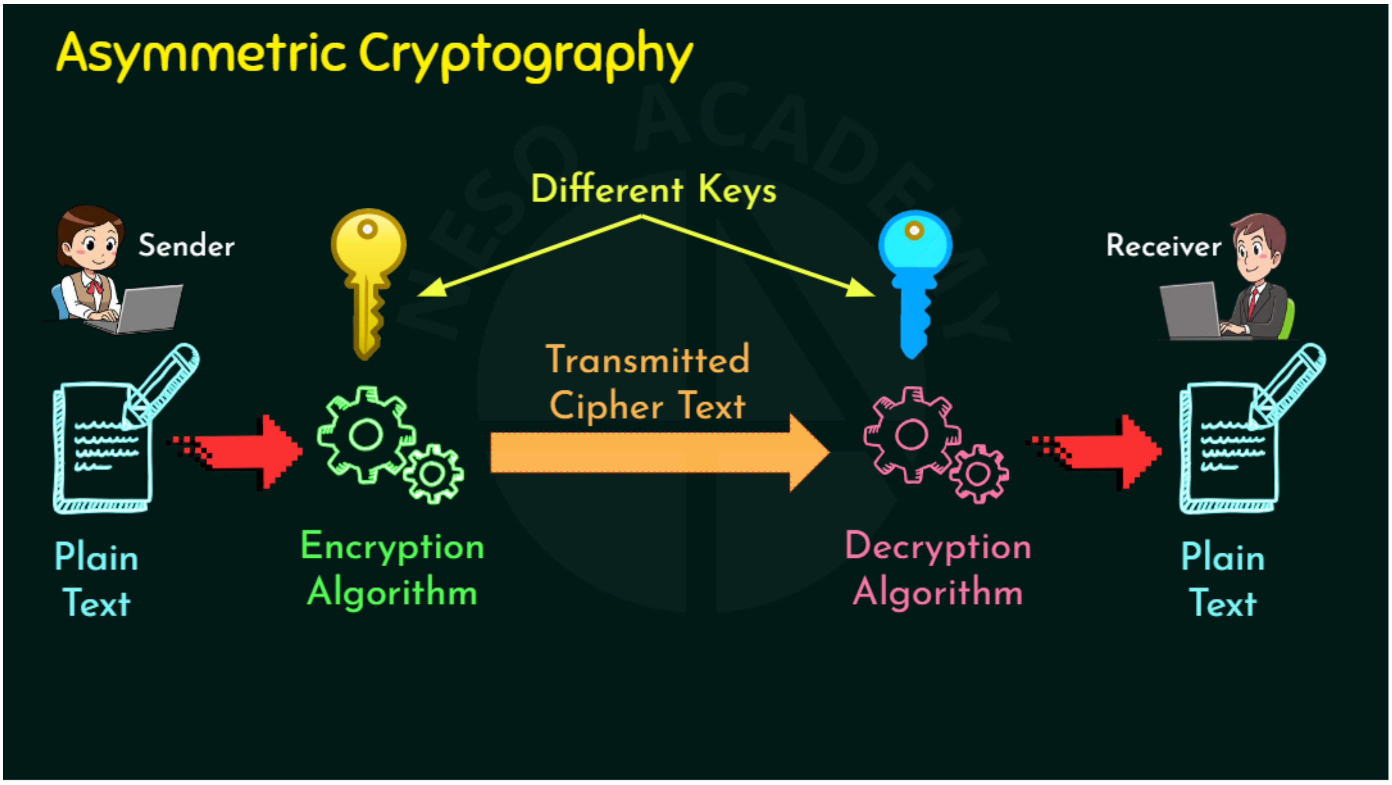
✓ Key Idea

👉 Two keys: One public, one private

👉 What one key encrypts, only the other can decrypt.

✓ Example

- RSA
- Diffie–Hellman
- ECC (Elliptic Curve Cryptography)
- DSA (Digital Signature Algorithm)



Advantages

- **No key sharing problem (public key can be shared openly)**
- **Useful for digital signatures, authentication, secure key exchange**

✓ Disadvantages

- **Slower than symmetric key**
- **More computationally expensive**