جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم الأمن السيبراني

Lecture: (4)

Digital Signature

Subject: authentication and access control

second Stage

Lecturer: Asst. Lecturer. Suha Alhussieny

Digital Signature

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically, the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the work source and integrity of the message.

Two types of digital signature:

- **Direct Digital Signature**
- **Arbitrated Digital Signature**

The most important development from the on public-key cryptography is the digital signature. The digital signature provides a set of security capabilities that would be difficult to implement in any other way.

Figure 13.1 is a generic model of the process of making and using digital signatures. Bob can sign a message using a digital signature generation algorithm. The inputs to the algorithm are the message and Bob's private key. Any other user, say Alice, can verify the signature using a verification algorithm, whose inputs are the message, the signature, and Bob's public key.

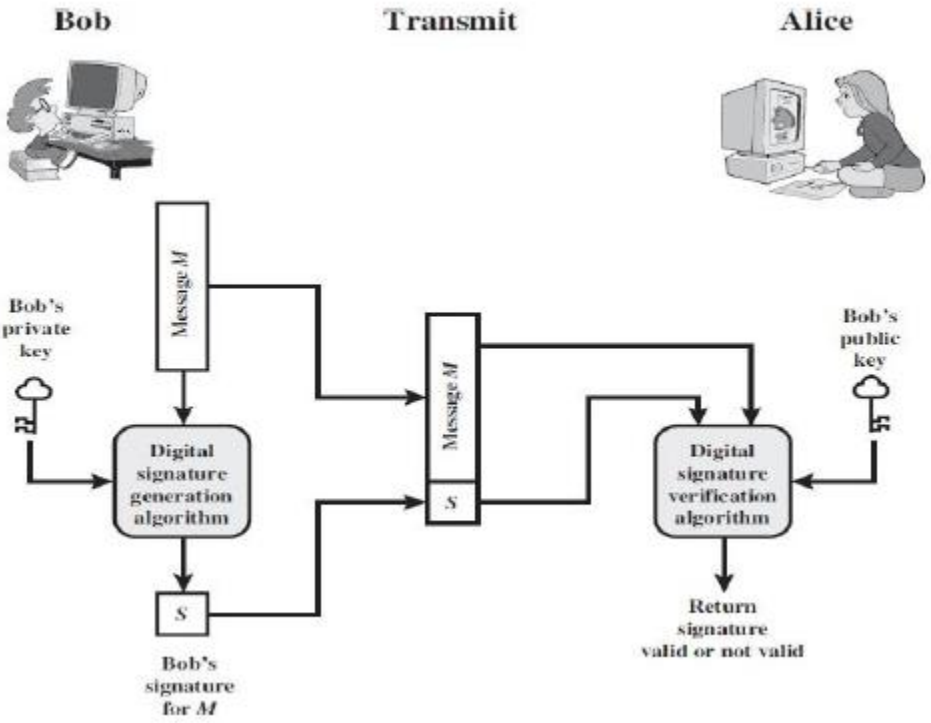

Figure (13.1) Generic Model of Digital Signature Process

In simplified terms, the essence of the digital signature mechanism is shown in **Figure 13.2**.

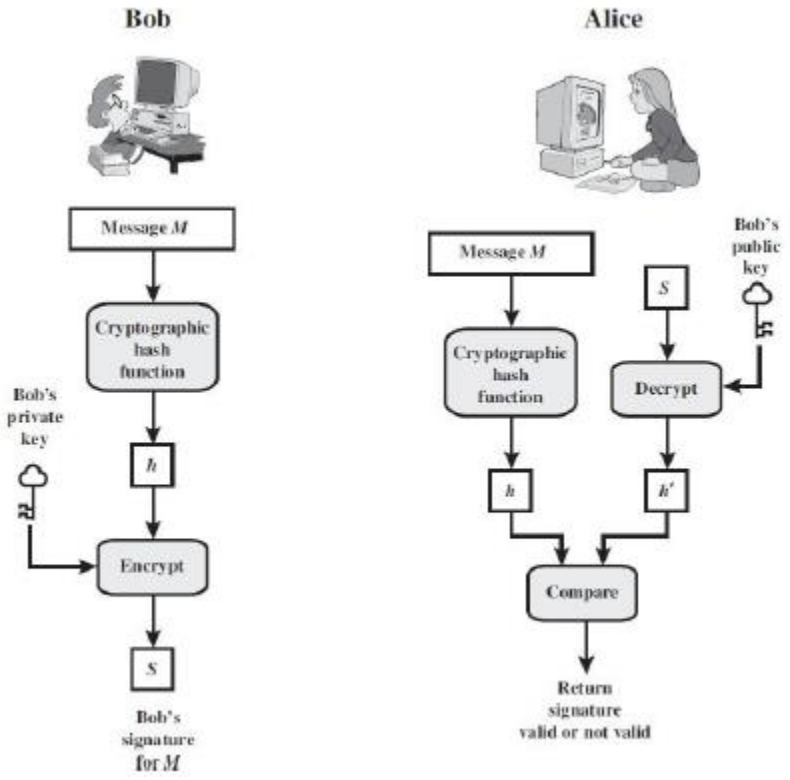

Figure 13.2 Simplified Depiction of Essential Elements of Digital Signature

The 5 steps to digitally signing a document:

1. **Document preparation:** Initially, the document to be digitally signed is prepared. This could be any electronic document like a PDF, Word file, or an email.

2. **Hash creation:** A unique hash (or "digest") of the document is created using a hashing algorithm. This ensures that the document has not been altered, providing a layer of integrity.

3. **Signing the hash with a private key:** The hash is then encrypted using the sender's private key. This encrypted hash serves as the digital signature for the document.

4. **Attachment:** The digital signature is then attached to the document, or sent alongside it, as evidence of the document's origin and integrity.

5. **Verification by the recipient:** Upon receiving the digitally signed document, the receiver can decrypt the hash using the sender's public key. If it matches the document's hash, it proves the signature is valid and the document is intact.

Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other. Several forms of dispute between the two are possible.

For example, suppose that John sends an authenticated message to Mary, using one of the schemes of Figure 12.1. Consider the following **disputes** that could arise.

1. Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share.

2. John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

Both scenarios are of legitimate concern. Here is an example of the first scenario: An electronic funds transfer takes place, and the receiver increases the amount of funds transferred and claims that the larger amount had arrived from the sender. An example of the second scenario is that an electronic mail message contains instructions to a stockbroker for a transaction that subsequently turns out badly. The sender pretends that the message was never sent.

In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature

A digital signature is used to assure:

- ✓ Authenticity

  The identity of the organization that sent the message (the message signer) is confirmed.

- ✓ Integrity

  The message content was not changed or tampered with since it was digitally signed.

Tip: You can also encrypt the message, which protects the confidentiality of the information in the message.

- ✓ Nonrepudiation

The origin of the signed content is verified to all parties so the message signer cannot deny association with the signed content.

Thus, the digital signature function includes the authentication function.

the general **requirements** for a digital signature often include the following:

- Certificate authority (CA)
- Private key
- Electronic signing

Let's take a look at each of these requirements in greater detail.

Certificate authority (CA)

You'll need a digital certificate from a reputable certificate authority (CA) to authenticate your identity. Certificate authorities are trusted organizations that issue digital certificates. These certificates serve to validate the identity of the individual or entity requesting the digital signature.

Private key

A unique private key is essential for creating the digital signature. This key should be securely stored and only accessible by the signer. Your private key is akin to your digital fingerprint. It's used to create the digital signature, and should be stored in a secure environment (like a private hard drive) to prevent unauthorized access.

Electronic signing

Digital signatures can only be applied to electronic documents. The document to be signed must be in electronic form, such as a PDF, a Word document, or a document on a contract lifecycle management (CLM) platform that includes digital signature functionality. Make sure the document you intend to sign is in a format that supports digital signatures.

Digital signature attacks

Possible attacks on digital signatures include the following:

- **Chosen-message attack.** The attacker either obtains the victim's public key or tricks the victim into digitally signing a document they don't intend to sign.
- **Known-message attack.** The attacker obtains messages the victim sent and a key that enables the attacker to forge the victim's signature on documents.
- **Key-only attack.** The attacker has access to the victim's public key and re-creates the victim's signature to digitally sign documents or messages that the victim doesn't intend to sign.

Remote User Authentication principles

Remote user authentication is a mechanism in which the remote server verifies the legitimacy of a user over an insecure communication channel. Password based authentication schemes have been widely deployed to verify the legitimacy of remote users as password authentication is one of the simplest and the most convenient authentication mechanism over insecure networks.

For example, user Alice Toklas could have the user identifier ABTOKLAS, This information needs to be stored on any server or computer system that Alice wishes to use and could be known to system administrators and other users. A typical item of authentication information associated with this user ID is a password, which is kept secret (known only to Alice and to the system).

obtain or guess Alice's password, then the combination of Alice's user ID and password enables administrators to set up Alice's access permissions and aud it her activity. Because Alice's ID is not secret, system users can send her e-mail, but because her password is secret, no one can pretend to be Alice.

The process of verifying an identity claimed by or for a system entity. An authentication process consists of two steps:

- **Identification step:** Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)
- **Verification step:** Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

Mutual authentication

An important application area is that of mutual authentication protocols. Such protocols enable communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys. There, the focus was key distribution. We return to this topic here to consider the wider implications of authentication.

Central to the problem of authenticated key exchange are two issues: confidentiality and timeliness. To prevent masquerade and to prevent compromise of session keys, essential identification and session-key information must be communicated in encrypted form. This requires the prior existence of secret or public keys that can be used for this purpose. The second issue, timeliness, is important because of the threat of message replays. Such replays, at worst, could allow an opponent to compromise a session key or successfully impersonate another party. At minimum, a successful replay can disrupt operations by presenting parties with messages that appear genuine but are not.

One-Way Authentication

One application for which encryption is growing in popularity is electronic mail (e-mail). The very nature of electronic mail, and its chief benefit, is that it is not necessary for the sender and receiver to be online at the same time. Instead, the e-mail message is forwarded to the receiver's electronic mailbox, where it is buffered until the receiver is available to read it.

The "envelope" or header of the e-mail message must be in the clear, so that the message can be handled by the store-and-forward e-mail protocol, such as the Simple Mail Transfer Protocol (SMTP) or X.400. However, it is often desirable that the mail-handling protocol not require access to the plaintext form of the message, because that would require trusting the mail-handling mechanism. Accordingly, the e-mail message should be encrypted such that the mail-handling system is not in possession of the decryption key.

A second requirement is that of **authentication**. Typically, the recipient wants some assurance that the message is from the alleged sender.