Digital Signature

Dr Samayveer Singh

Assistant Professor

Department of Computer Science & Engineering

National Institute Technology Jalandhar, Punjab, India

samays@nitj.ac.in

13-1   COMPARISON

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

Topics discussed in this section:

13.1.1 **Inclusion**
13.1.2 **Verification Method**
13.1.3 **Relationship**
13.1.4 **Duplicity**

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.*

- *The sender sends two messages: Message and Signature*

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.*

13.1.3 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.*

13.1.4 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.*

13-2   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.
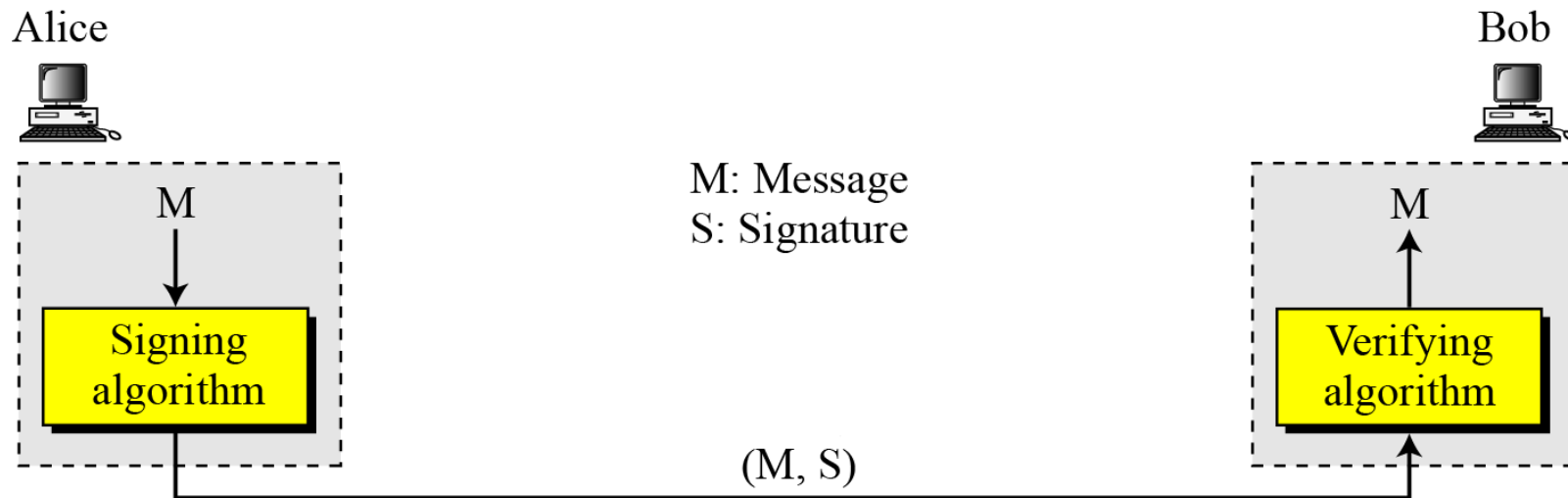
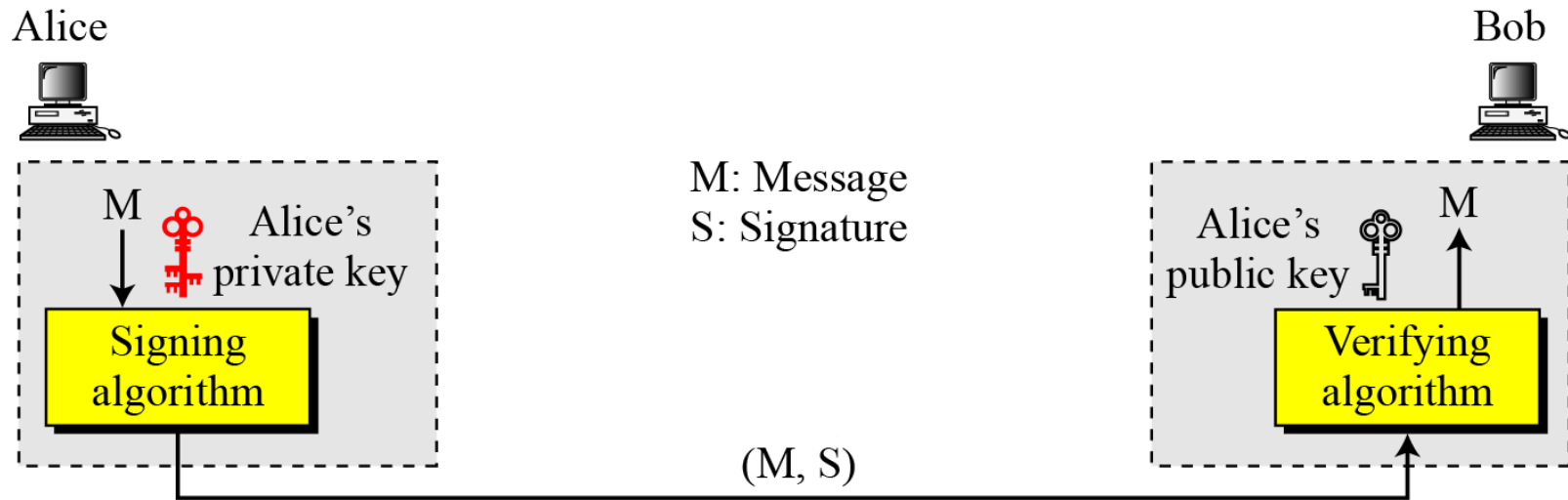*Topics discussed in this section:*

13.2.1 **Need for Keys**
13.2.2 **Signing the Digest**

Figure 13.1 *Digital signature process*

Alice

Bob

M

M: Message
S: Signature

M

Signing
algorithm

Verifying
algorithm

(M, S)

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.
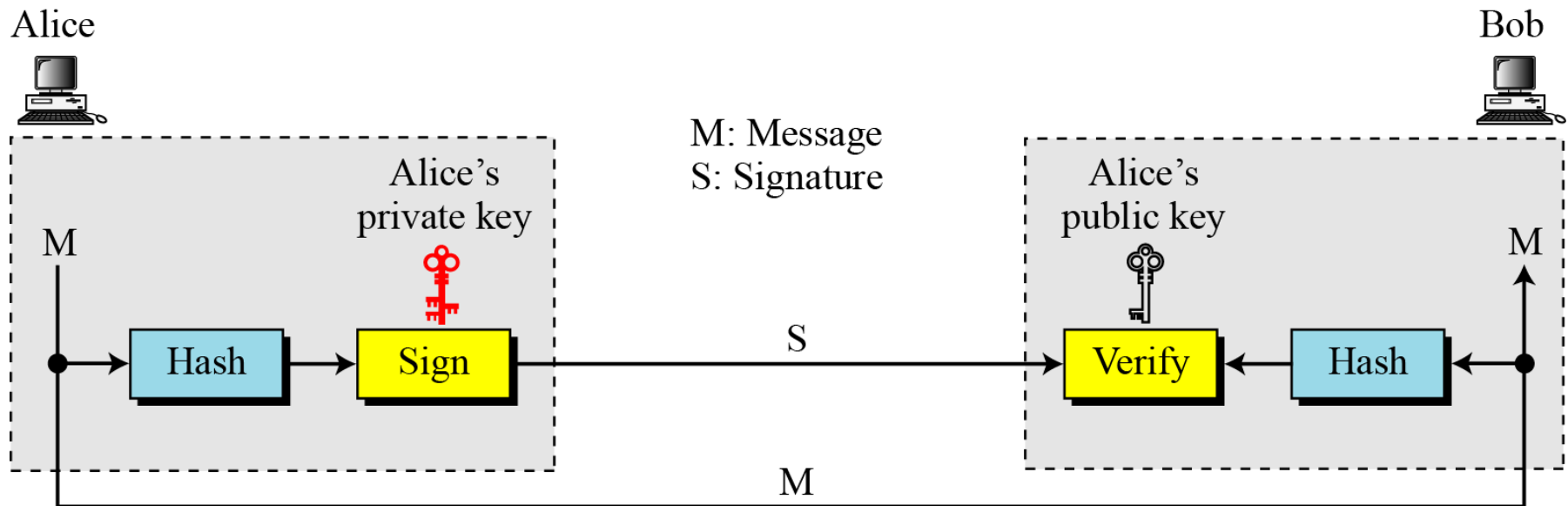
Note

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

Figure 13.3 *Signing the digest*

Alice

Bob

M: Message
S: Signature

Alice's
private key

Alice's
public key

M

M

Hash → Sign

S

Verify ← Hash

M

13-3   SERVICES

We discussed several security services in previous lectures 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**

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.
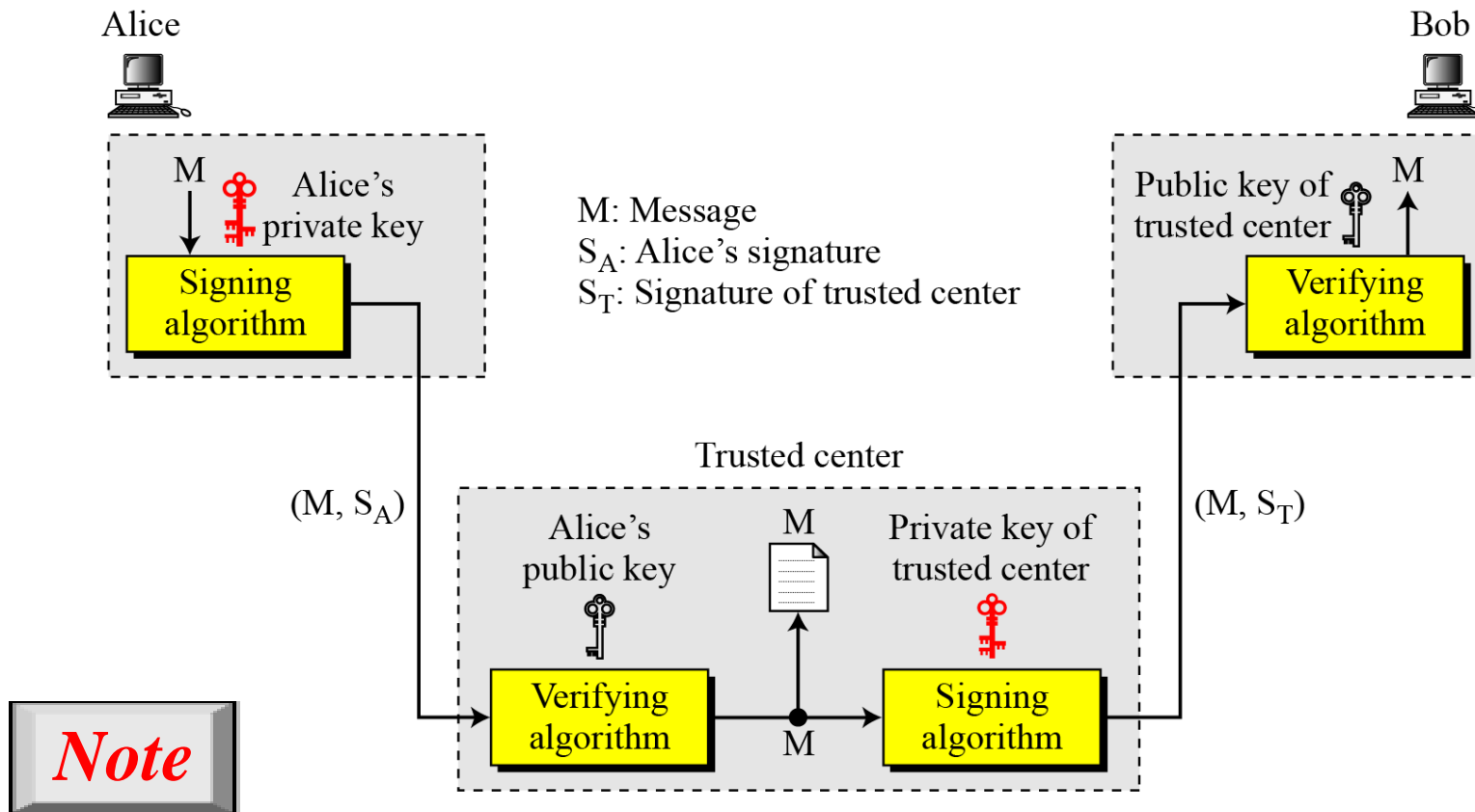
13.3.2 Message Integrity

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.

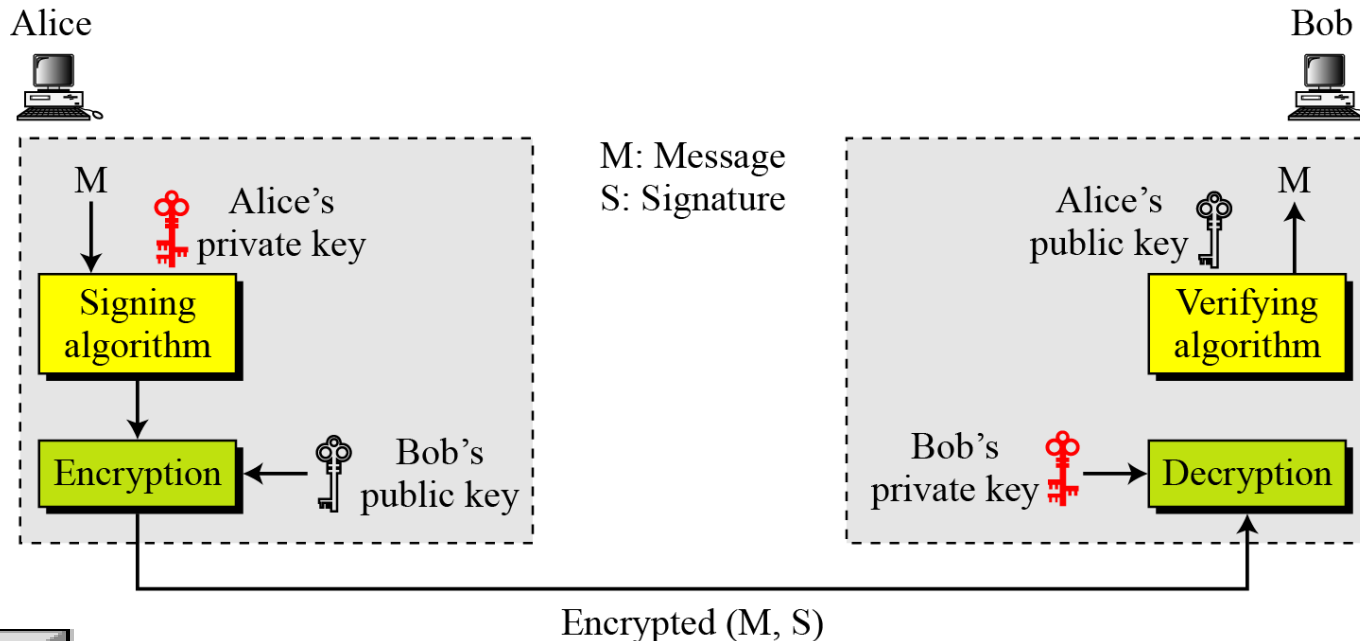**Note**

A digital signature provides message integrity.

Figure 13.4 *Using a trusted center for nonrepudiation*

Note

Nonrepudiation can be provided using a trusted party.

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.

13-5   DIGITAL SIGNATURE SCHEMES

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

Topics discussed in this section:

13.5.1 RSA Digital Signature Scheme
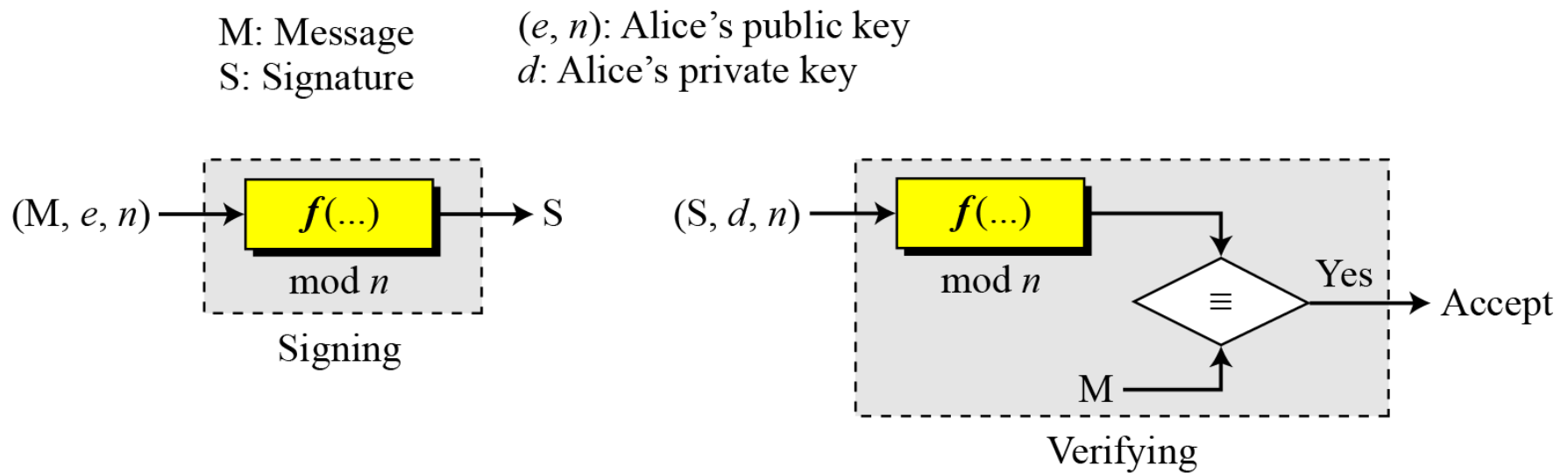13.5.2 ElGamal Digital Signature Scheme
13.5.3 Schnorr Digital Signature Scheme
13.5.4 Digital Signature Standard (DSS)
13.5.5 Elliptic Curve Digital Signature Scheme

13.5.1 RSA Digital Signature Scheme

Figure 13.6 *General idea behind the RSA digital signature scheme*

Key Generation

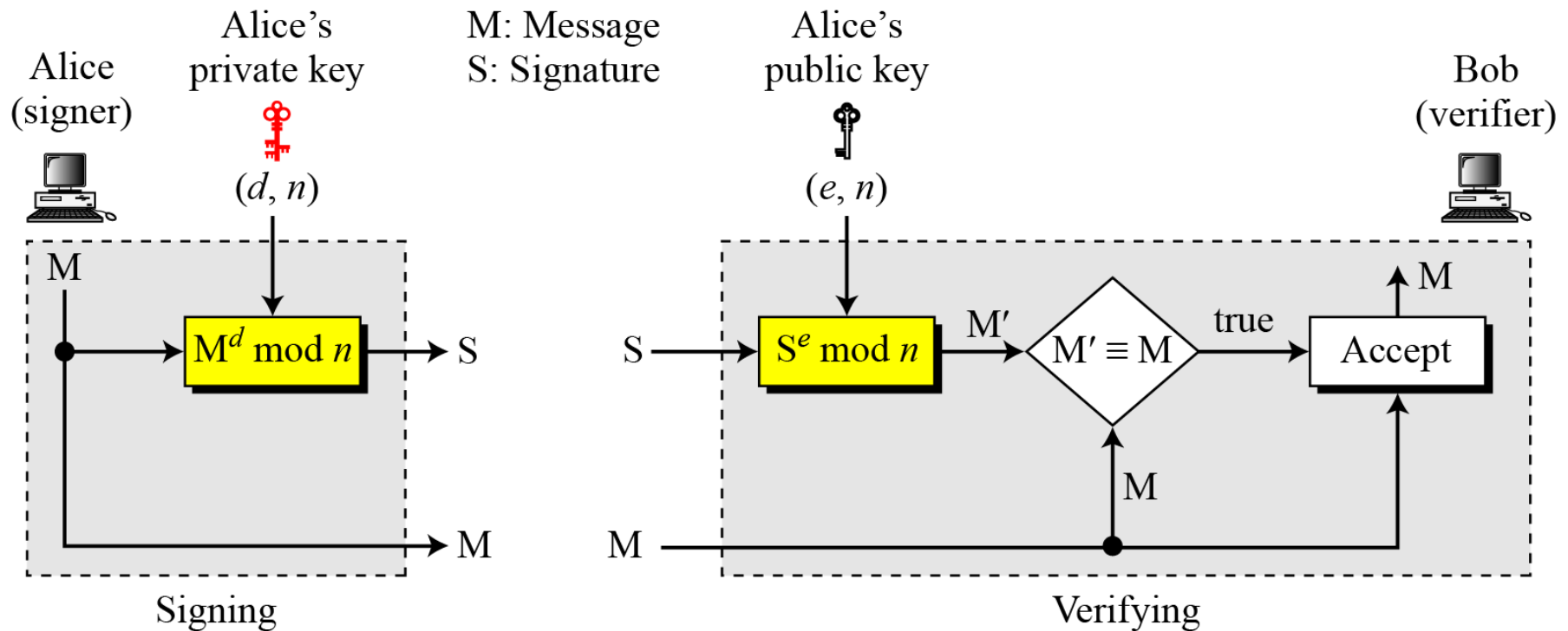*Key generation in the RSA digital signature scheme is exactly the same as key generation in the RSA*

Note

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

Signing and Verifying

Figure 13.7 *RSA digital signature scheme*

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, 160009, to sign the message:

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

Alice sends the message and the signature to Bob. Bob receives the message and the signature. He calculates
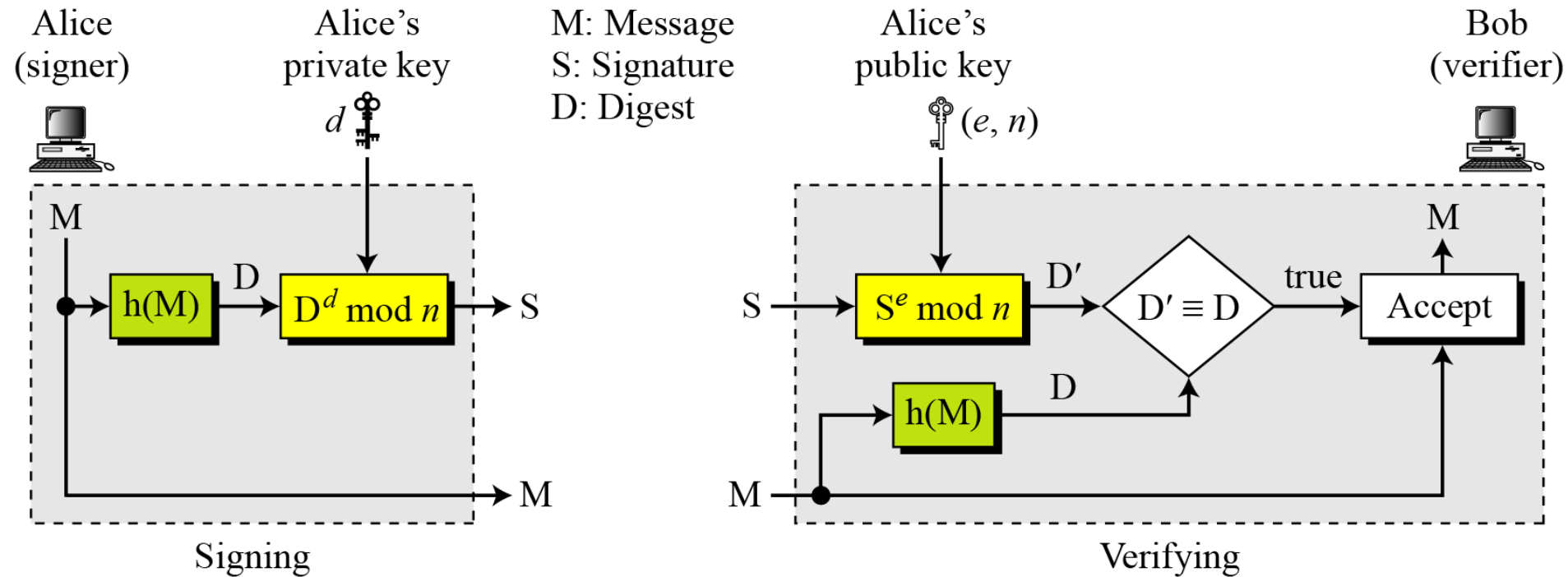
$$M' = 210625^{313} \bmod 784319 = 19070 \bmod 784319 \quad \rightarrow \quad M \equiv M' \bmod n$$

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

RSA Signature on the Message Digest

Figure 13.8 *The RSA signature on the message digest*

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.

Figure 13.9 *General idea behind the ElGamal digital signature scheme*
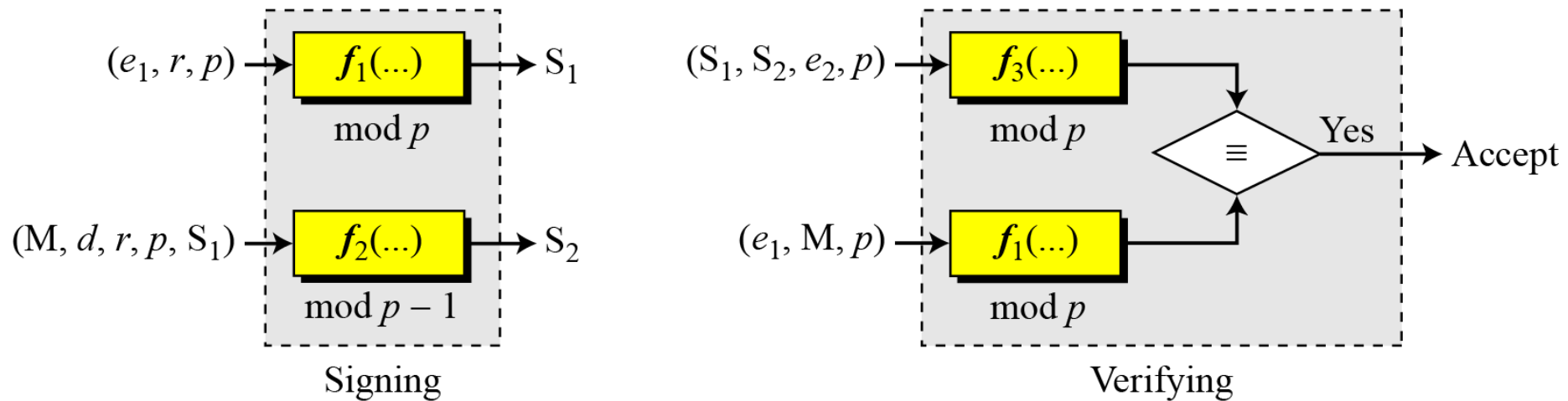
S₁, S₂: Signatures
M: Message
(e₁, e₂, p): Alice's public key

d: Alice's private key
r: Random secret

Key Generation

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

Note

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

Verifying and Signing

Figure 13.10 *ElGamal digital signature scheme*

M: Message r: Random secret
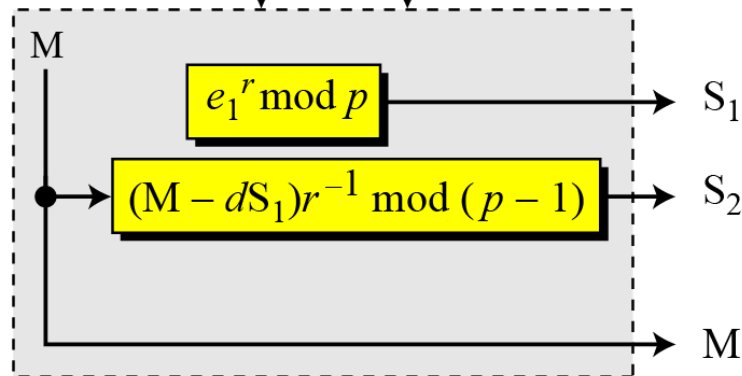S_1, S_2: Signatures d: Alice's private key
V_1, V_2: Verifications (e_1, e_2, p): Alice's public key

Alice
(signer)

d

r

M

$e_1^r \bmod p$ → S_1

$(M - dS_1)r^{-1} \bmod (p-1)$ → S_2

M

Signing

(e_1, e_2, p)

Bob
(verifier)

M

S_1 → $e_2^{S_1} S_1^{S_2} \bmod p$ → V_2

$V_1 \equiv V_2$ → true → Accept

$e_1^M \bmod p$ → V_1

S_2

M
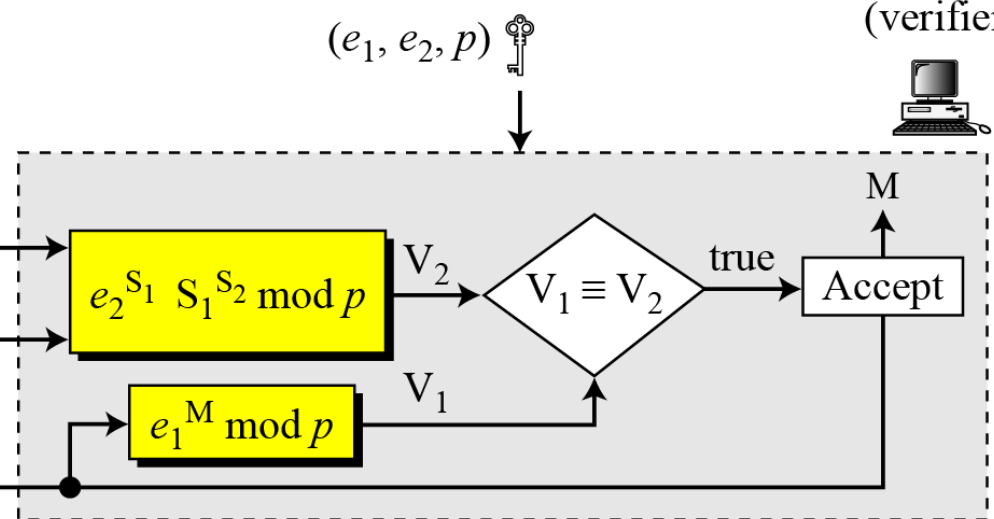
Verifying

Example 13.2

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.

$$V_1 = e_1{}^M = 2^{320} = 3006 \bmod 3119$$
$$V_2 = d^{S_1} \times S_1{}^{S_2} = 1702^{2083} \times 2083^{2105} = 3006 \bmod 3119$$

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.

$$M = 3000$$
$$S_1 = e_1{}^r = 2^{107} = 2732 \bmod 3119$$
$$S_2 = (M - d \times S_1)\, r^{-1} = (3000 - 127 \times 2083) \times 107^{-1} = 2526 \bmod 3118$$

$$V_1 = e_1{}^M = 2^{3000} = 704 \bmod 3119$$
$$V_2 = d^{S_1} \times S_1{}^S = 1702^{2732} \times 2083^{2526} = 704 \bmod 3119$$

Figure 13.11 *General idea behind the Schnorr digital signature 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

Key Generation

1) *Alice selects a prime p, which is usually 1024 bits in length.*

2) *Alice selects another prime q.*

3) *Alice chooses e_1 to be the qth root of 1 modulo p.*

   $e_1 = e_0^{(p-1)/q}$ mod p where e_0 is the primitive element in Z_p^*.

4) *Alice chooses an integer, d, as her private key.*

5) *Alice calculates $e_2 = e_1^d$ 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).

Signing and Verifying

Figure 13.12 *Schnorr digital signature scheme*

M: Message r: Random secret | : Concatenation
S_1, S_2: Signatures   (d): Alice's private key   h(...): Hash algorithm
V: Verification   (e_1, e_2, p, q): Alice's public key

Alice (signer)   (d)   r   (e_1, e_2, p, q)   Bob (verifier)

M

$M \mid e_1^{r} \bmod p$ h(...) → S_1 $S_1 \equiv V$ → true → Accept → M

$r + dS_1 \bmod q$ → S_2 $M \mid e_1^{S_1} e_2^{-S_2} \bmod p$ h(...) → V

M
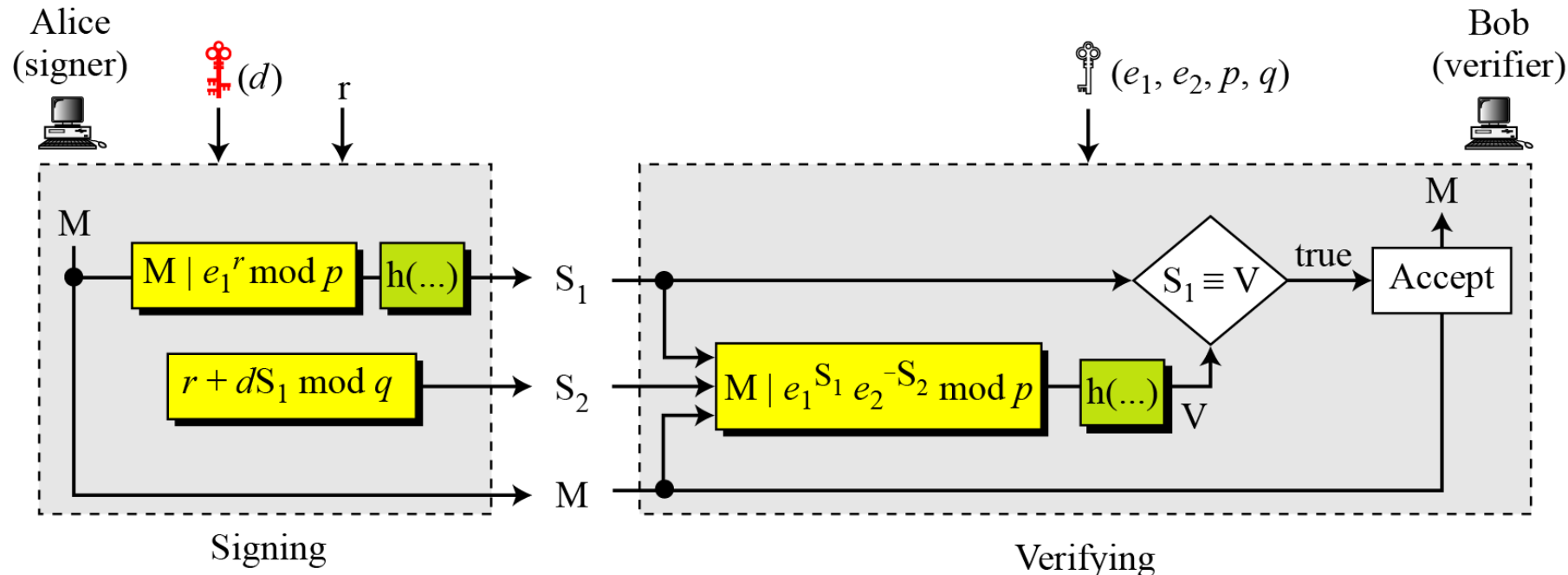
Signing   Verifying

Signing

1. Alice chooses a random number r.

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 $V = h (M / e_1^{S2} e_2^{-S1} \bmod p)$.

2. If S_1 is congruent to V modulo p, the message is accepted;

13.5.1 Continued

Example 13.4

Here is a trivial example. Suppose we choose $q = 103$ and $p = 2267$. We choose $e_0 = 2$, which is a primitive in Z_{2267}^*. Then $(p - 1) / q = 22$, so we have $e_1 = 2^{22}$ mod $2267 = 354$. We choose $d = 30$, so $e_2 = 354^{30}$ mod $2267 = 1206$. 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 $e_2{}^r = 354^{11} = 630$ mod 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 S1 = 200. Alice calculates S2 = $r + d \times S_1$ mod $q = 11 + 30 \times 200$ mod $103 = 37$. Alice sends the message M =1000, $S_1 = 200$, and $S_2 = 37$. The verification is left as an exercise.

Figure 13.13 *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

Key Generation.

1) **Alice chooses primes p and q.**

2) **Alice uses $<Z_p^*, \times>$ and $<Z_q^*, \times>$.**

3) **Alice creates e_1 to be the qth root of 1 modulo p.**
$e_1 = e_0^{(p-1)/q}$ mod p where e_0 is the primitive element in Z_p^*.

4) **Alice chooses d and calculates $e_2 = e_1^d$ mod p**

5) **Alice's public key is (e_1, e_2, p, q); her private key is (d).**

Verifying and Signing

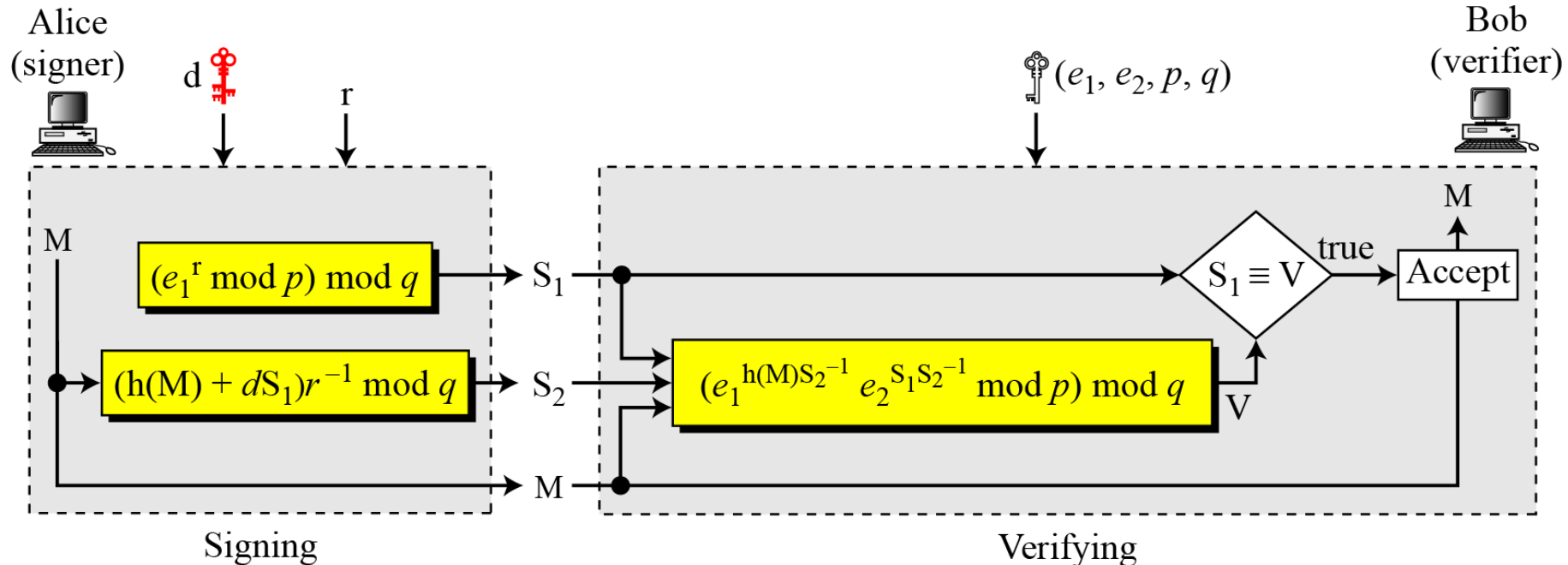**Figure 13.14** *DSS scheme*

M: Message r: Random secret   h(M): Message digest

S_1, S_2: Signatures d: Alice's private key

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

Alice (signer)

Bob (verifier)

d r (e_1, e_2, p, q)

M

$(e_1^{\,r} \bmod p) \bmod q$ → S_1

$(h(M) + dS_1)r^{-1} \bmod q$ → S_2

$(e_1^{\,h(M)S_2^{-1}} \, e_2^{\,S_1 S_2^{-1}} \bmod p) \bmod q$ V

$S_1 \equiv V$ true   Accept   M

→ M

Signing   Verifying

Example 13.5

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 $r = 61$:

$$h(M) = 5000 \qquad r = 61$$
$$S_1 = (e_1^r \bmod p) \bmod q = 54$$
$$S_2 = ((h(M) + d\,S_1)\,r^{-1}) \bmod q = 40$$

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

$$S_2^{-1} = 48 \bmod 101$$
$$V = [(6968^{5000 \times 48} \times 2038^{54 \times 48}) \bmod 8081] \bmod 101 = 54$$

DSS Versus RSA

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

DSS Versus ElGamal

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