Network Security: Digital Signature

Q1. What is a Digital Signature?

Answer:
A digital signature is an electronic form of a handwritten signature used to verify the **authenticity**, **integrity**, and **origin** of a digital message or document.
It ensures that:

- The message really came from the sender (authentication).
- The message was not changed (integrity).
- The sender cannot deny sending it (nonrepudiation).

A digital signature is created using the sender's private key and verified using the sender's public key.
Example:
Alice signs a message using her private key. Bob uses Alice's public key to verify the message. If it matches, Bob knows the message is truly from Alice and has not been changed.

Q2. What is Inclusion in Digital Signature?

Answer:
Inclusion means that a digital signature includes specific information (like the signer's identity, document hash, and timestamp) inside it to ensure authenticity.
Example:
When you sign a PDF digitally, the signature includes your name, certificate, and time — proving who signed it and when.

Q3. What is Verification Method?

Answer:
Verification method is the process used to check whether a digital signature is valid and the document has not been changed.
Example:
The receiver uses the sender's public key to verify the signature. If the signature matches the document's hash, it is valid.

Q4. What is Relationship in Digital Signature?

Answer:
For a conventional signature, one signature can be used for many documents (one-to-many relationship). But in a digital signature, there is a one-to-one relationship between a signature and a message. Each message has its own unique signature.

Example:
If Alice sends two different messages to Bob, the first message's signature cannot verify the second message. Each message needs a new signature.

Q5. What is Duplicity in Digital Signature?

Answer:
Duplicity means using or copying a signature dishonestly to make a fake version of a document or identity. Digital signatures prevent duplicity because each signature is unique and tied to one message.

Example:
If someone copies your digital signature from one file to another, verification will fail because the signature does not match the new document's hash.

Q6. Explain the Services Provided by Digital Signature.

Answer:
A digital signature provides the following main security services:

1. **Message Authentication:** It proves who sent the message. The receiver verifies it using the sender's public key. Example: Alice sends a signed email; Bob verifies it came from Alice.

2. **Message Integrity:** It ensures the message has not been changed. Digital signatures use hash functions to detect changes. Example: If someone edits the message, the signature becomes invalid.

3. **Nonrepudiation:** The sender cannot deny sending the message later. Example: If Alice signs a bank transfer message, she cannot deny it later. A trusted third party can be used to store message records and prevent denial.

Summary Table:

Service	**Purpose**	**How Achieved**
Message Authentication	Verify sender identity	Using sender's public key
Message Integrity	Detect message change	Using hash function
Nonrepudiation	Prevent denial by sender	Using trusted third party

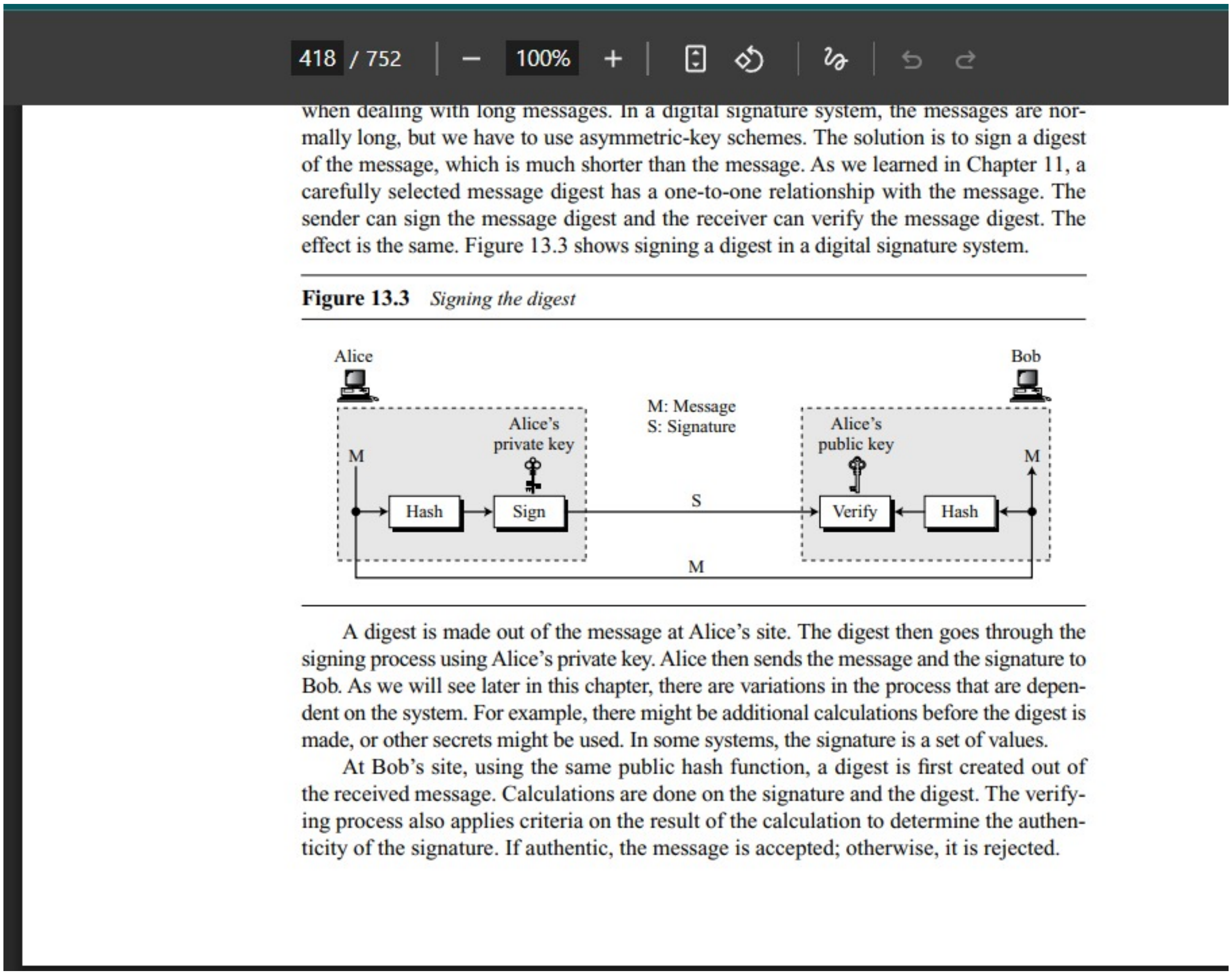
Q7. What is Confidentiality in Digital Signature?

Answer:
A digital signature alone does not provide confidentiality — it only proves authenticity and integrity. If confidentiality is required, both the message and the signature must be **encrypted** using either:

- A secret-key (symmetric) method, or
- A public-key (asymmetric) method.

In short: Digital signature = authenticity + integrity
Encryption = confidentiality

Example: Alice signs a message and encrypts it with Bob's public key. Only Bob can decrypt and read it, ensuring both authenticity and confidentiality.



when dealing with long messages. In a digital signature system, the messages are normally long, but we have to use asymmetric-key schemes. The solution is to sign a digest of the message, which is much shorter than the message. As we learned in Chapter 11, a carefully selected message digest has a one-to-one relationship with the message. The sender can sign the message digest and the receiver can verify the message digest. The effect is the same. Figure 13.3 shows signing a digest in a digital signature system.

Figure 13.3 *Signing the digest*

A digest is made out of the message at Alice's site. The digest then goes through the signing process using Alice's private key. Alice then sends the message and the signature to Bob. As we will see later in this chapter, there are variations in the process that are dependent on the system. For example, there might be additional calculations before the digest is made, or other secrets might be used. In some systems, the signature is a set of values.

At Bob's site, using the same public hash function, a digest is first created out of the received message. Calculations are done on the signature and the digest. The verifying process also applies criteria on the result of the calculation to determine the authenticity of the signature. If authentic, the message is accepted; otherwise, it is rejected.

Figure 1: Block Diagram of Hashing.

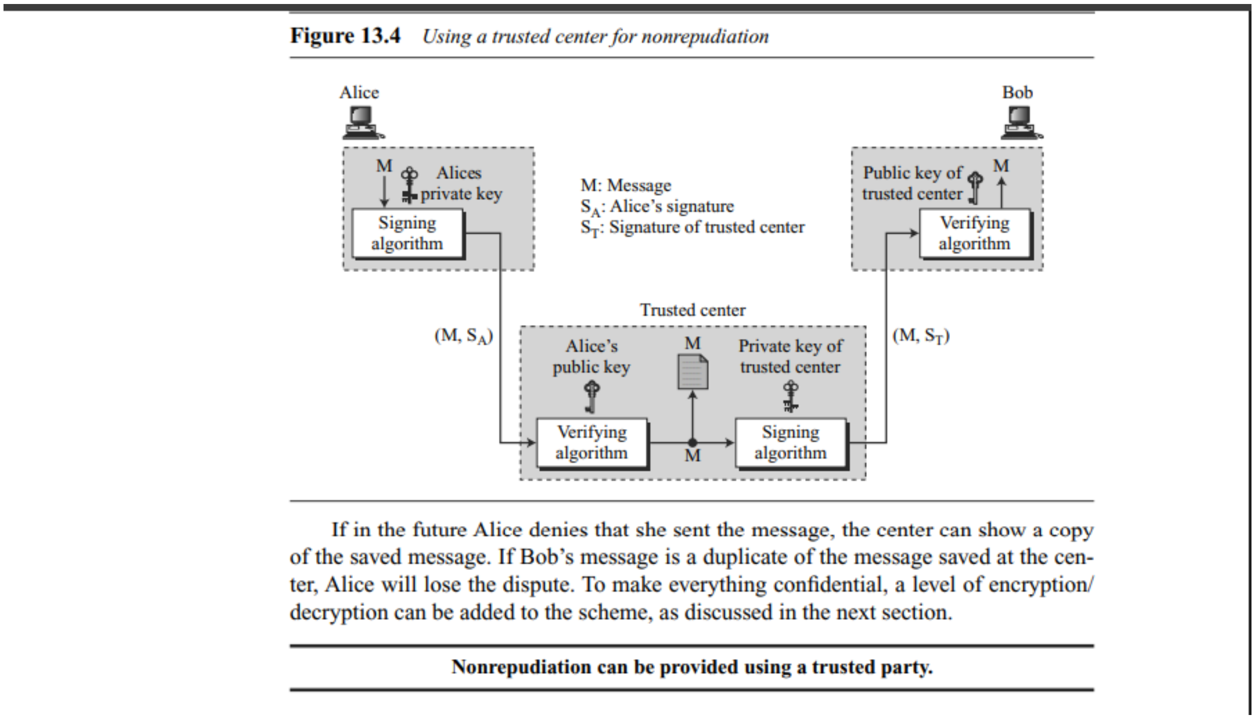


Figure 13.4 *Using a trusted center for nonrepudiation*

If in the future Alice denies that she sent the message, the center can show a copy of the saved message. If Bob's message is a duplicate of the message saved at the center, Alice will lose the dispute. To make everything confidential, a level of encryption/decryption can be added to the scheme, as discussed in the next section.

Nonrepudiation can be provided using a trusted party.

Figure 2: Using a trusted center for nonrepudiation.