[Part 3] Integrity, Authenticity, and Key Management

Chapter 13

Digital Signature

Forouzan, B.A. Cryptography and Network Security (International Edition). United States: McGraw Hill, 2008.

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 a digital signature scheme, RSA.
- To describe some applications of digital signatures.

Chapter 13 Contents

13.1 Introduction
13.2 Digital Signature Schemes
13.3 Summary

13.3

Chapter 13 Contents

13.1 Introduction
- Comparison
- Process
- Services
- Attacks on Digital Signature

13.2 Digital Signature Schemes
13.3 Summary

13.4

Chapter 13

13.1 Introduction

- We are familiar with the concept of a signature before.
- A person signs a document to show that it originated from him or was approved by him.
- The signature is proof to the recipient that the document comes from the correct entity and nobody else.
- A sign of authentication: A verified signature on a document.
- A message can be signed electronically.
- The electronic signature can prove the authenticity of the sender of the message → *digital signature*.

13.5

Chapter 13

13.1 Introduction

Comparison

	Conventional Signature	Digital Signatures
(1) Inclusion	Included in the document as part of the document.	Send the signature as a separate document.
(2) Verification Method	Recipient compares the signature on the document with the signature on file.	• 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.
(3) Relationship	Normally a *one-to-many* relationship between a signature and documents.	*One-to-one* relationship between a signature and a message.
(4) Duplicity	A copy of the signed document can be distinguished from the original one on file.	No such distinction unless there is a factor of time on the document

13.6

Chapter 13

13.1 Introduction

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.

13.7

Chapter 13

13.1 Introduction

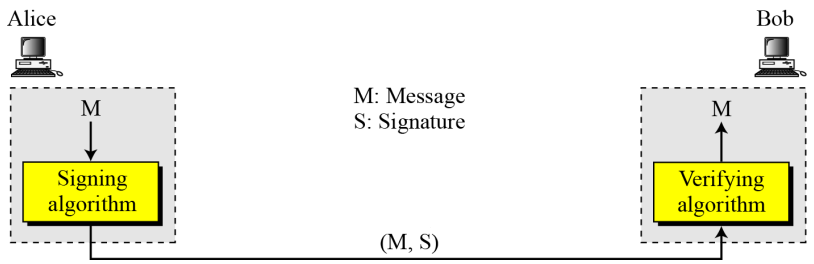


Figure 13.1: Digital signature process

13.8

Chapter 13 13.1 Introduction

Need for Keys:

- In digital signature, the signer uses his private key, applied to a *signing algorithm*, to **sign** the document.
- The verifier (recipient), uses the public key of the signer, applied to the *verifying algorithm*, to **verify** the document.

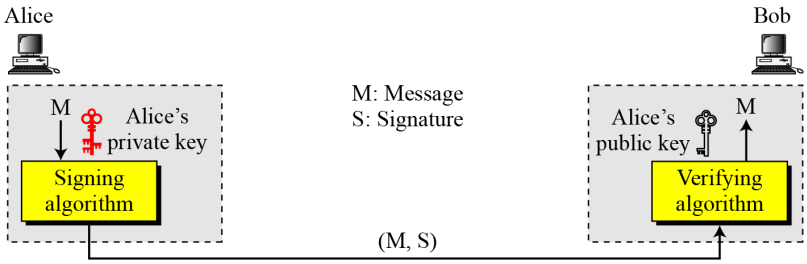


Figure 13.2: Adding key to the signature process

13.9

Chapter 13 13.1 Introduction

Signing the Digest:

- In Chapter 10, we learned that the asymmetric-key cryptosystems are very inefficient when dealing with long messages.
- In digital signature system, the messages are normally long, but we have to use asymmetric-key schemes.
- **Solution**:
  - To sign a digest of the message, which is shorter than a message.
- Figure 13.3 shows signing a digest in a digital signature system.

13.10

Chapter 13

13.1 Introduction

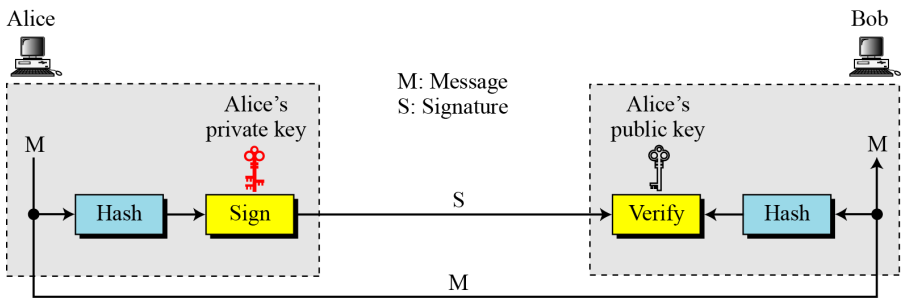


Figure 13.3: Signing the digest

13.11

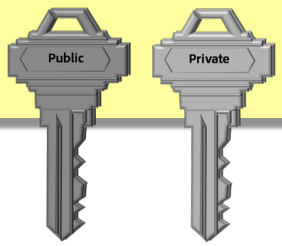
Chapter 13

13.1 Introduction

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.



https://glynrob.com/wp-content/uploads/000_keys.jpg.png

13.12

Chapter 13

13.1 Introduction

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.

13.13

Chapter 13

13.1 Introduction

Message *authentication* :

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

13.14

Chapter 13 13.1 Introduction

Nonrepudiation : Nonrepudiation can be provided using a trusted party.

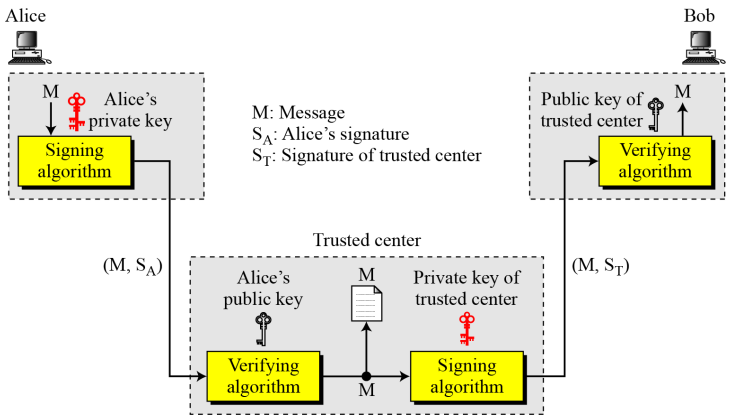


Figure 13.4: Using a trusted center for nonrepudiation

13.15

Chapter 13 13.1 Introduction

Message *confidentiality*:

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

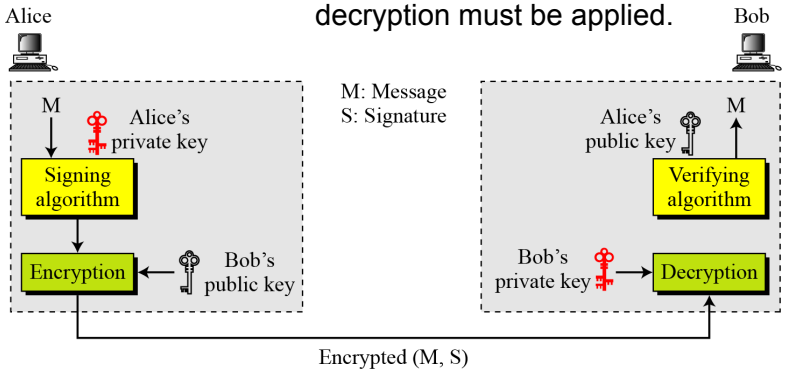


Figure 13.5: Adding confidentiality to a digital signature scheme

13.16

Chapter 13

13.1 Introduction

Attacks on Digital Signature

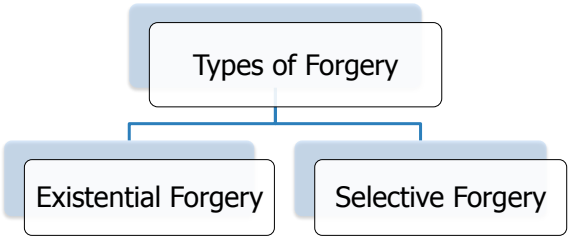
- This section describes some attacks on digital signatures and defines the types of forgery.
- Three kind of **attacks**:
  - Key-only attack.
  - Known-message attack.
  - Chosen-message attack.

13.17

Chapter 13

13.1 Introduction

- If the attack is successful, the result is a **forgery**.



13.18

Chapter 13 Contents

13.1 Introduction
13.2 Digital Signature Schemes
- RSA Digital Signature
13.3 Summary

13.19

Chapter 13 13.2 Digital Signature Schemes

Introduction

- Several digital signature schemes have evolved during the last few decades.
- Some of them have been implemented.
  - *RSA digital signature scheme.*
  - *ElGamal digital signature scheme.*
  - *Schnorr digital signature scheme.*
  - *Digital Signature Standard (DSS).*
  - *Elliptic Curve digital signature scheme.*
- However, this chapter will discuss on RSA digital signature scheme only.

13.20

Chapter 13

13.2 Digital Signature Schemes

RSA Digital Signature Scheme

- In chapter 10, we discussed how to use RSA cryptosystem to provide *confidentiality*.
- The RSA idea can also be used for signing and verifying a message.
- In this case, it is called the *RSA digital signature scheme*.

- The digital signature scheme changes the roles of the private and public keys:
  - ① The private and public keys of the senders are used.
  - ② The sender uses his own private key to sign the document; the receiver uses the sender's public key to verify the document.

13.21

Chapter 13

13.2 Digital Signature Schemes

- The *signing* and *verifying* sites use the same function, but with different parameters.
- The verifier compares the message and the output of the function for **congruence**; If the result is true, the message accepted.

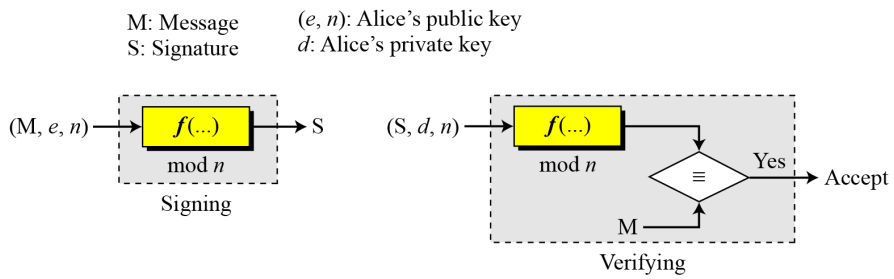


Figure 13.6: General idea behind the RSA digital signature scheme

13.22

Chapter 13 13.2 Digital Signature Schemes

Key Generation:

- Key generation in the RSA digital signature scheme is exactly the same as key generation in the RSA.

Note

In the RSA digital signature scheme, d is private; e and n are public.

13.23

Chapter 13 13.2 Digital Signature Schemes

Signing and Verifying:

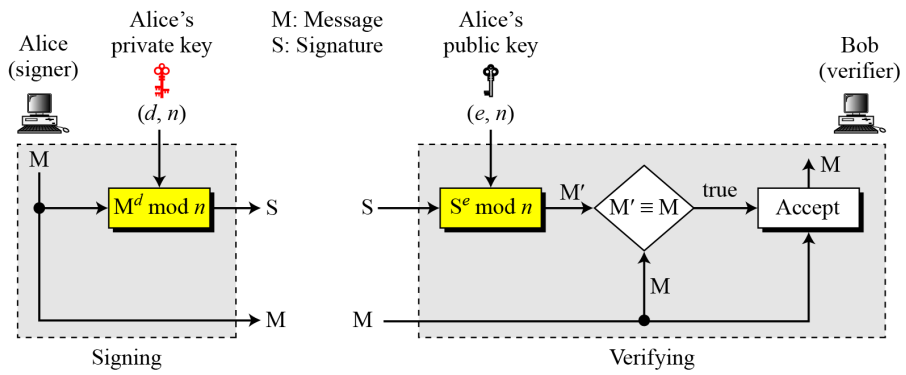


Figure 13.7: RSA digital signature scheme

13.24

Chapter 13 13.2 Digital Signature Schemes

Example 13.1: As a trivial example, suppose that Alice chooses $p = 823$ and $q = 953$, and calculates $n = 784319$.

- The value of $\phi(n)$ is 782544.
- Now she chooses $e = 313$ and calculates $d = 160009$.

- At this point key generation is complete. Now imagine that Alice wants to send a message with the value of $M = 19070$ to Bob. She uses her private exponent, $e = 160009$, to sign the message:

$$\text{M: } 19070 \quad \rightarrow \quad S = (19070^{160009}) \bmod 784319 = 210625 \bmod 784319$$

(*continued*)

Chapter 13 13.2 Digital Signature Schemes

- Alice sends the message and the signature to Bob.
- Bob receives the message and the signature.

- He calculates:

$$M' = 210625^{313} \bmod 784319 = 19070 \bmod 784319 \quad \rightarrow \quad M \equiv M' \bmod n$$

- Bob accepts the message because he has verified Alice's signature.

13.26

Chapter 13 13.2 Digital Signature Schemes

RSA Signature on the Message Digest

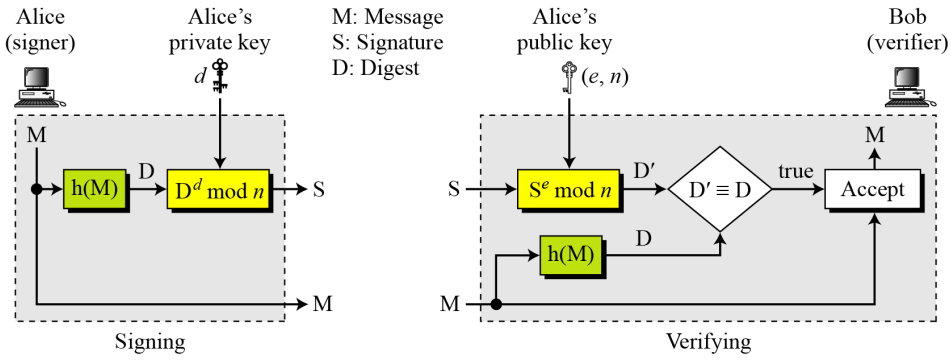


Figure 13.8: The RSA signature on the message digest

13.27

Chapter 13 13.2 Digital Signature Schemes

Note

When the digest is signed instead of the message itself, the susceptibility of the RSA digital signature scheme depends on the strength of the hash algorithm.

13.28

Chapter 13

Contents

13.1 Introduction
13.2 Digital Signature Schemes
13.3 Summary

13.29

Chapter 13

13.3 Summary

- A digital signature scheme can provide the same services provided by a conventional signature.
  - A conventional signature is included in the same document; a digital signature is a separate entity.
  - To verify a conventional signature, the recipient compares the signature with the signature on file; in digital signature, the recipient applies a verifying process to the document and signature.

13.30

Chapter 13

13.3 Summary

- Digital signatures provide:
  - Message *authentication*.
  - Message *integrity* if the digest of the message is signed instead of the message itself.
  - *Nonrepudiation* if a trusted third party is used.
- Digital signature cannot provide *confidentiality* for the message; if needed, a cryptosystem must be applied over the digital signature scheme.

13.31

Chapter 13

13.3 Summary

- A digital signatures needs an asymmetric-key system by using the private and public keys of the sender.
- The RSA digital signature scheme uses RSA cryptosystem, but the roles of the private and public keys are swapped.

13.32

Chapter 13 Exercises

Exercise 13.1:

a) Compare and contrast a conventional signature and a digital signature.

b) List the security services provided by a digital signature.

Chapter 13 Exercises

Exercise 13.1:

Using the RSA scheme, let $p = 809$, $q = 751$, and $d = 23$. Calculate the public key e. Then,

a) Sign and verify a message with $M_1 = 100$. Call the signature S_1.

b) Sign and verify a message with $M_2 = 50$. Call the signature S_2.