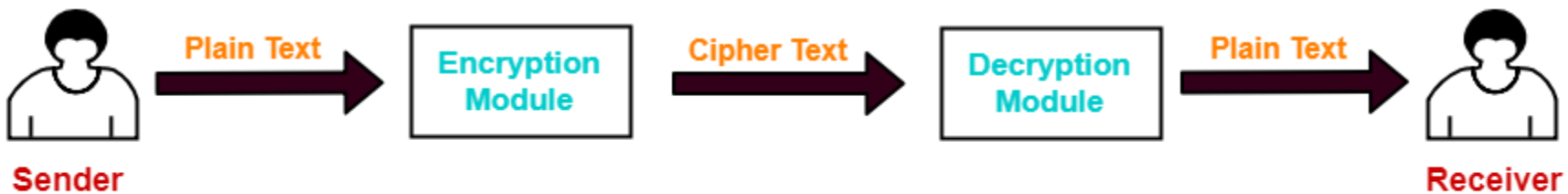
Cryptography and Digital Sig

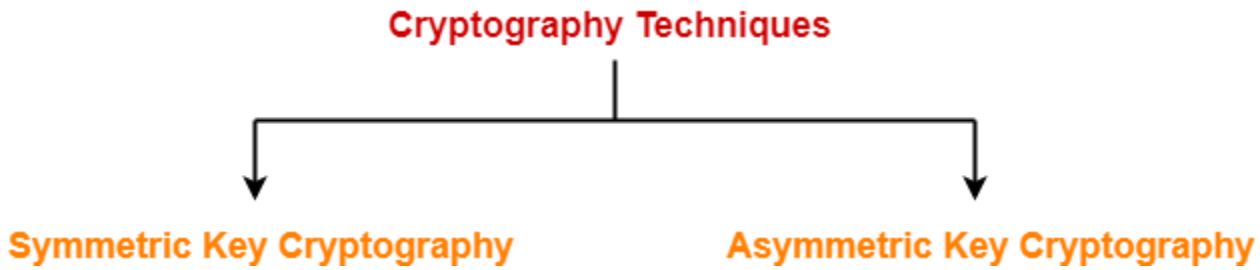
Cryptography in Network Security

- In network security,
- Cryptography is a method of storing and transmitting data in a particular form.
- It ensures that only the person for whom the message is intended can read the message.
- The message exchange using cryptography involves the following steps-



Cryptography

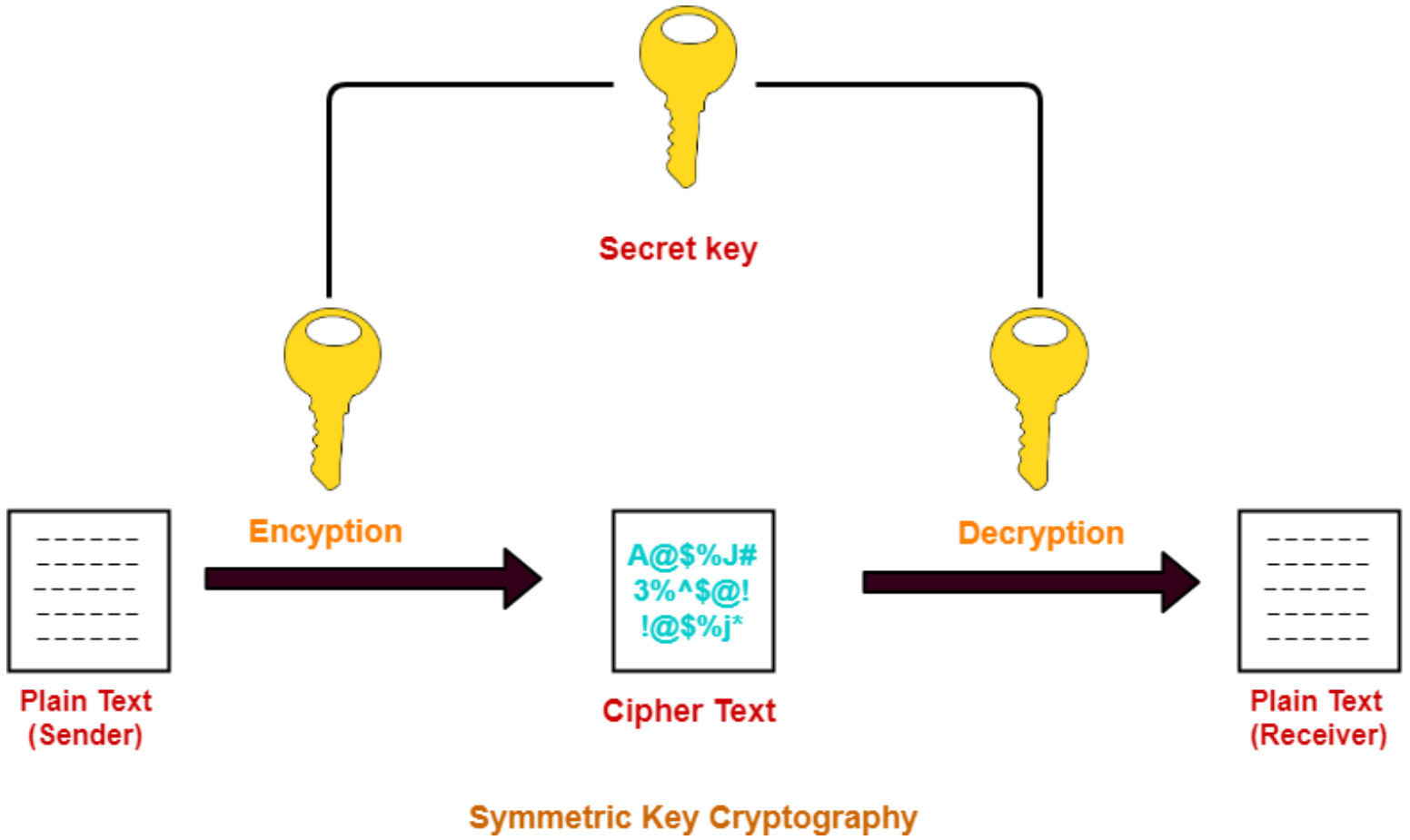
Cryptography Techniques



Symmetric Key Cryptography

- In this technique,
- Both sender and receiver uses a common key to encrypt and decrypt the message.
- This secret key is known only to the sender and to the receiver.
- It is also called as **secret key cryptography**.

Working


Secret key
Encyption
Decryption
A@$%J#
3%^$@!
!@$%j*
Plain Text
(Sender)
Cipher Text
Plain Text
(Receiver)
Symmetric Key Cryptography

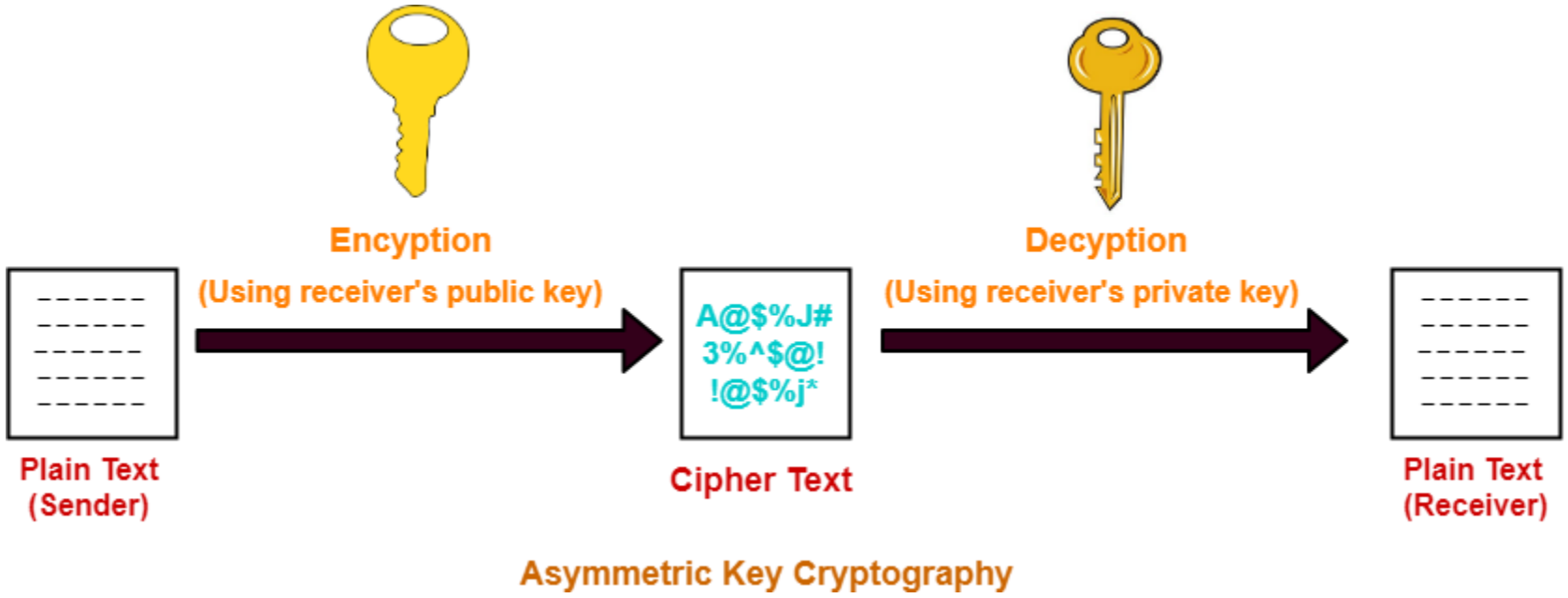
Working

- Before starting the communication, sender and receiver shares the secret key.
- This secret key is shared through some external means.
- At sender side, sender encrypts the message using his copy of the key.
- The cipher text is then sent to the receiver over the communication channel.
- At receiver side, receiver decrypts the cipher text using his copy of the key.
- After decryption, the message converts back into readable format.

Asymmetric Key Cryptography

- In this technique,
- Sender and receiver use different keys to encrypt and decrypt the message.
- It is called so because sender and receiver use different keys.
- It is also called as **public key cryptography**.

Working


Encyption
(Using receiver's public key)
Decyption
(Using receiver's private key)
A@$%J#
3%^$@!
!@$%j*
Plain Text
(Sender)
Cipher Text
Plain Text
(Receiver)
Asymmetric Key Cryptography

- **Step-01:**
- At sender side,
- Sender encrypts the message using receiver’s public key.
- The public key of receiver is publicly available and known to everyone.
- Encryption converts the message into a cipher text.
- This cipher text can be decrypted only using the receiver’s private key.
- **Step-02:**
- The cipher text is sent to the receiver over the communication channel.
- **Step-03:**
- At receiver side,
- Receiver decrypts the cipher text using his private key.
- The private key of the receiver is known only to the receiver.
- Using the public key, it is not possible for anyone to determine the receiver’s private key.
- After decryption, cipher text converts back into a readable format.

Digital Signatures-

- The signature on a document is the proof to the receiver that the document is coming from the correct entity.

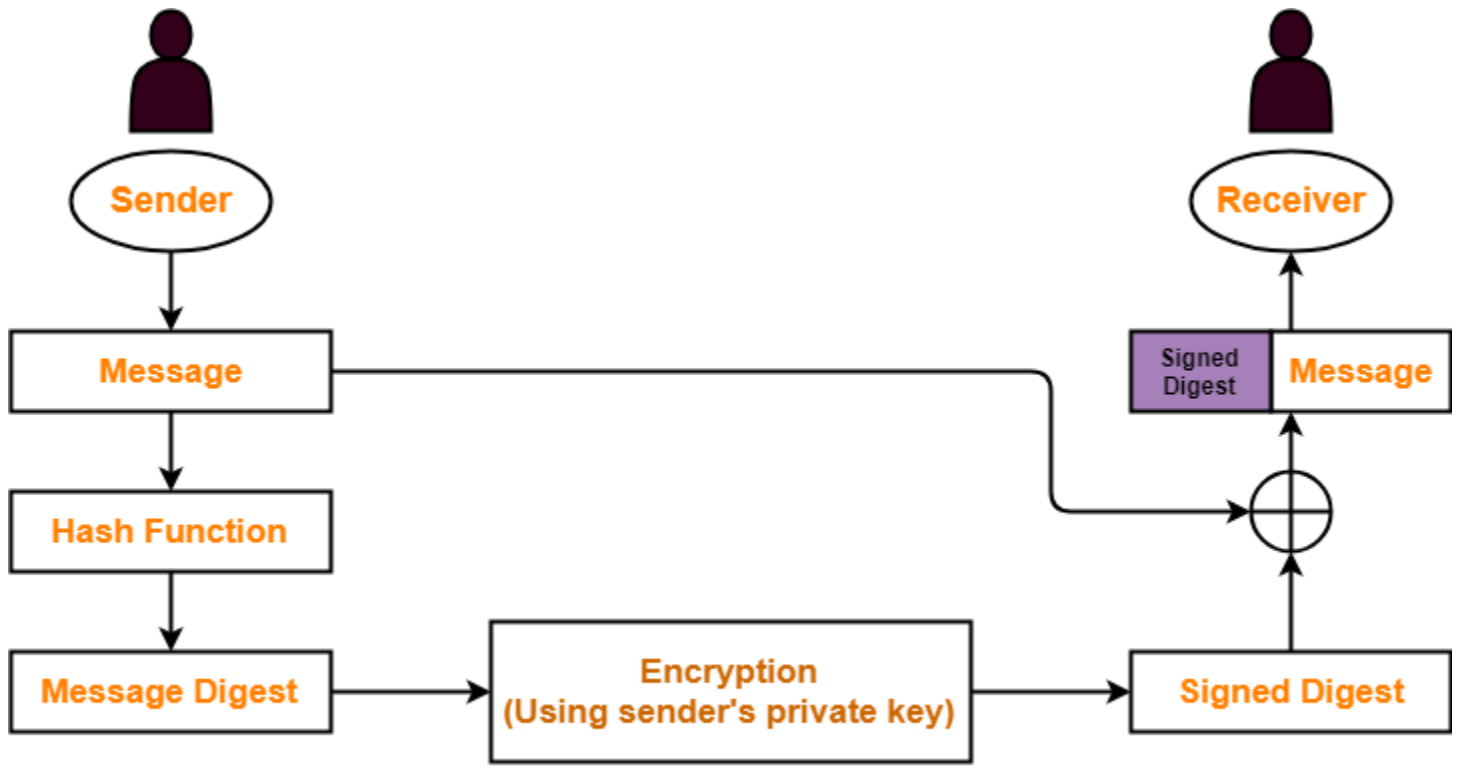
- A digital signature guarantees the authenticity of an electronic document in digital communication.

Digital Signature Working

- The sender of the document digitally signs the document.
- The receiver of the document verifies the signature.

At Sender Side-

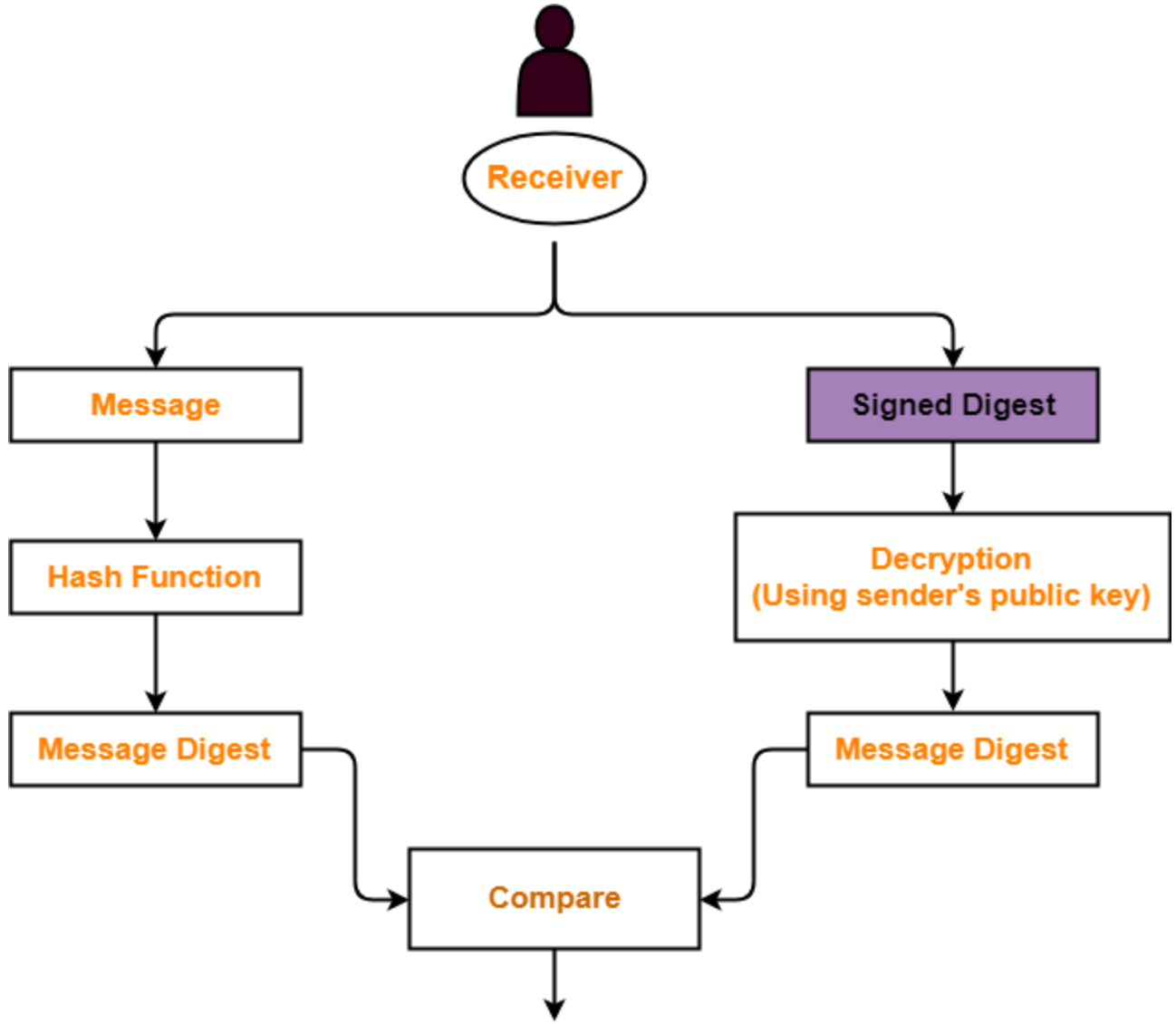
- Using a hash function, sender converts the message to be sent into a digested form.
- There are various hash functions that may be used like SHA-1, MD5 etc.
- The message in digested form is called as **message digest**.
- Sender encrypts the message digest using his private key.
- The encrypted message digest is called as **signed digest** or **signature** of the sender.
- Sender sends the signed digest along with the original message to the receiver.



At Sender Side

At Receiver Side

- At receiver side,
- Receiver receives the original message and the signed digest.
- Using a hash function, receiver converts the original message into a message digest.
- Also, receiver decrypts the received signed digest using the sender’s public key.
- On decryption, receiver obtains the message digest.
- Now, receiver compares both the message digests.
- If they are same, then it is proved that the document is coming from the correct entity.



At Receiver Side