Digital Signatures

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.

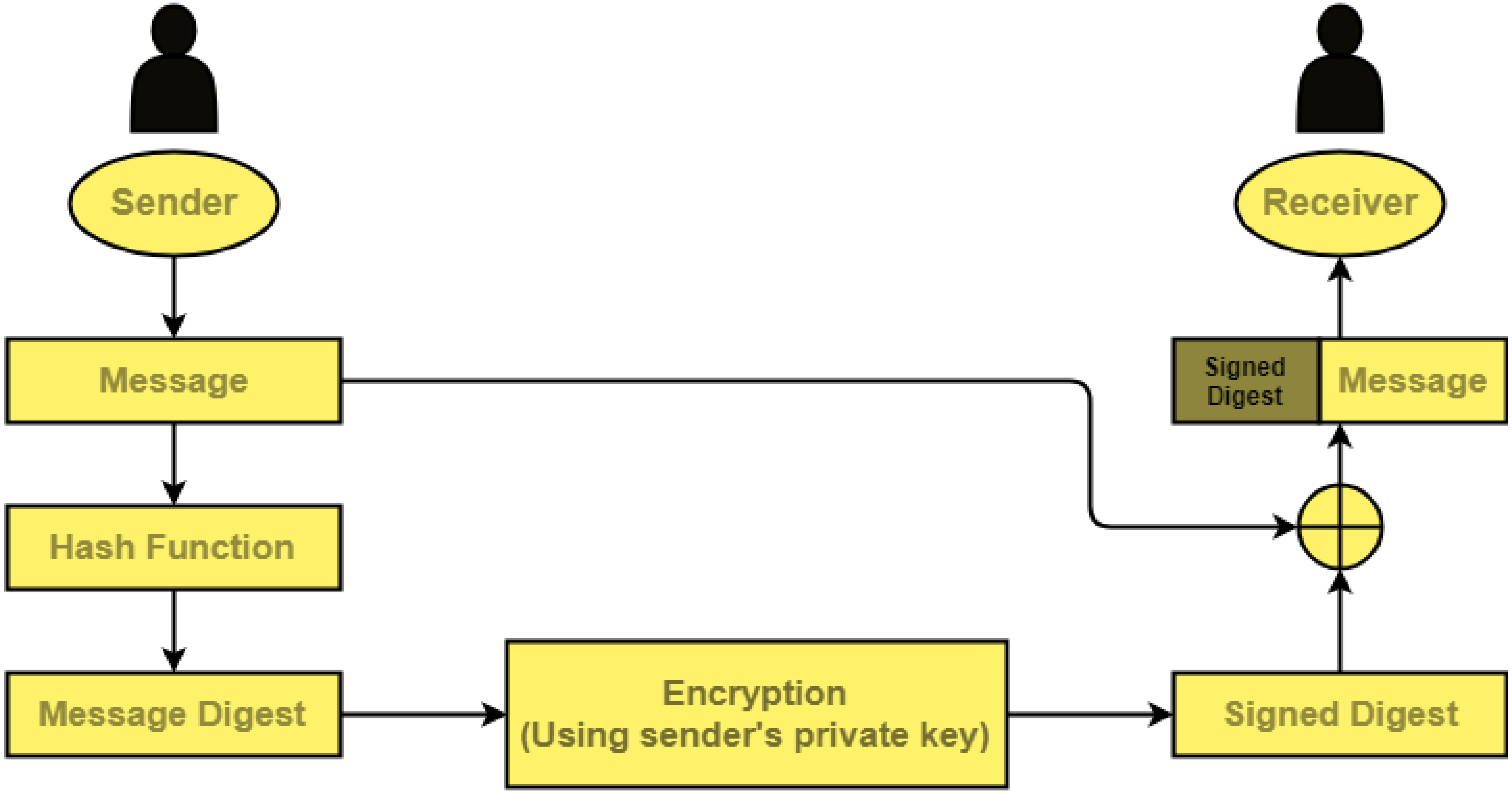
How Digital Signature Works?

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

The steps involved in the digital signature algorithm are:

At Sender Side-

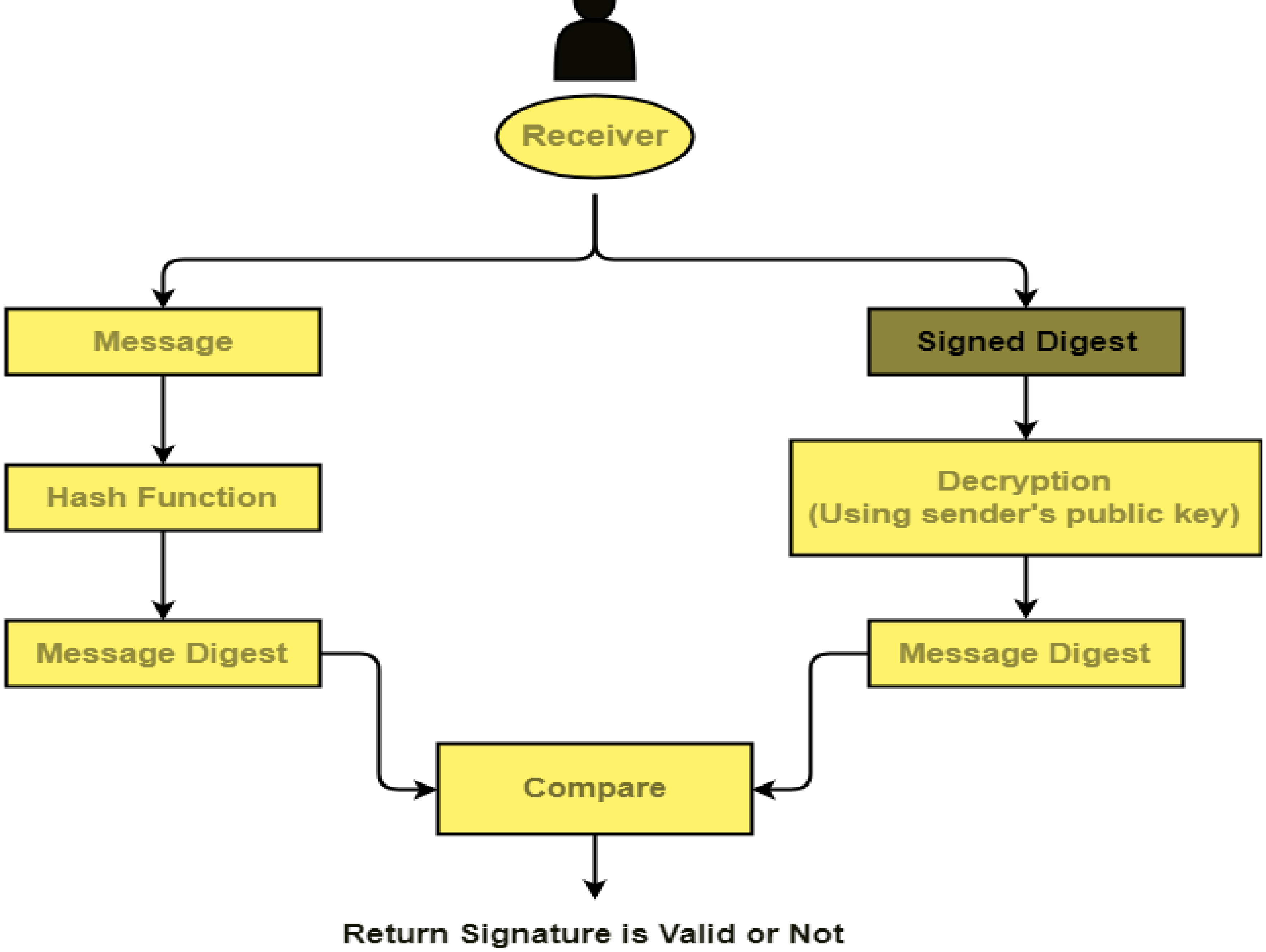
- Using a hash function, sender converts the message to be sent into a digested form.
- There are various hash functions that may be used like SHA-1, MD5 etc.
- The message in digested form is called as **message digest**.
- Sender encrypts the message digest using his private key.
- The encrypted message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

- 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

NOTE:

Point-01:

After digitally signing the document, sender sends the following two things to the receiver-

- **Signed digest or signature**
- **Original message**

Point-02:

- **Sender uses his private key to digitally sign the document.**
- **Receiver uses the sender’s public key to verify the signature.**

Point-03:

- **Digital signature of a person varies from document to document.**
- **This ensures authenticity of the document.**

Point-04:

In digital signature,

- **There is one to one relationship between a message and a signature.**
- **Each message has its own signature.**

Point-05:

Digital signature verifies-

- **Authenticity**
- **Integrity**
- **Non-repudiation**