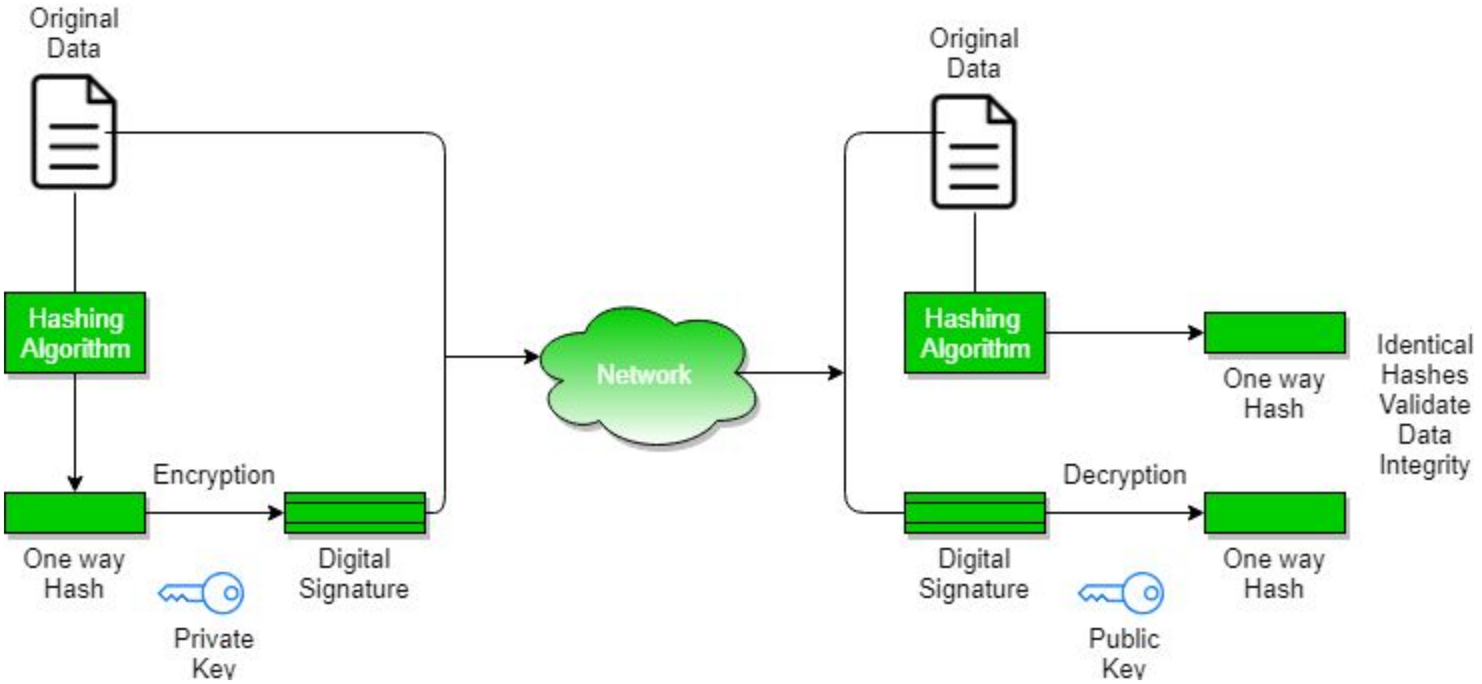
Digital Signature

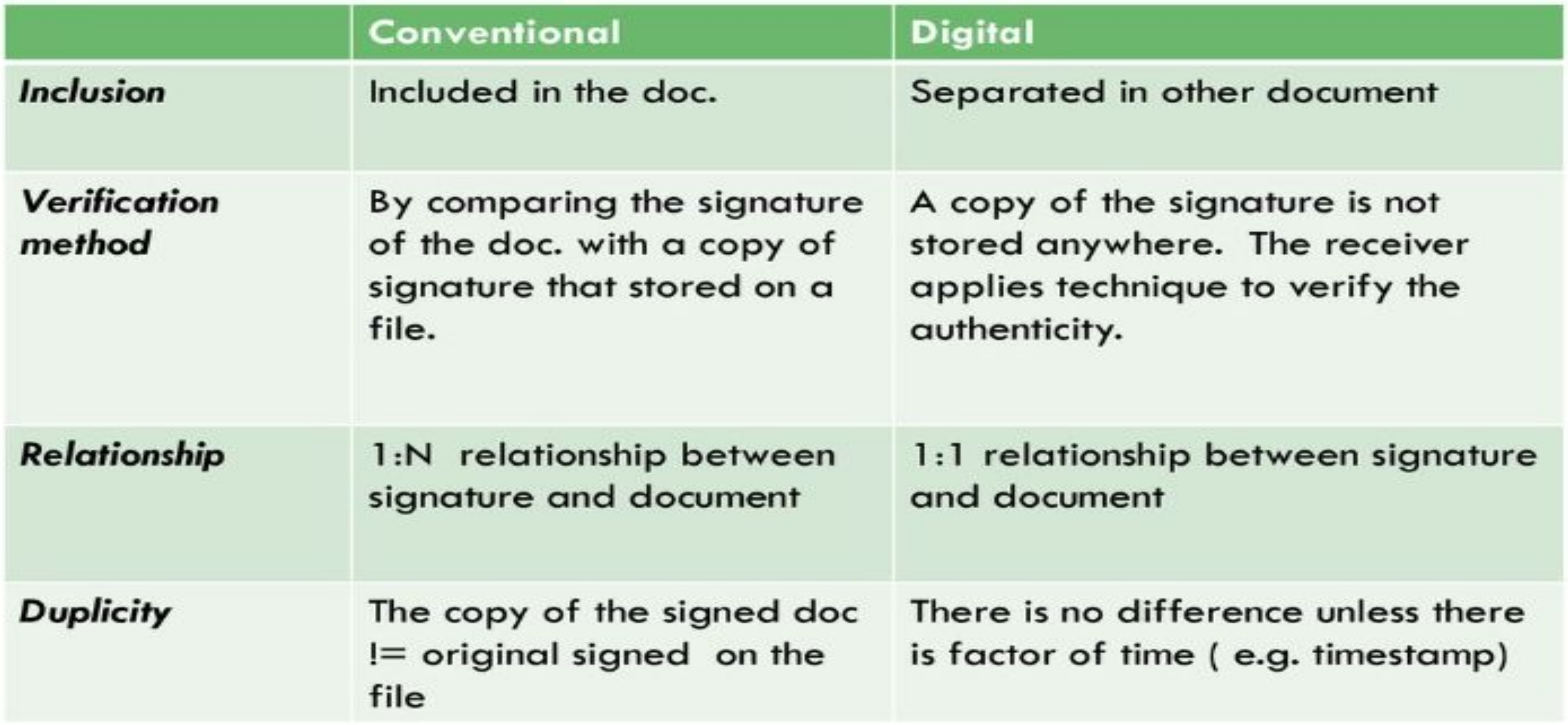
Digital Signature

Digital signature is a **mathematical method** used to verify the **authenticity and integrity of digital messages** or documents, similar to a handwritten signature, but using **cryptographic techniques and public-key infrastructure**



COMPARISON

Let us begin by looking at the differences between conventional signatures and digital signatures.



	Conventional	Digital
Inclusion	Included in the doc.	Separated in other document
Verification method	By comparing the signature of the doc. with a copy of signature that stored on a file.	A copy of the signature is not stored anywhere. The receiver applies technique to verify the authenticity.
Relationship	1:N relationship between signature and document	1:1 relationship between signature and document
Duplicity	The copy of the signed doc != original signed on the file	There is no difference unless there is factor of time (e.g. timestamp)

Inclusion

A conventional signature is included in the document; it is part of the document. But when we sign a document digitally, we send the signature as a separate document.

Verification Method

For a conventional signature, when the recipient receives a document, she compares the signature on the document with the signature on file. For a digital signature, the recipient receives the message and the signature. The recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.

Relationship

For a conventional signature, there is normally a one-to-many relationship between a signature and documents. For a digital signature, there is a one-to-one relationship between a signature and a message.

Duplicity

In conventional signature, a copy of the signed document can be distinguished from the original one on file. In digital signature, there is no such distinction unless there is a factor of time on the document.

PROCESS

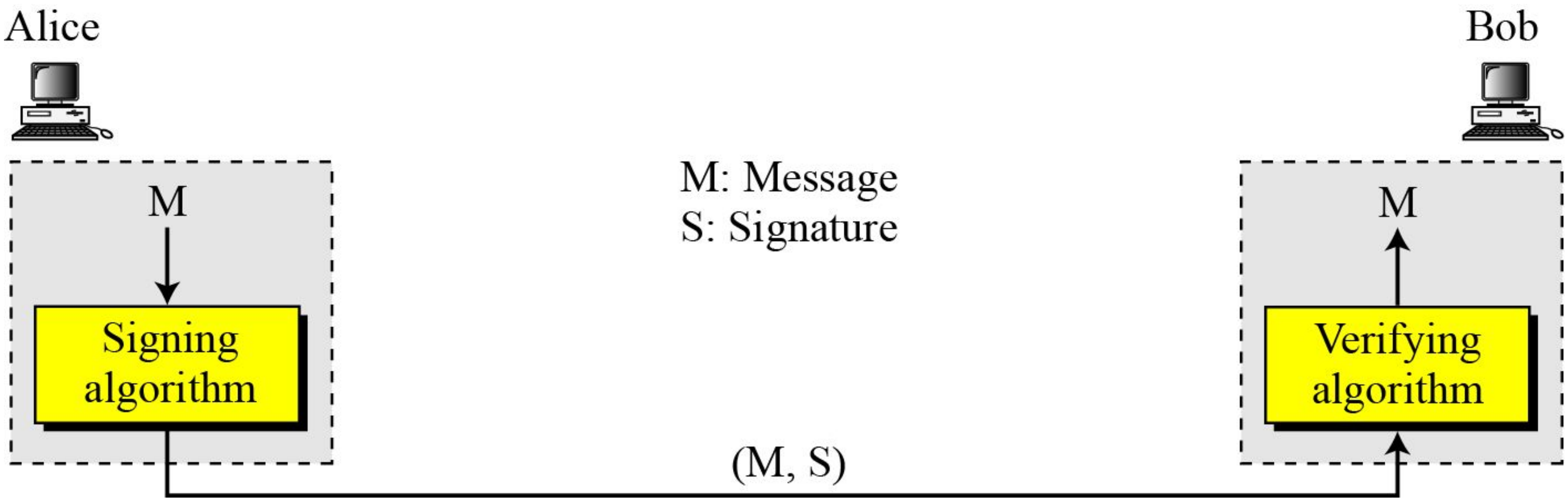
Figure 13.1 shows the digital signature process. The sender uses a signing algorithm to sign the message. The message and the signature are sent to the receiver. The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted; otherwise, it is rejected.

Topics discussed in this section:

13.2.1 Need for Keys
13.2.2 Signing the Digest

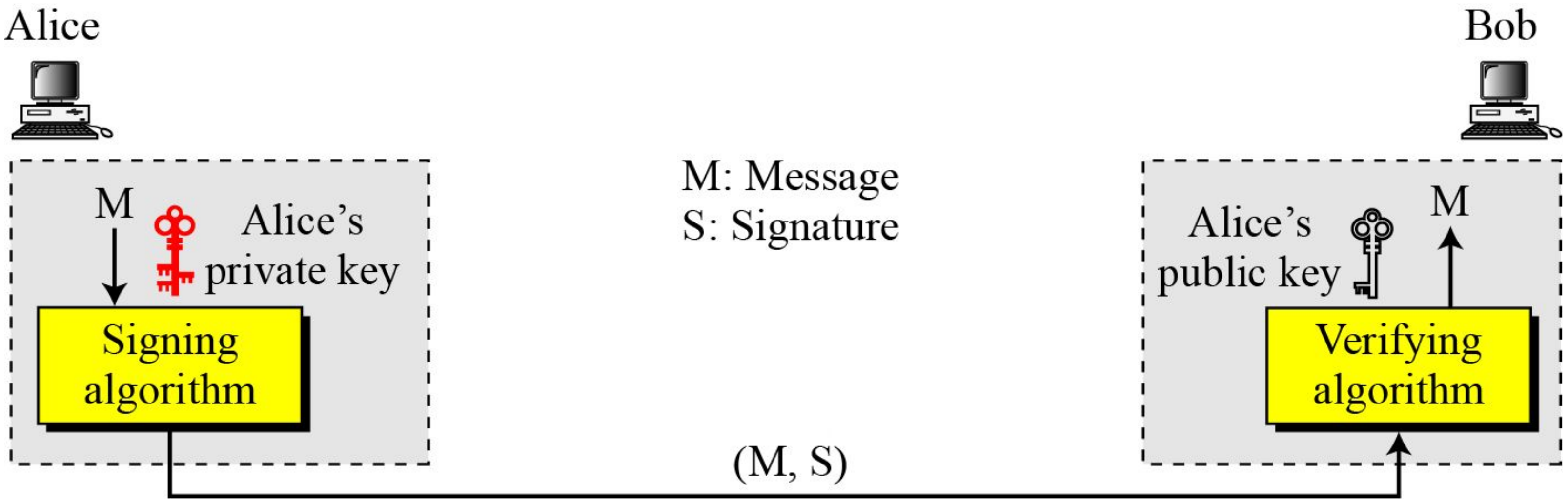
Continued

Figure 13.1 ***Digital signature process***



Need for Keys

Figure 13.2 ***Adding key to the digital signature process***

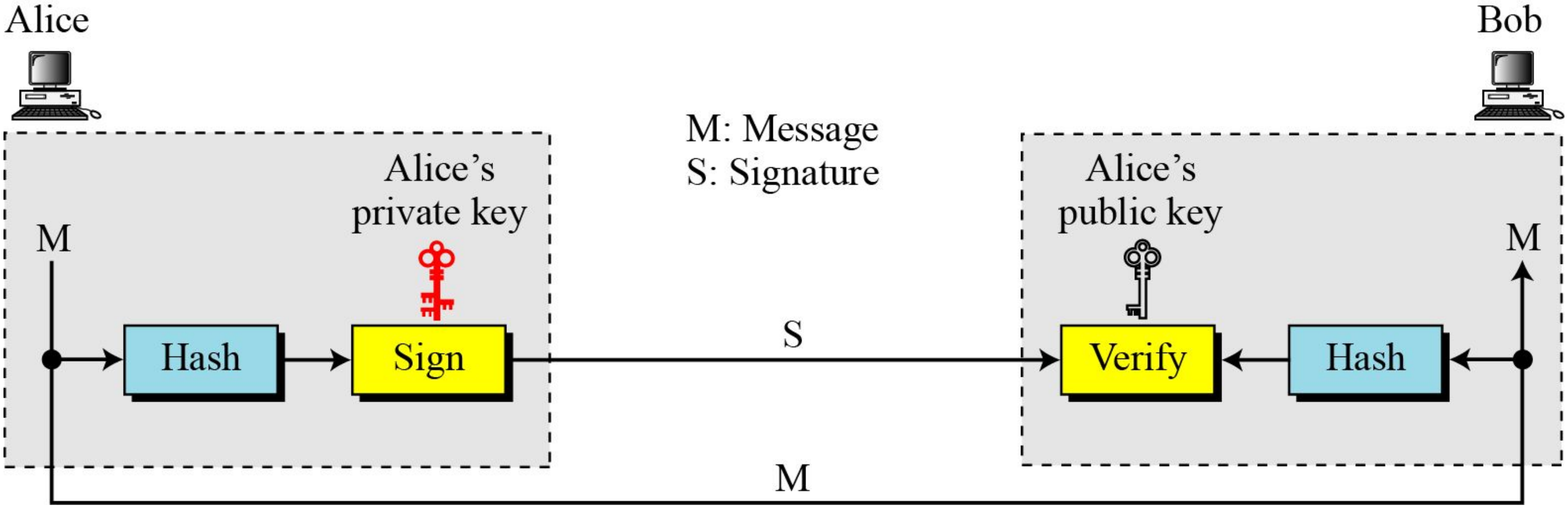


Note

A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.

Signing the Digest

Figure 13.3 ***Signing the digest***



SERVICES

We discussed several security services in Chapter 1 including message confidentiality, message authentication, message integrity, and nonrepudiation. A digital signature can directly provide the last three; for message confidentiality we still need encryption/decryption.

Topics discussed in this section:

13.3.1 Message Authentication
13.3.2 Message Integrity
13.3.3 Nonrepudiation
13.3.4 Confidentiality

Message Authentication

A secure digital signature scheme, like a secure conventional signature can provide message authentication.

Note

A digital signature provides message authentication.

Message Integrity

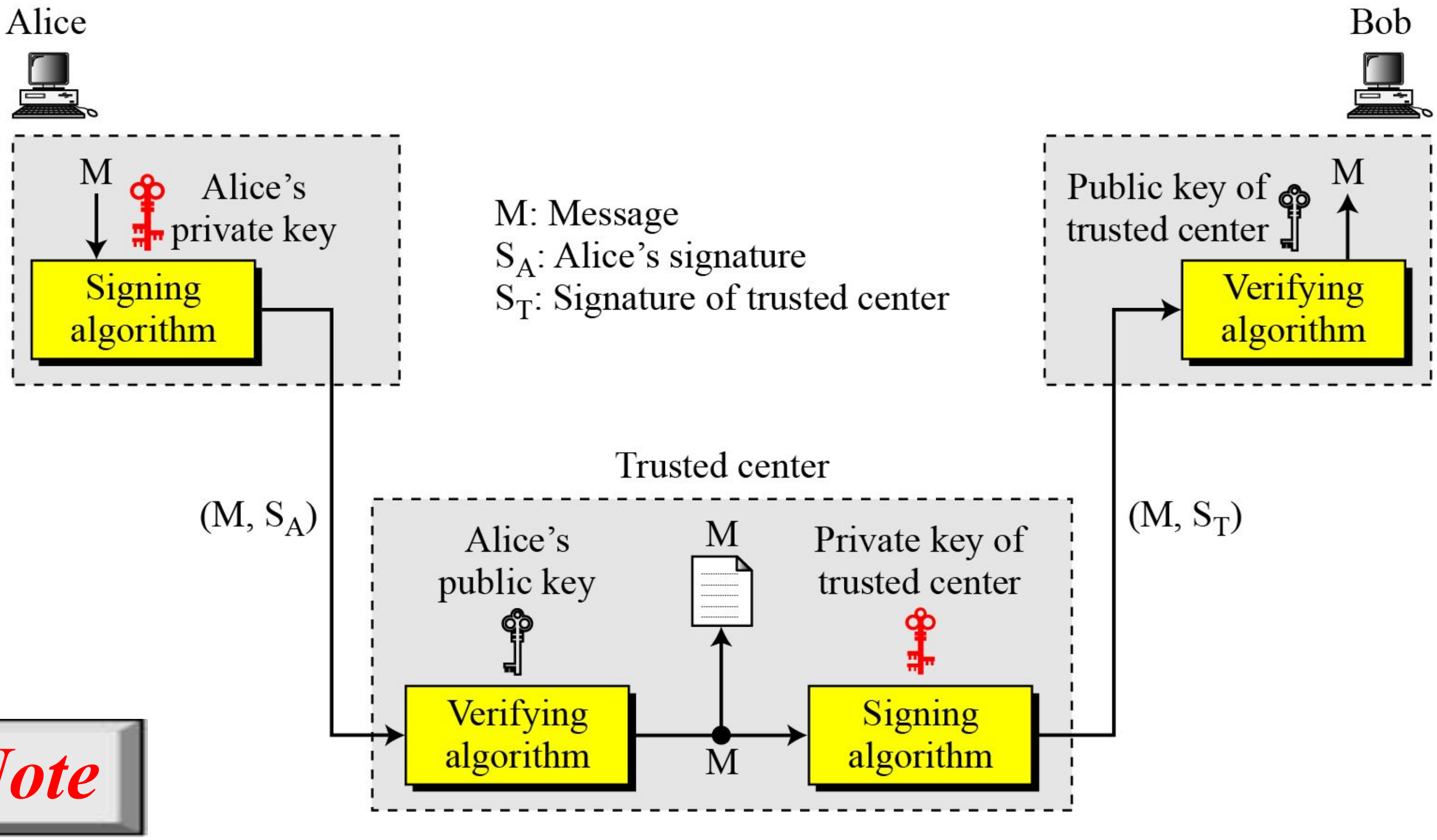
The integrity of the message is preserved even if we sign the whole message because we cannot get the same signature if the message is changed.

Note

A digital signature provides message integrity.

Nonrepudiation

Figure 13.4 *Using a trusted center for nonrepudiation*

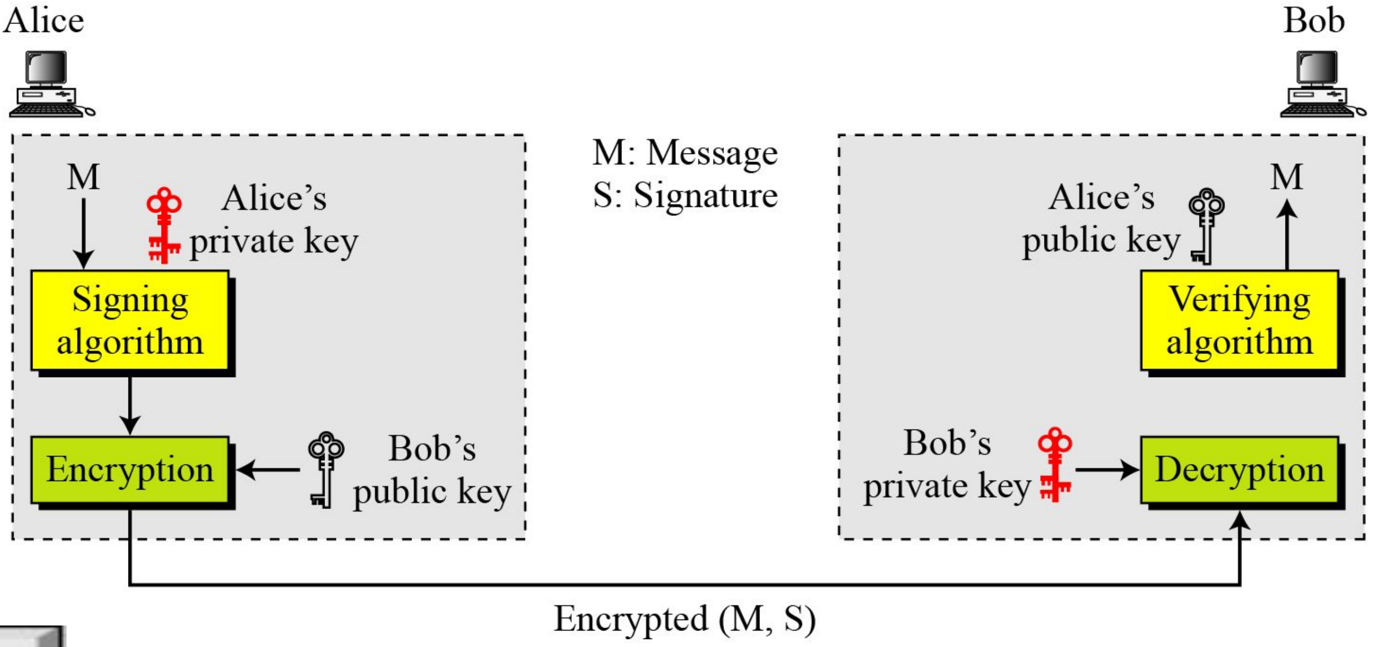


Note

Nonrepudiation can be provided using a trusted party.

Confidentiality

Figure 13.5 ***Adding confidentiality to a digital signature scheme***



Note

A digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.