Cryptography and Network Security — Behrouz Forouzan

Chapter 13

Digital Signature

Chapter 13 Objectives

- To define a digital signature
- To define security services provided by a digital signature
- To define attacks on digital signatures
- To discuss some digital signature schemes, including RSA, ElGamal,
- Schnorr, DSS, and elliptic curve
- To describe some applications of digital signatures

13.2

13-1 COMPARISON

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

Topics discussed in this section:

13.3

13.1.1 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.

13.4

13.1.2 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.

13.5

13.1.3 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.

13.6

13.1.4 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.

13.7

13-2 PROCESS

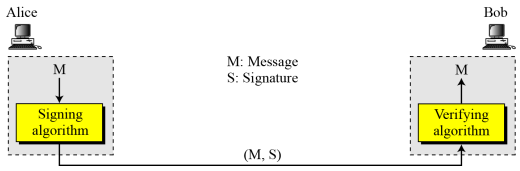
Figure 13.1 shows the digital signature process. The sender uses a signing algorithm to sign the message. The message and the signature are sent to the receiver. The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message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

Topics discussed in this section:

13.8

13-2 Continued

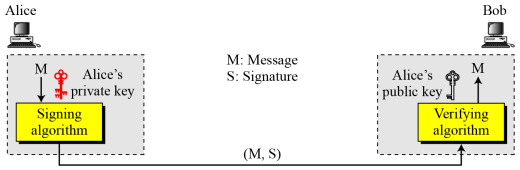
Figure 13.1 *Digital signature process*



13.9

13.2.1 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.

13.10

13.2.1 Continued

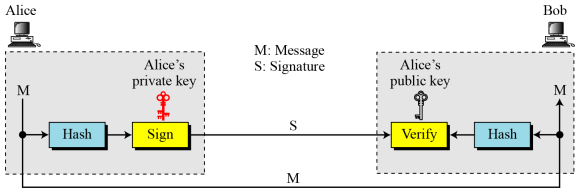
Note

A cryptosystem uses the private and public keys of the receiver: a digital signature uses the private and public keys of the sender.

13.11

13.2.2 Signing the Digest

Figure 13.3 *Signing the digest*



13.12

13-3 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:

13.13

13.3.1 Message Authentication

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

Note

A digital signature provides message authentication.

13.14

13.3.2 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.

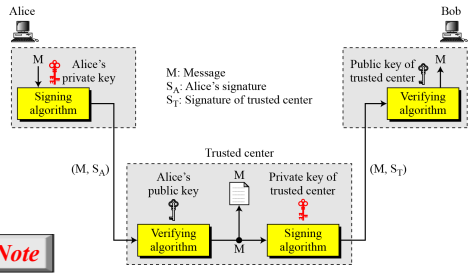
Note

A digital signature provides message integrity.

13.15

13.3.3 Nonrepudiation

Figure 13.4 *Using a trusted center for nonrepudiation*



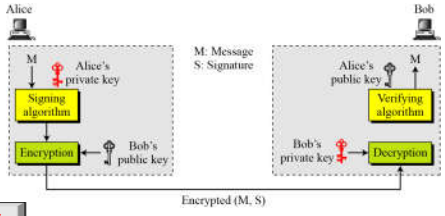
Note

Nonrepudiation can be provided using a trusted party.

13.16

13.3.4 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.

13.17