3. Digital certification 📄

Digital certificate

> An electrical document used to prove the identity of a website or individual. It contains a public key and information identifying the website owner or individual, issued by a **Certificate Authority (CA)**

Contains:

- Serial number
- Hashing algorithm
  - To produce the message digest
- Public key
  - To decrypt/encrypt data
- Dates valid
- Name of organization
- Signature to verify it came from the issuers
- Name of issuer
- Purpose of the public key
- Thumb print/finger print algorithm

  > This is the hash function used to produce a message digest

- CA digital certificate

Explain how asymmetric encryption uses the content of the digital certificate to ensure that the message has not been altered during transmission

- A's message is encrypted using B's public key
- A's hashing algorithm is used on the message to produce the message digest
- The message digest is then encrypted with A's private key to provide a digital signature
- Both the encrypted message and the digital signature is sent
- The message is decrypted with B's private key
- A's digital signature is decrypted with A's public key to obtain the message digest

- A's hashing algorithm recreates the message digest from the decrypted message
- The two message digests are compared, if they are the same then the message should be authentic / has not been tampered.

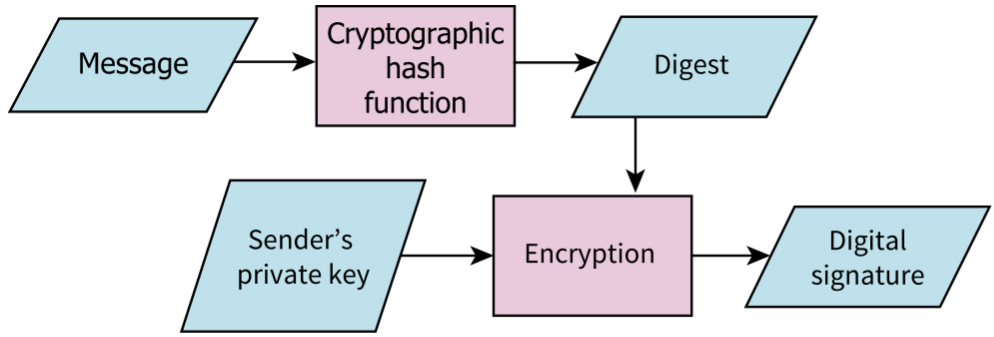

Figure 21.02 Sender using a one-way hash function to send a digital signature

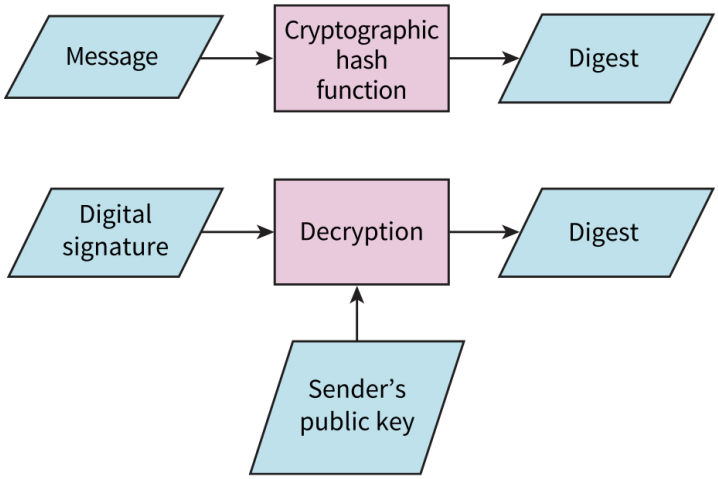

Figure 21.03 Receiver checking that the received transmission is authentic and unchanged

---

Explain the process organisation follows to obtain digital certificate

- Appied to an issuing Certificate Authority (CA)
  - With some proof of identity
  - Eg: name of organisation, address of organization
  - So their identity can be checked by the organisational registration authority
  - So that the digital certificate will only be issued to a trusted organization

Digital signature✒

> Electronic way of validating the authenticity of digital documents; that is, making sure they have not been tampered with during transmission and also proof that a document was sent by a known user

Purpose:

- To ensure a document is authentic // came from a trusted source
- To ensure a document has not benn altered during transmission
- Non-repudiation

	Digital certificate & digital signature
Similarities:	Both used for authentication Both are unique to the owner/subject Include / use owner's public key Include / make use of hashing algorithm
Differences:	Certificate obtained from issuing authority Signature created from a message Certificate provides authentication of owner Signature used to authenticate message that are sent by the owner Certificate remains unchanged whilst it is valid New signature created for every message Only certificate provide extra information Only signature make use of a private key

Past paper questions

1.

Give two uses where the encrypted message digest is advisable:

- Financial transaction
- Legal document
- Software distribution

A user downloads software from the internet.

State what should be part of the download to provide proof that the software is authentic

- Digital signature

Describe the process for ensuring that the software is both authentic and has not been altered

- Software is put through a hashing algorithm to produce a digest
- The digest is encrypted using the private key to produce a digital signature
- The software is sent along with the digital signature
- The receiver is in possession of the sender’s public key
- The received digital signature is decrypted with sender’s public key to produce the digest
- The received software is hashed to produce another digest
- Compare if the two digests are equal
- If so, then the software is authentic and has not been altered