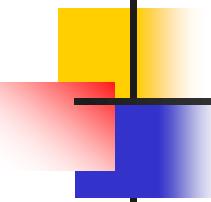


Chữ Ký Số

Digital Signature



NỘI DUNG

- Phân biệt chữ ký số và chữ ký thông thường;
- Dịch vụ bảo mật được cung cấp bởi chữ ký số;
- Đánh giá xác định các cuộc tấn công vào chữ ký số;
- Lược đồ chữ ký số, bao gồm RSA, ElGamal;
- Ứng dụng của chữ ký số.

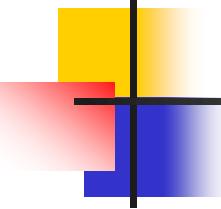
1 COMPARISON

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

Chúng ta hãy bắt đầu bằng cách xem xét sự khác biệt giữa chữ ký thông thường và chữ ký số.

Topics discussed in this section:

- 1.1 Inclusion**
- 1.2 Verification Method**
- 1.3 Relationship**
- 1.4 Duplicity**



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.

*Một chữ ký thông thường được bao gồm trong tài liệu; nó là một phần của tài liệu. Nhưng khi chúng ta ký một tài liệu bằng kỹ thuật số, **chúng ta gửi chữ ký như một tài liệu riêng biệt.***

1.2 Verification Method

Phương pháp xác thực

*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.*

*Đối với chữ ký truyền thống, khi người nhận nhận được tài liệu, cô ấy sẽ so sánh chữ ký trên tài liệu với chữ ký trên hồ sơ. Đối với chữ ký điện tử, người nhận sẽ nhận được thông điệp và chữ ký. Người nhận cần áp dụng kỹ thuật xác minh kết hợp giữa bản tin và chữ ký để **xác minh tính xác thực**.*

1.3 Relationship: Mối quan hệ

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.

*Đối với chữ ký thông thường, thường có mối quan hệ **một-nhiều** giữa chữ ký và các tài liệu. Đối với chữ ký điện tử, có mối quan hệ 1-1 giữa chữ ký và bản tin.*

1.4 Duplicity: Sự trùng lặp

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.

Trong chữ ký thông thường, bản sao của tài liệu đã ký có thể được phân biệt với bản gốc trong hồ sơ. Trong chữ ký điện tử, không có sự phân biệt như vậy trừ khi có yếu tố thời gian trên tài liệu.

2 PROCESS: QUÁ TRÌNH

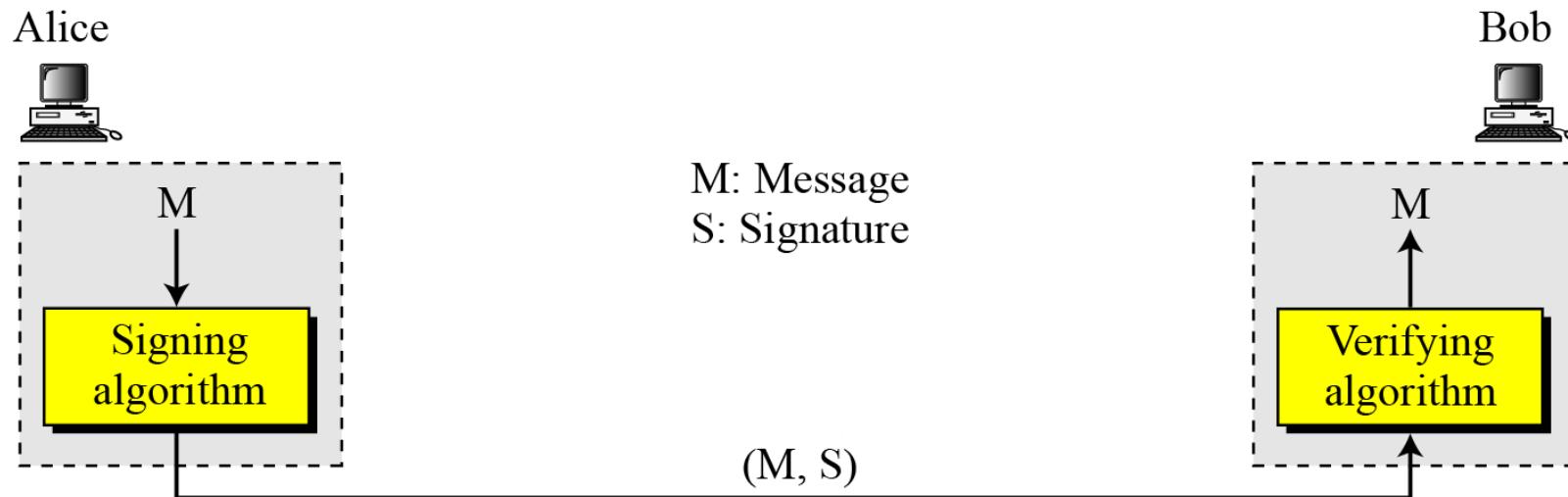
*Figure 1 shows the digital signature process. The sender uses a **signing algorithm** to sign the message. The message and the signature are sent to the receiver. The receiver receives the message and the signature and applies the **verifying algorithm to the combination**. If the result is true, the message is accepted; otherwise, it is rejected.*

Topics discussed in this section:

- 2.1 Need for Keys**
- 2.2 Signing the Digest**

2 Continued

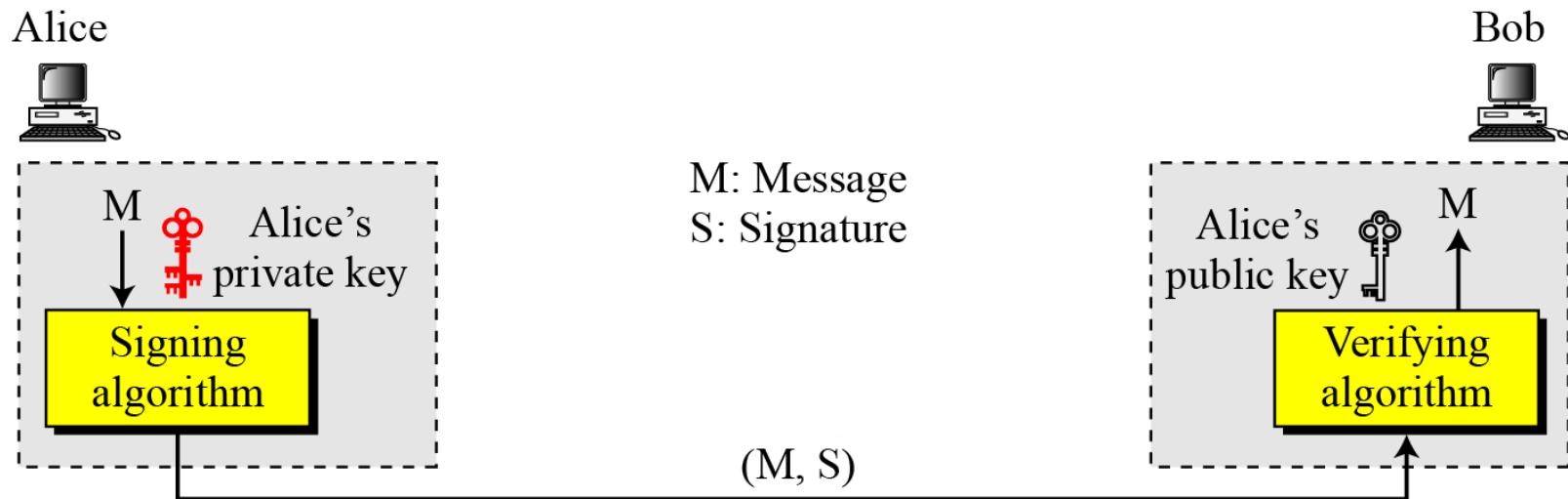
Figure 1 *Digital signature process*



Hình 1 cho thấy quy trình chữ ký điện tử. Người gửi sử dụng một thuật toán ký để ký vào bản tin. Tin nhắn và chữ ký được gửi đến người nhận. Người nhận nhận được thông điệp và chữ ký và áp dụng thuật toán xác thực cho sự kết hợp. Nếu kết quả là true, thông báo được chấp nhận; nếu không, nó bị từ chối.

2.1 Need for Keys: Cần có các khóa

Figure 2 Adding key to the digital signature process



Note

Một chữ ký điện tử cần một hệ thống khóa công khai. Người ký bằng khóa riêng của cô ấy; người xác minh xác minh bằng khóa công khai của người ký.

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

2.1 Continued

Một chữ ký điện tử cần một hệ thống khóa công khai. Người ký gửi bằng khóa riêng của cô ấy; người xác minh xác minh bằng khóa công khai của người ký.

Note

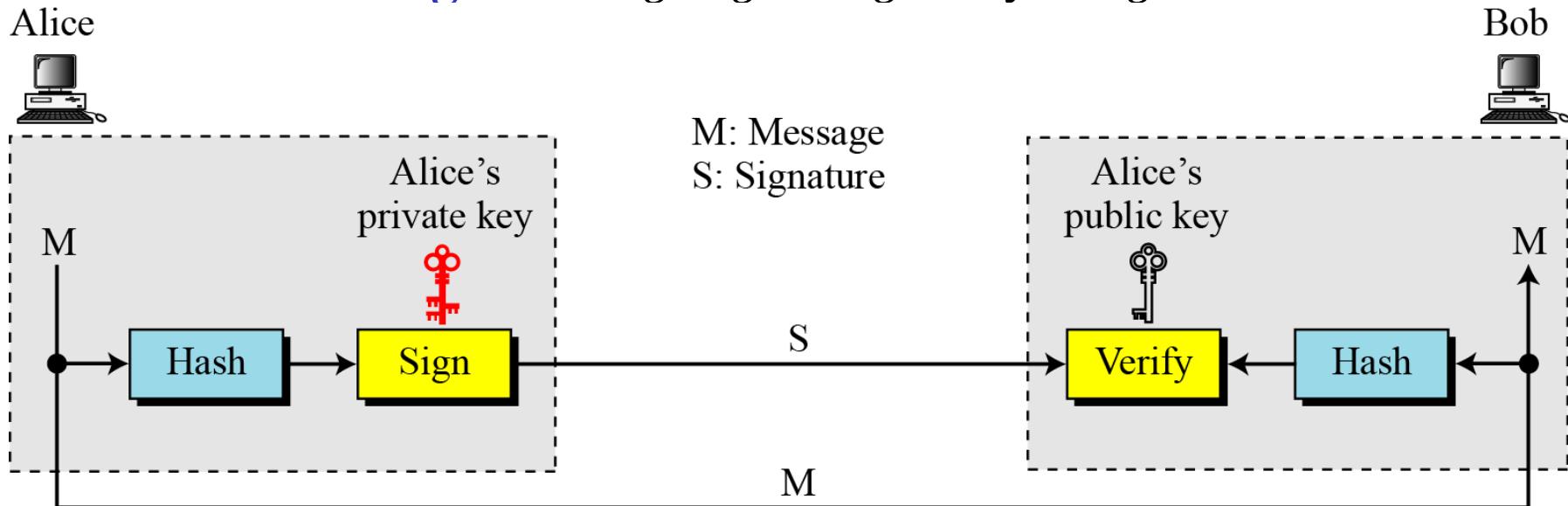
A cryptosystem uses the private and public keys of the receiver: a digital signature uses the private and public keys of the sender.

Chúng ta cần phân biệt khóa bí mật và công khai trong chữ ký số so với khóa công khai và bí mật trong hệ thống mật mã bất đối xứng.

- + Đối với hệ mật bất đối xứng, khóa bí mật và công khai sinh bởi bên người nhận, khóa công khai được sử dụng cho phép mã hóa, khóa bí mật được sử dụng để giải mã hóa.
- + Trong chữ ký số, khóa bí mật và công khai do bên người gửi sử dụng, bên gửi sử dụng khóa bí mật, bên nhận sử dụng khóa công khai của bên gửi.

2.2 Signing the Digest: Ký thông báo

Figure 3 Signing the digest: Ký thông báo



Trong hệ thống chữ ký số, các bản tin thường dài, nên giải pháp đưa ra là ký bản tin Digest (có độ dài cố định, ngắn hơn bản tin gốc rất nhiều) của nó. Khi đó cần chú ý việc chọn Digest phải có quan hệ 1-1 với bản tin gốc.

3 SERVICES: Các dịch vụ

*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:

- 3.1 Message Authentication**
- 3.2 Message Integrity**
- 3.3 Nonrepudiation**
- 3.4 Confidentiality**

3 SERVICES: Các dịch vụ

Chúng ta đã thảo luận về một số dịch vụ bảo mật trong Chương 1 bao gồm bí mật thông điệp, xác thực thông báo, tính toàn vẹn của thông điệp và không từ chối. Một chữ ký điện tử có thể cung cấp trực tiếp ba phần cuối cùng; để bảo mật thư, chúng ta vẫn cần mã hóa / giải mã.

3.1 Message Authentication

Xác thực bản tin

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

Một lược đồ chữ ký số an toàn, giống như một chữ ký thông thường an toàn có thể cung cấp việc xác thực thông điệp (không dễ bị sao chép).

Note

A digital signature provides message authentication.

Chữ ký điện tử cung cấp xác thực bản tin.

3.2 Message Integrity: Toàn vẹn bản tin

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.

Tính toàn vẹn của thông điệp được bảo toàn ngay cả khi chúng ta ký toàn bộ thông điệp vì chúng ta không thể có được chữ ký giống nhau nếu thông điệp bị thay đổi.

Hiện nay, việc sử dụng lược đồ hàm băm để ký và thuật toán xác thực được sử dụng phổ biến.

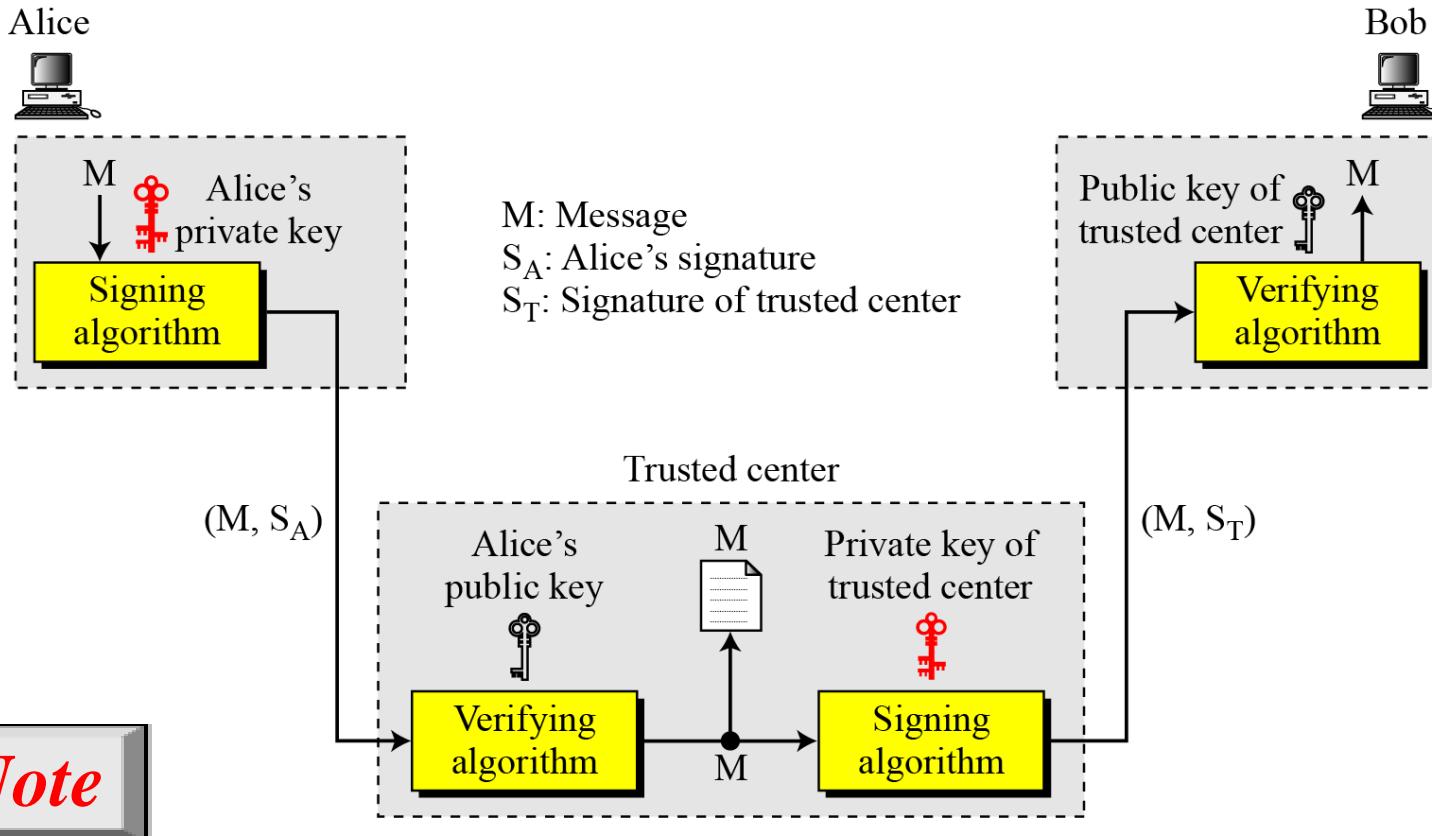
Note

A digital signature provides message integrity.

3.3 Nonrepudiation: Không bác bỏ

Figure 4 Using a trusted center for nonrepudiation

Sử dụng một trung tâm đáng tin cậy để không từ chối



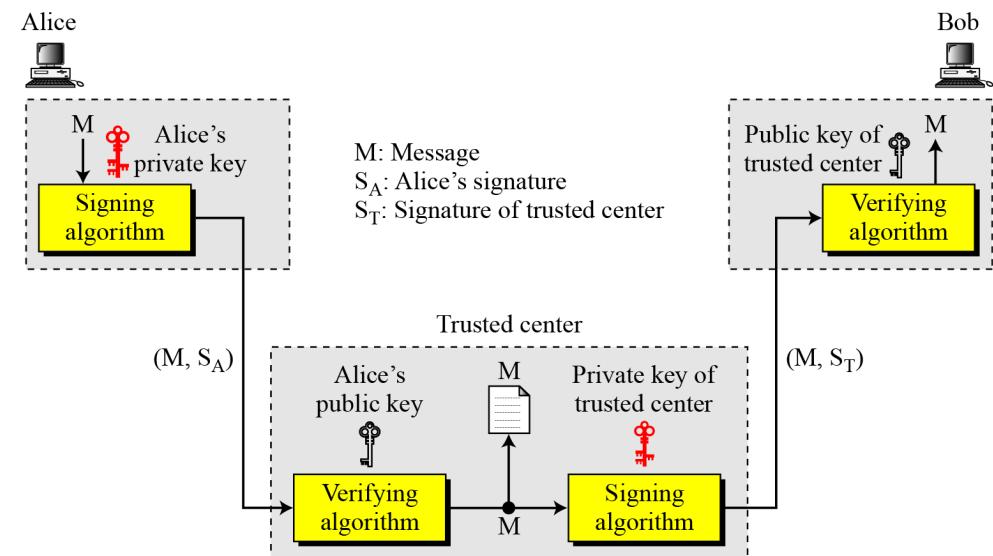
Nonrepudiation can be provided using a trusted party.

3.3 Nonrepudiation: Không bác bỏ

If Alice signs a message and then denies it, can Bob later prove that Alice actually signed it? For example, if Alice sends a message to a bank (Bob) and asks to transfer \$10,000 from her account to Ted's account, can Alice later deny that she sent this message? With the scheme we have presented so far, Bob might have a problem. Bob must keep the signature on file and later use Alice's public key to create the original message to prove the message in the file and the newly created message are the same. This is not feasible because Alice may have changed her private or public key during this time; she may also claim that the file containing the signature is not authentic.

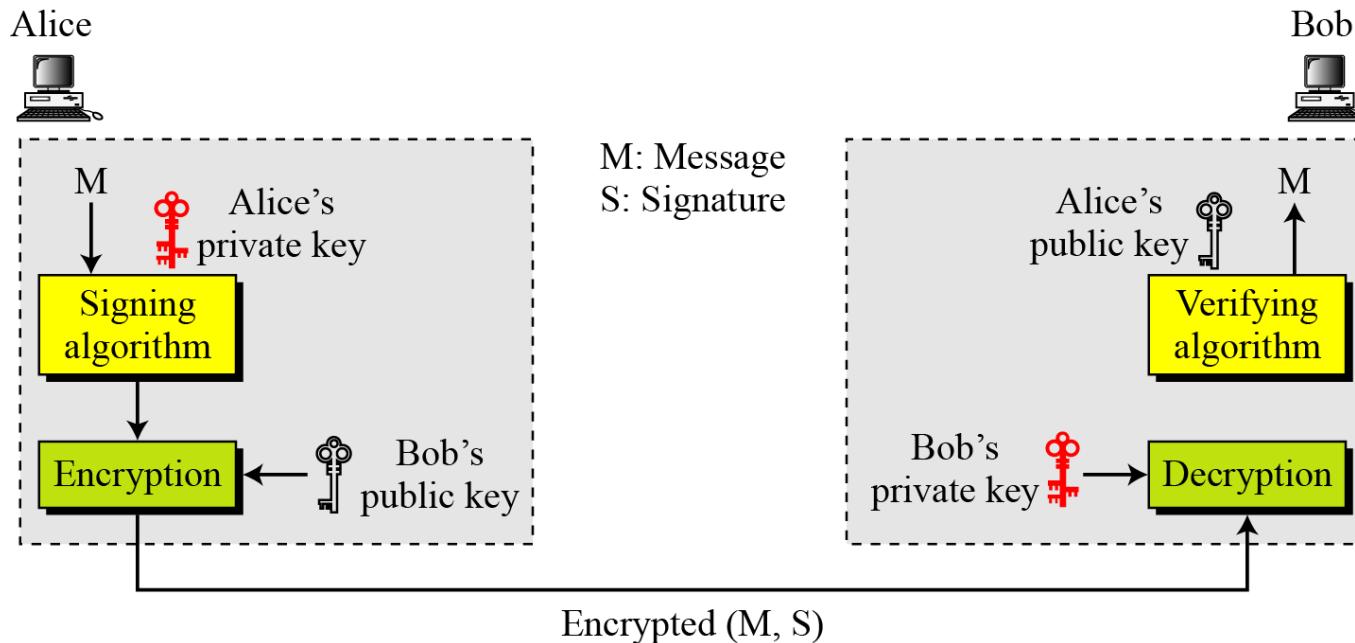
One solution is a trusted third party. People can create an established trusted party among themselves.

Nonrepudiation can be provided using a trusted party.



3.4 Confidentiality: Bí mật

Figure 5 Adding confidentiality to a digital signature scheme



Note

Chữ ký điện tử không cung cấp quyền riêng tư. Nếu có nhu cầu về quyền riêng tư, một lớp mã hóa / giải mã khác phải được áp dụng.

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

4 ATTACKS ON DIGITAL SIGNATURE

This section describes some attacks on digital signatures and defines the types of forgery.

Phần này mô tả một số cuộc tấn công vào chữ ký điện tử và xác định các loại giả mạo.

Topics discussed in this section:

- 4.1 Attack Types: Các loại tấn công**
- 4.2 Forgery Types: Các loại giả mạo**

4.1 Attack Types: Các loại tấn công

Key-Only Attack: Tấn công chỉ vào khóa

Eve tấn công vào thông tin công khai cho bởi Alice. Để tách được bản tin M , Eve cần tạo chữ ký giả của Alice để thuyết phục Bob cho rằng nó là đến từ Alice.

Known-Message Attack: Tấn công bản tin đã biết

Eve truy cập vào một hoặc nhiều cặp bản tin đã ký của Alice sau đó cố tạo ra một bản tin khác để cho Alice ký vào đó.

Chosen-Message Attack: Tấn công bản tin được chọn

4.2 Forgery Types: Các loại giả mạo

Existential Forgery: Giả mạo tồn tại

Selective Forgery: Giả mạo có chọn lọc

5 DIGITAL SIGNATURE SCHEMES

Several digital signature schemes have evolved during the last few decades. Some of them have been implemented.

Một số lược đồ chữ ký điện tử đã phát triển trong vài thập kỷ qua. Một số trong số chúng đã được thực hiện.

Topics discussed in this section:

- 5.1 RSA Digital Signature Scheme**
- 5.2 ElGamal Digital Signature Scheme**
- 5.3 Schnorr Digital Signature Scheme**
- 5.4 Digital Signature Standard (DSS)**
- 5.5 Elliptic Curve Digital Signature Scheme**

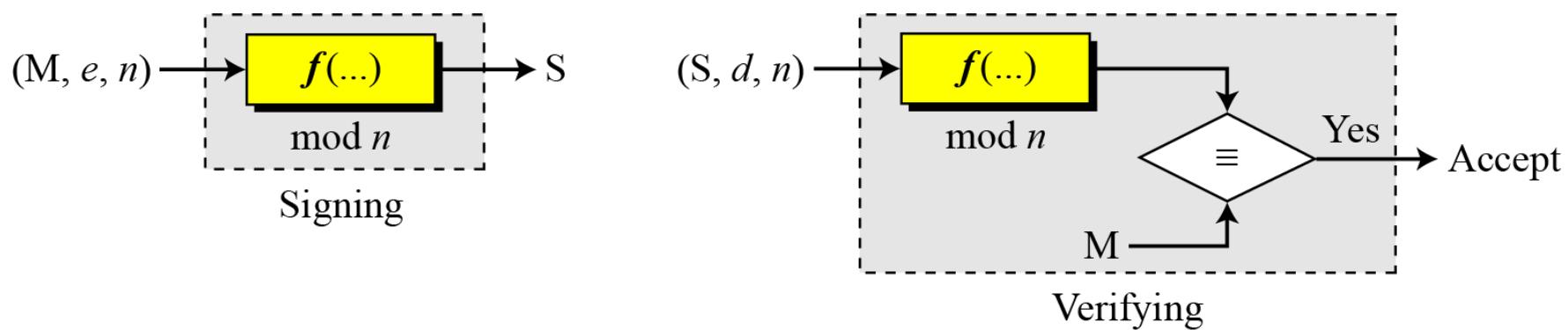
5.1 RSA Digital Signature Scheme

Sơ đồ chữ ký số RSA

Figure 6 General idea behind the RSA digital signature scheme
Ý tưởng chung đằng sau lược đồ chữ ký số RSA

M: Message
S: Signature

(e, n) : Alice's public key
 d : Alice's private key



- + Sơ đồ chữ ký số RSA thay đổi vai trò của các khóa bí mật và công khai: các khóa bí mật và công khai sử dụng là của bên gửi (không phải bên nhận); bên gửi sử dụng khóa bí mật để ký, bên nhận sử dụng khóa công khai của bên gửi để xác thực.
- + Khóa bí mật đóng vai trò chữ ký của bên gửi, khóa công khai của bên gửi đóng vai trò bản sao của chữ ký. Hàm $f(\dots)$ dùng chung cho signing và verifying

5.1 Continued

Key Generation: Tạo khóa

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

Việc tạo khóa trong lược đồ chữ ký số RSA hoàn toàn giống với việc tạo khóa trong RSA

Note

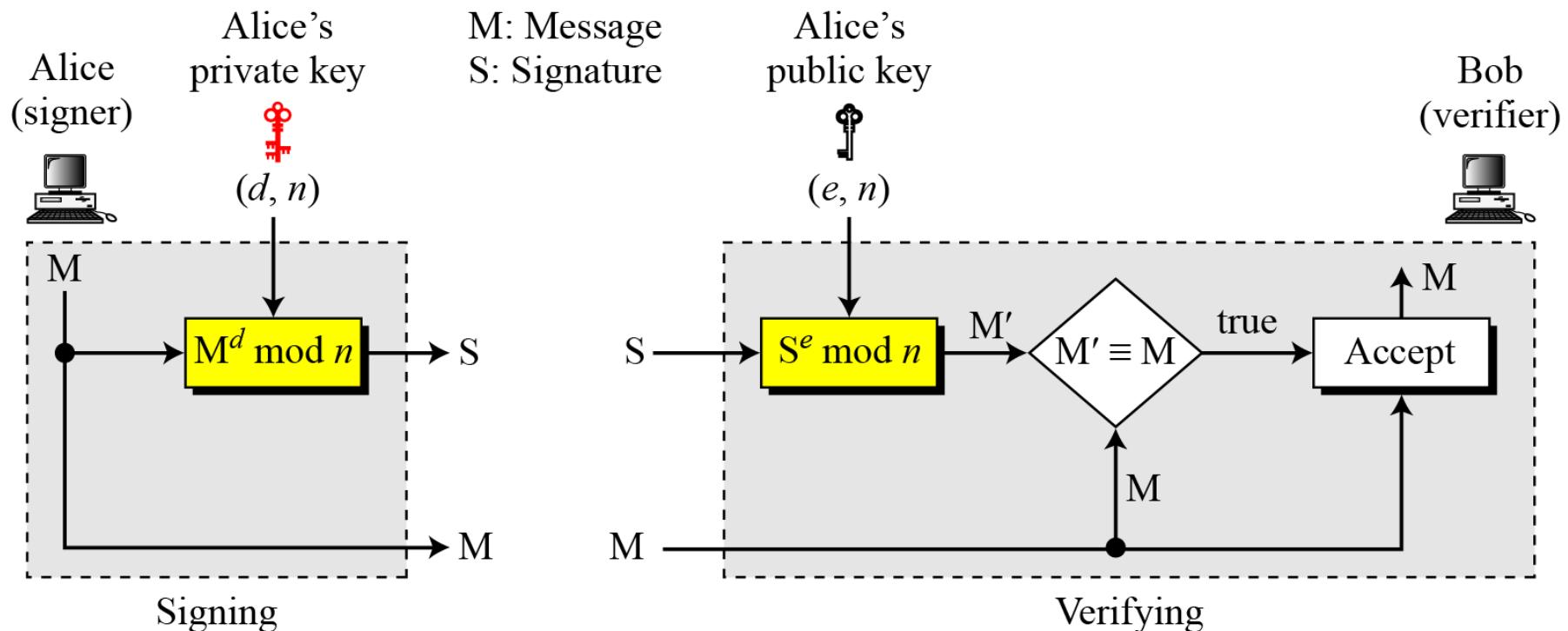
In the RSA digital signature scheme, d is private;
 e and n are public.

5.1 Continued

Signing and Verifying Ký và Xác minh

Chọn hai số nguyên tố p, q , tính $n=p \times q$,
 $\Phi(n)=(p-1)(q-1)$, chọn e , tính d thỏa mãn
 $e \times d = 1 \pmod{\Phi(n)}$

Figure 7 RSA digital signature scheme



5.1 *Continued*

Example 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, **160009**, to sign the message:

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

Alice sends the message and the signature to Bob. Bob receives the message and the signature. He calculates

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

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

5.1 Continued

Example 1

Ví dụ đơn giản, giả sử Alice chọn $p = 823$ và $q = 953$, và tính $n = 784319$. Giá trị của $\phi(n)$ là 782544 . Bây giờ cô ấy chọn $e = 313$ và tính $d = 160009$. Tại thời điểm này, sinh khóa hoàn tất. Bây giờ, hãy tưởng tượng rằng Alice muốn gửi một tin nhắn có giá trị $M = 19070$ cho Bob. Cô ấy sử dụng số mū riêng của mình, 160009 , để ký tin nhắn:

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

Alice gửi tin nhắn và chữ ký cho Bob. Bob nhận được tin nhắn và chữ ký và tính toán

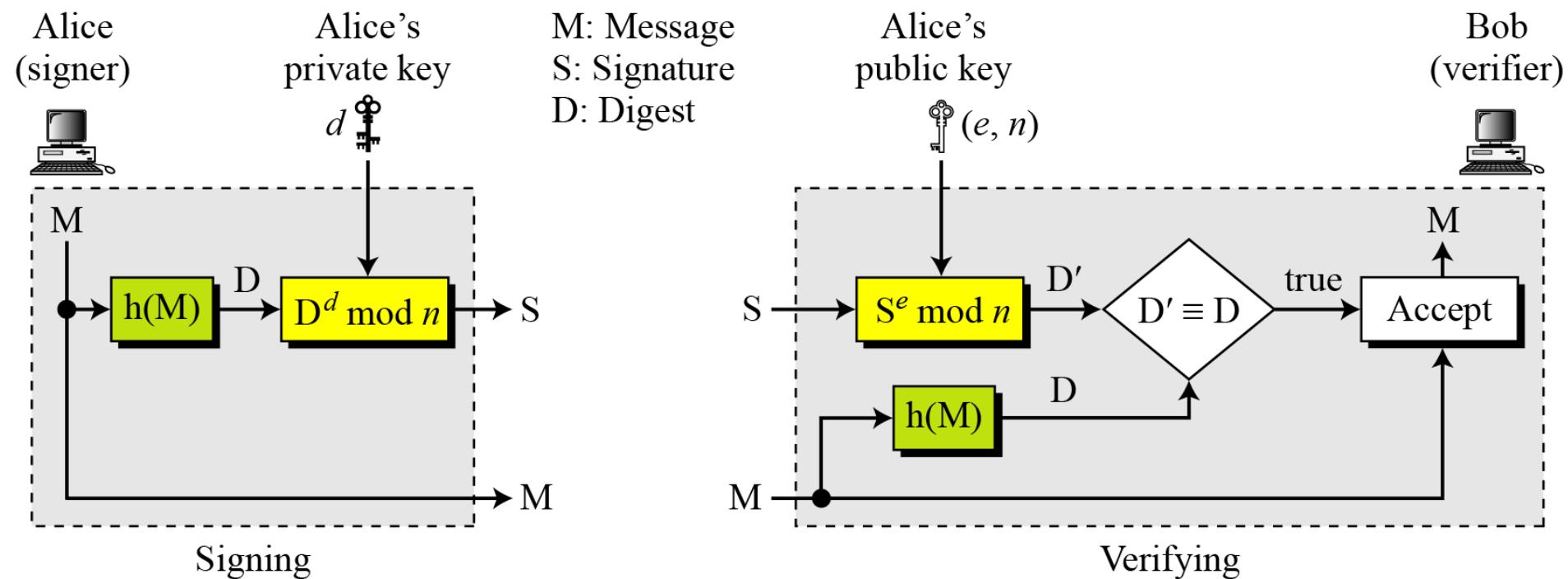
$$M' = 210625^{313} \bmod 784319 = 19070 \bmod 784319 \rightarrow M \equiv M' \bmod n$$

Bob chấp nhận tin nhắn vì Bob đã xác minh chữ ký của Alice.

5.1 Continued

RSA Signature on the Message Digest

Figure 8 The RSA signature on the message digest



5.1 Continued

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.

Khi Digest được ký thay vì chính thông điệp, tính nhạy cảm của lược đồ chữ ký số RSA phụ thuộc vào độ mạnh của thuật toán băm.

5.2 ElGamal Digital Signature Scheme

Lược đồ chữ ký số ElGamal

Figure 9 General idea behind the ElGamal digital signature scheme
Ý tưởng chung

S_1, S_2 : Signatures

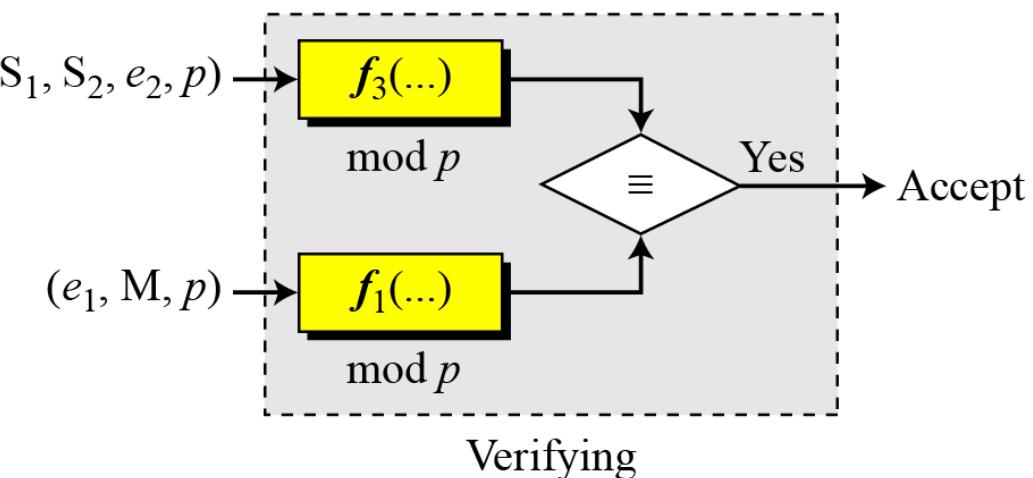
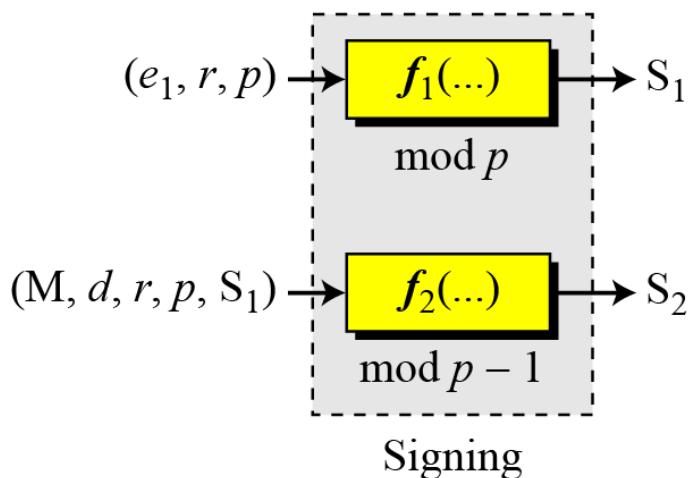
M: Message

(e_1, e_2, p) : Alice's public key

d : Alice's private key

r : Random secret

$$e_2 = e_1^d$$



5.2 Continued

Key Generation: Tạo Khóa

The key generation procedure here is exactly the same as the one used in the cryptosystem.

Quy trình tạo khóa ở đây hoàn toàn giống với quy trình được sử dụng trong hệ thống mật mã

Note

In ElGamal digital signature scheme, (e_1, e_2, p) is Alice's public key; d is her private key.

5.2 Continued

Verifying and Signing: Xác minh và ký

Figure 10 ElGamal digital signature scheme
Lược đồ chữ ký số ElGamal

M: Message

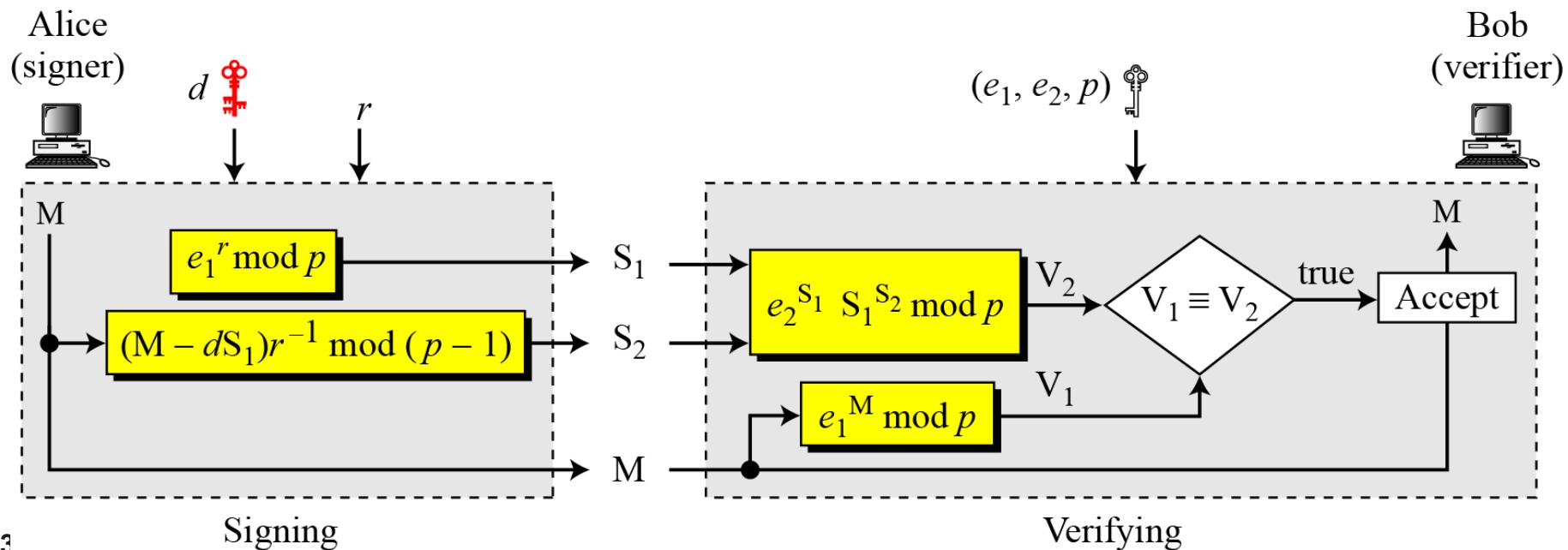
S₁, S₂: Signatures

V₁, V₂: Verifications

r: Random secret

d: Alice's private key

(e₁, e₂, p): Alice's public key



5.1 *Continued*

Example 2

Here is a trivial example. Alice chooses $p = 3119$, $e_1 = 2$, $d = 127$ and calculates $e_2 = 2^{127} \bmod 3119 = 1702$. She also chooses r to be 307. She announces $e1$, $e2$, and p publicly; she keeps d secret. The following shows how Alice can sign a message.

$$M = 320$$

$$S_1 = e_1^r = 2^{307} = 2083 \bmod 3119$$

$$S_2 = (M - d \times S_1) \times r^{-1} = (320 - 127 \times 2083) \times 307^{-1} = 2105 \bmod 3118$$

Alice sends M , S_1 , and S_2 to Bob. Bob uses the public key to calculate V_1 and V_2 .

$$V_1 = e_1^M = 2^{320} = 3006 \bmod 3119$$

$$V_2 = d^{S_1} \times S_1^{S_2} = 1702^{2083} \times 2083^{2105} = 3006 \bmod 3119$$

5.1 *Continued*

Example 2

Đây là một ví dụ nhỏ. Alice chọn $p = 3119$, $e_1 = 2$, $d = 127$ và tính $e_2 = 2^{127} \text{ mod } 3119 = 1702$. Cô ấy cũng chọn r là 307. Cô ấy công bố e_1 , e_2 và p ; cô ấy giữ bí mật d . Sau đây là cách Alice có thể ký một tin nhắn.

$$M = 320$$

$$S_1 = e_1^r = 2^{307} = 2083 \text{ mod } 3119$$

$$S_2 = (M - d \times S_1) \times r^{-1} = (320 - 127 \times 2083) \times 307^{-1} = 2105 \text{ mod } 3118$$

Alice gửi M , S_1 và S_2 cho Bob. Bob sử dụng khóa công khai để tính V_1 và V_2 .

$$V_1 = e_1^M = 2^{320} = 3006 \text{ mod } 3119$$

$$V_2 = d^{S_1} \times S_1^{S_2} = 1702^{2083} \times 2083^{2105} = 3006 \text{ mod } 3119$$

5.1 *Continued*

Example 13.3

Now imagine that Alice wants to send another message, $M = 3000$, to Ted. She chooses a new r , 107. Alice sends M , S_1 , and S_2 to Ted. Ted uses the public keys to calculate V_1 and V_2 .

Bây giờ, hãy tưởng tượng rằng Alice muốn gửi một tin nhắn khác, $M = 3000$, cho Ted. Cô ấy chọn một r mới, 107. Alice gửi M , S_1 và S_2 cho Ted. Ted sử dụng các khóa công khai để tính V_1 và V_2 .

$$M = 3000$$

$$S_1 = e_1^r = 2^{107} = 2732 \text{ mod } 3119$$

$$S_2 = (M - d \times S_1) r^{-1} = (3000 - 127 \times 2083) \times 107^{-1} = 2526 \text{ mod } 3118$$

$$V_1 = e_1^M = 2^{3000} = 704 \text{ mod } 3119$$

$$V_2 = d^{S_1} \times S_1^S = 1702^{2732} \times 2083^{2526} = 704 \text{ mod } 3119$$

Bài Tập Chữ ký số RSA, ElGamal

1. Sử dụng lược đồ RSA: cho $p=809$, $q=751$ và $d=23$, tính khóa công khai e sau đó thực hiện:
 - a. Ký và xác thực bản tin $M_1=100$, kết quả là S_1
 - b. Ký và xác thực bản tin $M_2=50$, kết quả là S_2
 - c. Chỉ ra nếu $M=M_1 \times M_2=50000$ thì $S=S_1 \times S_2$?

2. Sử dụng lược đồ ElGamal, cho $p=881$ và $d=700$, tìm giá trị e_1 và e_2 , chọn $r=17$, hãy tìm giá trị S_1 và S_2 nếu cho $M=400$?

5.3 Schnorr Digital Signature Scheme

Sơ đồ chữ ký số Schnorr

Figure 11 General idea behind the Schnorr digital signature scheme
Ý tưởng chung dựa trên lược đồ ElGamal

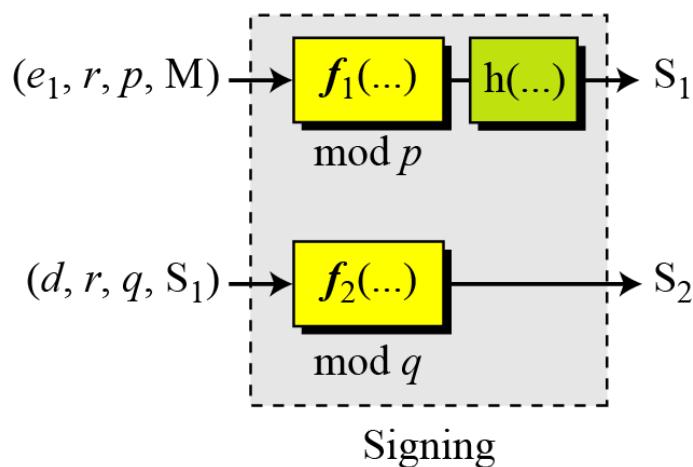
S_1, S_2 : Signatures

(d): Alice's private key

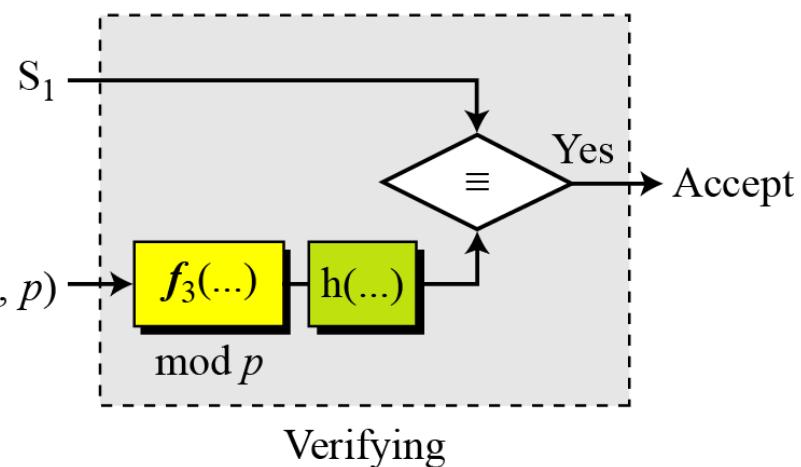
M: Message

r: Random secret

(e_1, e_2, p, q): Alice's public key



$(S_1, S_2, M, e_1, e_2, p)$



Accept

5.3 Continued

Key Generation: Tạo khóa

- 1) Alice selects a prime p , which is usually 1024 bits in length.
- 2) Alice selects another prime q (thường cùng kích thước digest của hàm $h(\dots)$)
- 3) Alice chooses e_1 to be the q th root of 1 modulo p . $e_1 = e_0^{(p-1)q} \text{ mod } p$, **e_0 là giá trị khởi tạo cho bảng.**
- 4) Alice chooses an integer, d , as her private key.
- 5) Alice calculates $e_2 = e_1^d \text{ mod } p$.
- 6) Alice's public key is (e_1, e_2, p, q) ; her private key is (d) .

Note

In the Schnorr digital signature scheme, Alice's public key is (e_1, e_2, p, q) ; her private key (d) .

5.3 Continued

Key Generation: Tạo khóa

- 1) Alice chọn một số nguyên tố p , thường có độ dài 1024 bit.
- 2) Alice chọn q nguyên tố khác.
- 3) Alice chọn e_1 là căn thứ q của 1 módun p .
- 4) Alice chọn một số nguyên, d , làm khóa riêng của cô ấy.
- 5) Alice tính $e_2 = e_1^d \text{ mod } p$.
- 6) Khóa công khai của Alice là (e_1, e_2, p, q) ; khóa riêng của cô ấy là (d) .

Note

In the Schnorr digital signature scheme, Alice's public key is (e_1, e_2, p, q) ; her private key (d) .

5.3 Continued

Signing and Verifying: Ký và Xác minh

Figure 12 Schnorr digital signature scheme

M: Message

S₁, S₂: Signatures

V: Verification

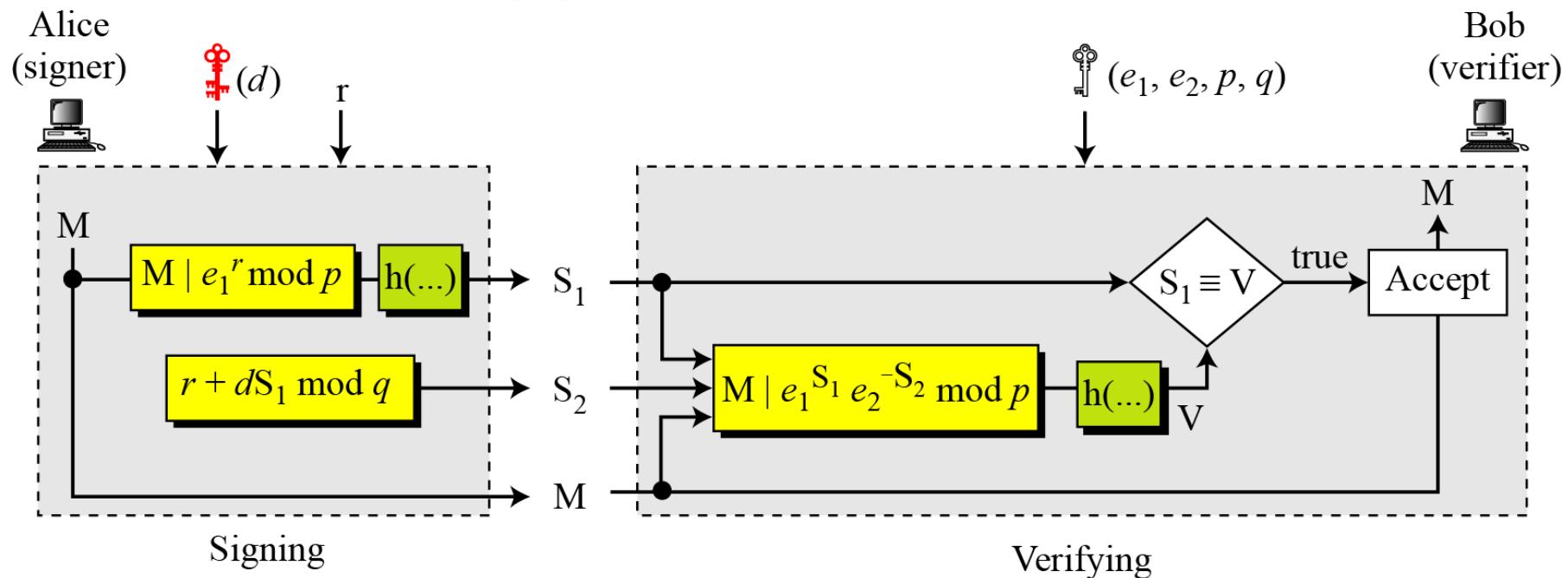
r: Random secret

(d): Alice's private key

(e₁, e₂, p, q): Alice's public key

| : Concatenation

h(...): Hash algorithm



5.3 Continued

Signing

1. Alice chooses a random number r , $1 < r < q$.
2. Alice calculates $S_1 = h(M|e_1^r \bmod p)$.
3. Alice calculates $S_2 = r + d \times S_1 \bmod q$.
4. Alice sends M , S_1 , and S_2 .

Verifying Message

1. Bob calculates $V = h(M | e_1^{S_2} e_2^{-S_1} \bmod p)$.
2. If S_1 is congruent to V modulo p , the message is accepted;

5.1 Continued

Example 4

Here is a trivial example. Suppose we choose $q = 103$ and $p = 2267$. Note that $p = 22 \times q + 1$. We choose $e_0 = 2$, which is a primitive in \mathbb{Z}_{2267}^* . Then $(p - 1) / q = 22$, so we have $e_1 = 2^{22} \bmod 2267 = 354$. We choose $d = 30$, so $e_2 = 354^{30} \bmod 2267 = 1206$. Alice's private key is now (d) ; her public key is (e_1, e_2, p, q) .

Alice wants to send a message M . She chooses $r = 11$ and calculates $e_2^r = 354^{11} = 630 \bmod 2267$. Assume that the message is 1000 and concatenation means 1000630. Also assume that the hash of this value gives the digest $h(1000630) = 200$. This means $S_1 = 200$. Alice calculates $S_2 = r + d \times S_1 \bmod q = 11 + 1026 \times 200 \bmod 103 = 35$. Alice sends the message $M = 1000$, $S_1 = 200$, and $S_2 = 35$. The verification is left as an exercise.

5.4 Digital Signature Standard (DSS)

Chuẩn Chữ Ký Số

Figure 13 General idea behind DSS scheme

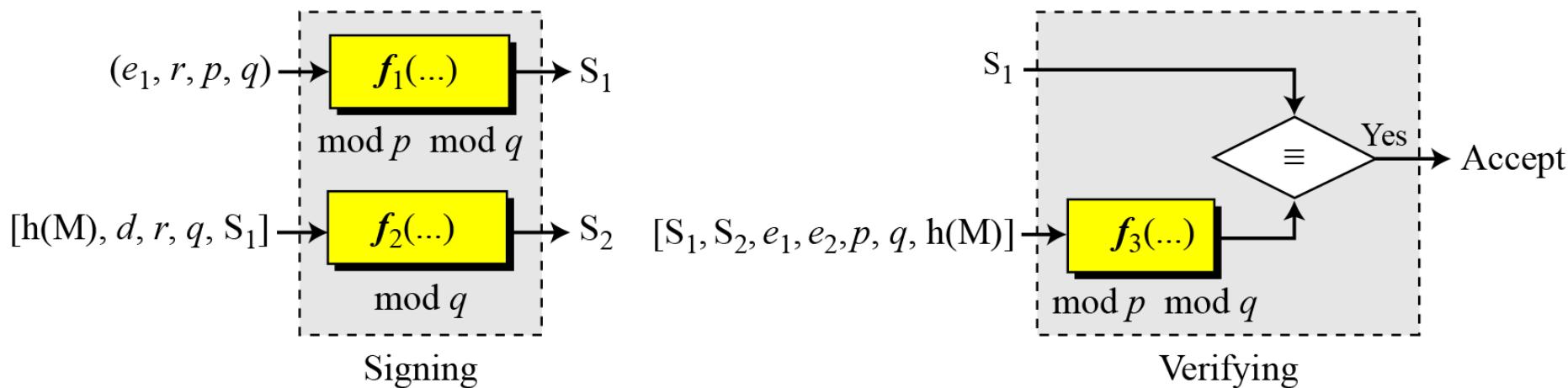
S_1, S_2 : Signatures

d : Alice's private key

M: Message

r : Random secret

(e_1, e_2, p, q) : Alice's public key



Chuẩn này được đưa ra bởi NIST năm 1994, DSS sử dụng thuật toán chữ ký số DSA dựa trên lược đồ ElGamal cùng với ý tưởng của lược đồ Schnorr.

5.4 Continued

Key Generation: Tạo khóa

- 1) *Alice chooses primes p and q , $p = 512 - 1024$ bits, $p =$ multiple of 64; q divides $(p-1)$*
- 2) *Alice uses $\langle \mathbb{Z}_p^*, \times \rangle$ and $\langle \mathbb{Z}_q^*, \times \rangle$.*
- 3) *Alice creates e_1 to be the q th root of 1 modulo p , $e_1^p = 1 \bmod p$.*
- 4) *Alice chooses d as private key and calculates $e_2 = e_1^d$.*
- 5) *Alice's public key is (e_1, e_2, p, q) ; her private key is (d) .*

5.4 Continued

Verifying and Signing

Figure 14 DSS scheme

M: Message

S_1, S_2 : Signatures

V: Verification

r: Random secret

d: Alice's private key

(e_1, e_2, p, q) : Alice's public key

$h(M)$: Message digest

Alice
(signer)



M

$$(e_1^r \bmod p) \bmod q$$

M

$$(h(M) + dS_1)r^{-1} \bmod q$$

S_1

M

$$(e_1^{h(M)S_2^{-1}} e_2^{S_1S_2^{-1}} \bmod p) \bmod q$$



Bob
(verifier)



M

Accept

true

V

$S_1 \equiv V$

Signing

Verifying

5.1 Continued

Example 5

Alice chooses $q = 101$ and $p = 8081$. Alice selects $e_0 = 3$ and calculates $e_1 = e_0^{(p-1)/q} \bmod p = 6968$. Alice chooses $d = 61$ as the private key and calculates $e_2 = e_1^d \bmod p = 2038$. Now Alice can send a message to Bob. Assume that $h(M) = 5000$ and Alice chooses $r = 61$:

$$h(M) = 5000 \quad r = 61$$

$$S_1 = (e_1^r \bmod p) \bmod q = 54$$

$$S_2 = ((h(M) + d S_1) r^{-1}) \bmod q = 40$$

Alice sends M , S_1 , and S_2 to Bob. Bob uses the public keys to calculate V .

$$S_2^{-1} = 48 \bmod 101$$

$$V = [(6968^{5000 \times 48} \times 2038^{54 \times 48}) \bmod 8081] \bmod 101 = 54$$

5.4 Continued

DSS Versus RSA: DSS so với RSA

Computation of DSS signatures is faster than computation of RSA signatures when using the same p.

Tính toán chữ ký DSS nhanh hơn tính toán chữ ký RSA khi sử dụng cùng một p.

DSS Versus ElGamal: DSS so với ElGamal

DSS signatures are smaller than ElGamal signatures because q is smaller than p.

Chữ ký DSS nhỏ hơn chữ ký ElGamal vì q nhỏ hơn p.

5.5 Elliptic Curve Digital Signature Scheme

Figure 15 General idea behind the ECDSS scheme

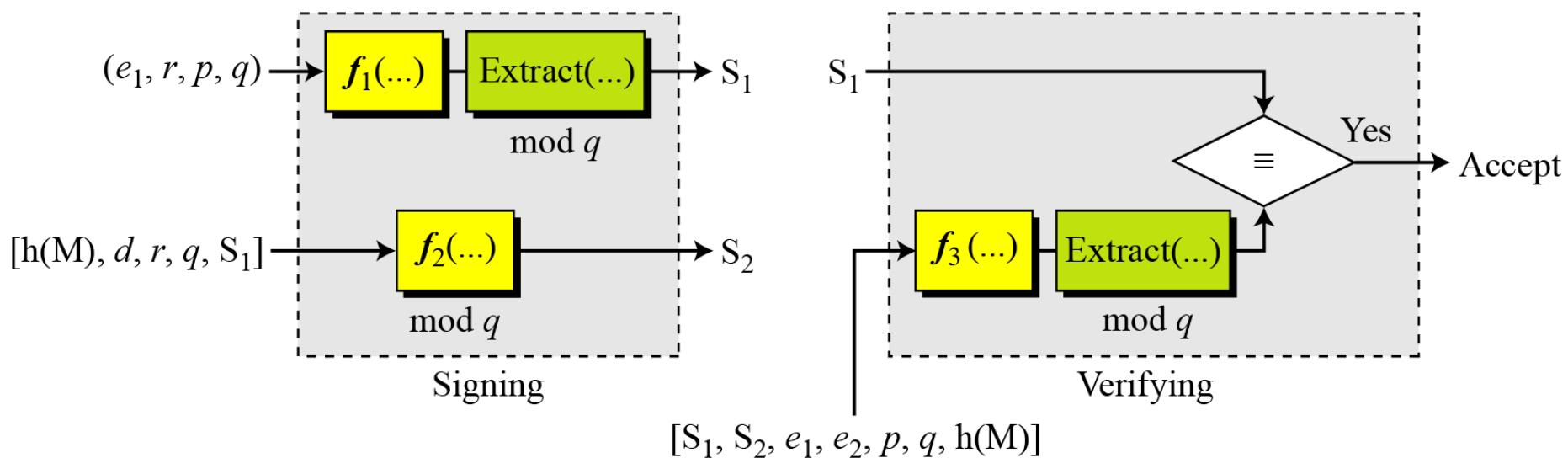
S_1, S_2 : Signatures

M: Message

(a, b, p, q, e_1, e_2) : Alice's public key

d : Alice's private key

r : Random secret



5.5 Continued

Key Generation

Key generation follows these steps:

- 1) *Alice chooses an elliptic curve $E_p(a, b)$.*
- 2) *Alice chooses another prime q the private key d .*
- 3) *Alice chooses $e_1(\dots, \dots)$, a point on the curve.*
- 4) *Alice calculates $e_2(\dots, \dots) = d \times e_1(\dots, \dots)$.*
- 5) *Alice's public key is $(a, b, p, q, e1, e2)$; her private key is d .*

5.5 Continued

Signing and Verifying

Figure 13.16 The ECDSS scheme

M: Message

S_1, S_2 : Signatures

V: Verification

r: Random secret

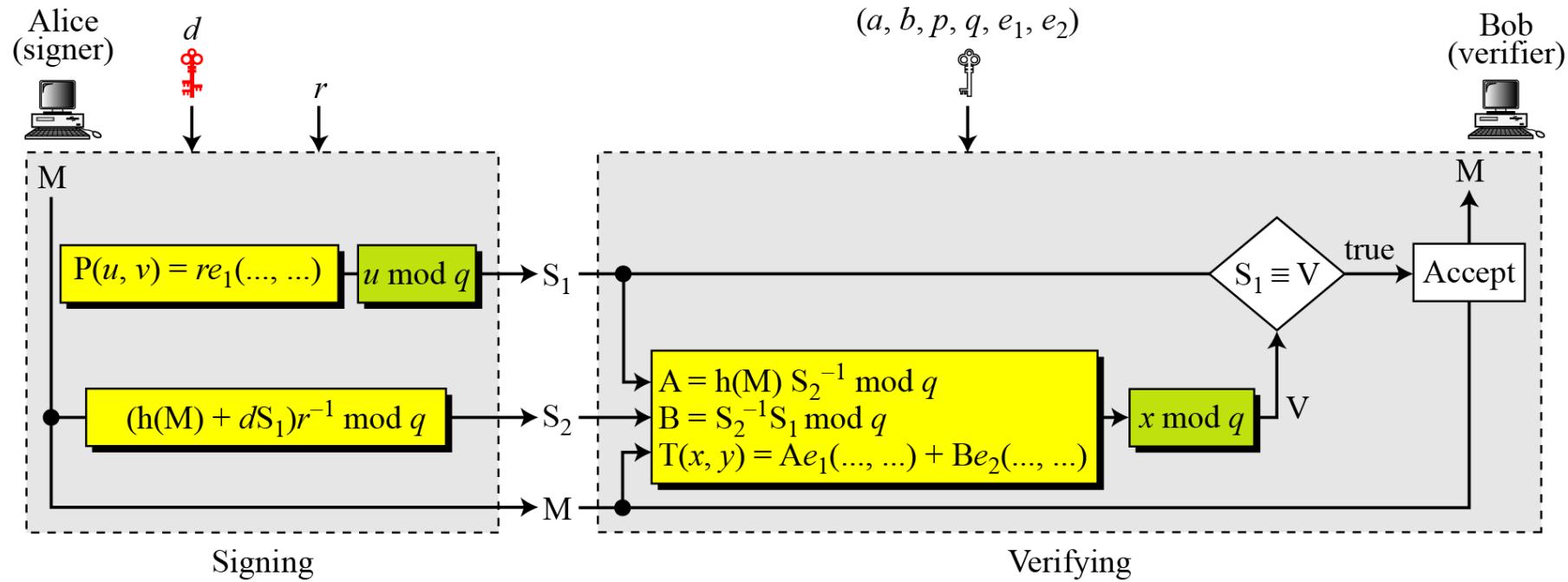
d: Alice's private key

(a, b, p, q, e_1, e_2): Alice's public key

$P(u, v), T(x, y)$: Points on the curve

$h(M)$: Message digest

A, B: Intermediate results



6 VARIATIONS AND APPLICATIONS

This section briefly discusses variations and applications for digital signatures.

Phần này thảo luận ngắn gọn về các biến thể và ứng dụng cho chữ ký điện tử.

Topics discussed in this section:

6.1 Variations

6.2 Applications

6.1 Variations

Time Stamped Signatures: Chữ ký đóng dấu thời gian

Sometimes a signed document needs to be time stamped to prevent it from being replayed by an adversary. This is called time-stamped digital signature scheme.

Đôi khi, một tài liệu đã ký cần được đóng dấu thời gian để tránh bị kẻ thù phát lại. Đây được gọi là lược đồ chữ ký điện tử có dấu thời gian.

Blind Signatures: Chữ ký mù

Sometimes we have a document that we want to get signed without revealing the contents of the document to the signer.

Đôi khi chúng ta có một tài liệu mà chúng ta muốn ký mà không tiết lộ nội dung của tài liệu đó cho người ký.