
Digital Signature

(Book: Cryptography and Network Security by Forouzan)

<https://youtu.be/y6e70OKHg7c?feature=shared>

<https://youtu.be/jXw-CXYT01M?feature=shared>

Introduction

- ▶ Differences between conventional signatures and digital signatures.
 - ▶ Signature Generation
 - ▶ 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.

Introduction...

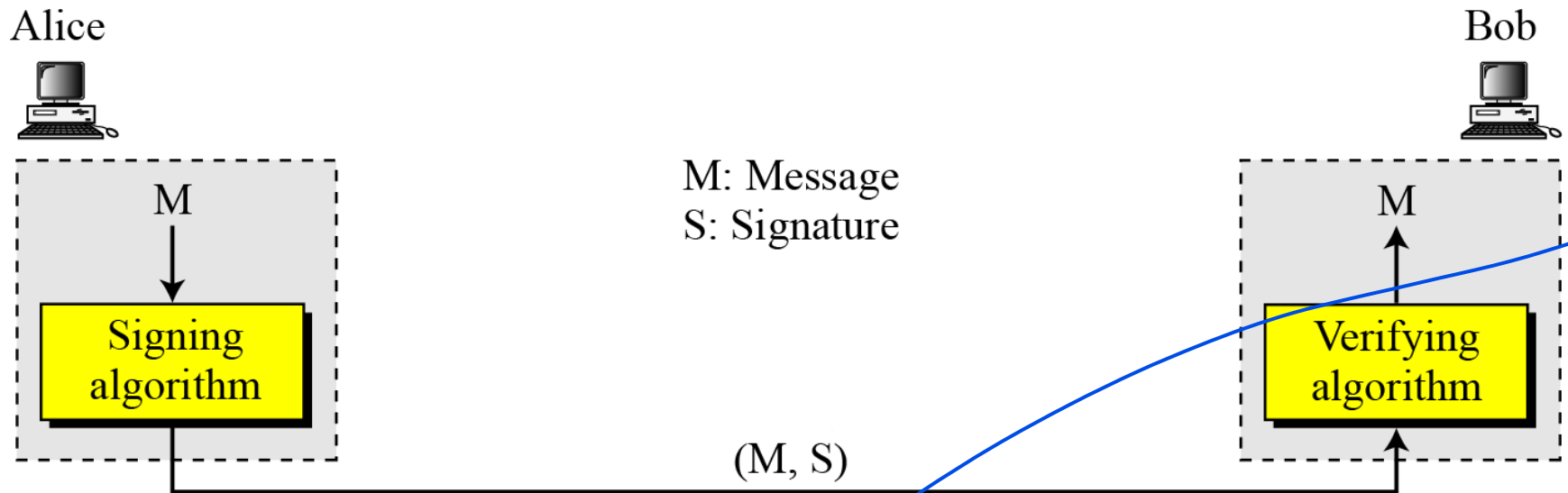
▶ Signature Verification

- ▶ 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.

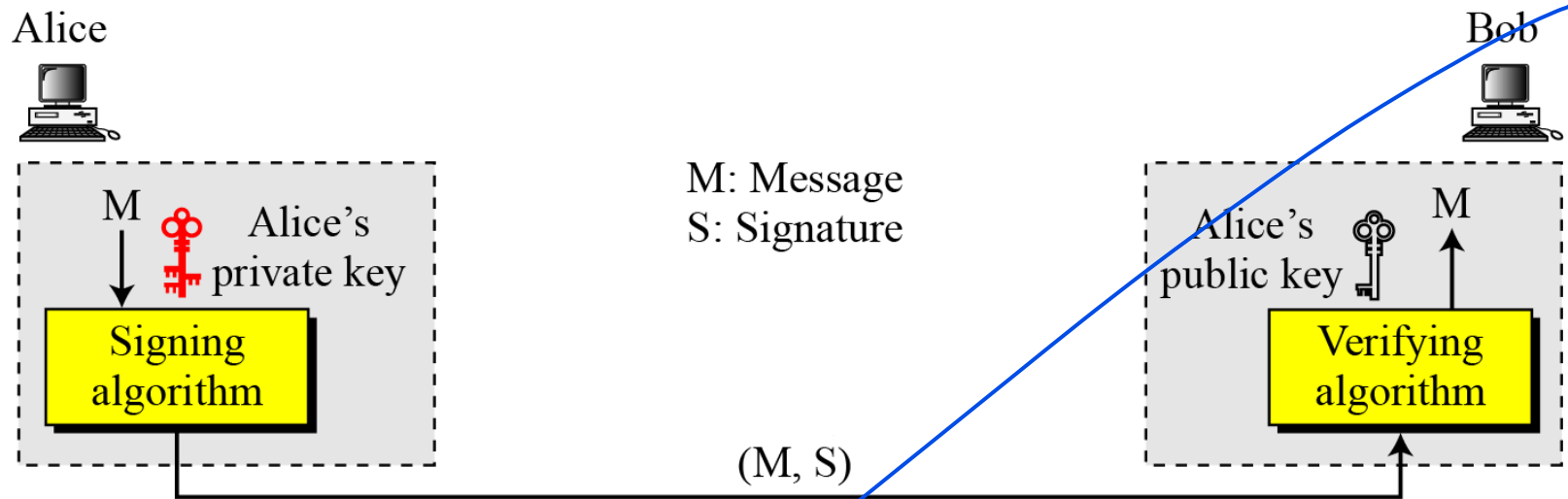
Introduction...

- ▶ 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.
- ▶ 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.

Digital Signature: Process



Need for Keys

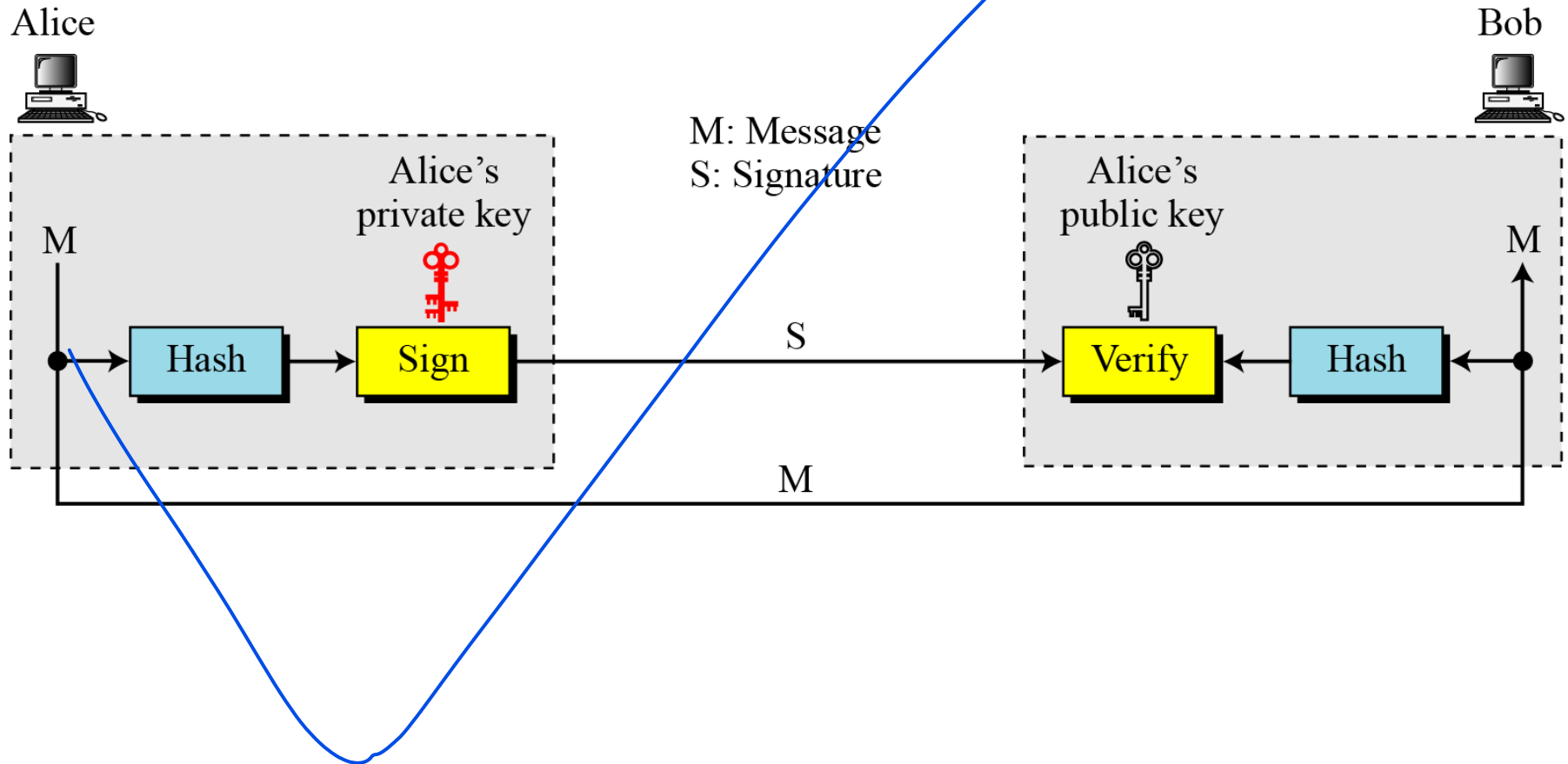


A digital signature needs a public-key system.
The signer signs with her private key; the verifier verifies with the signer's public key.

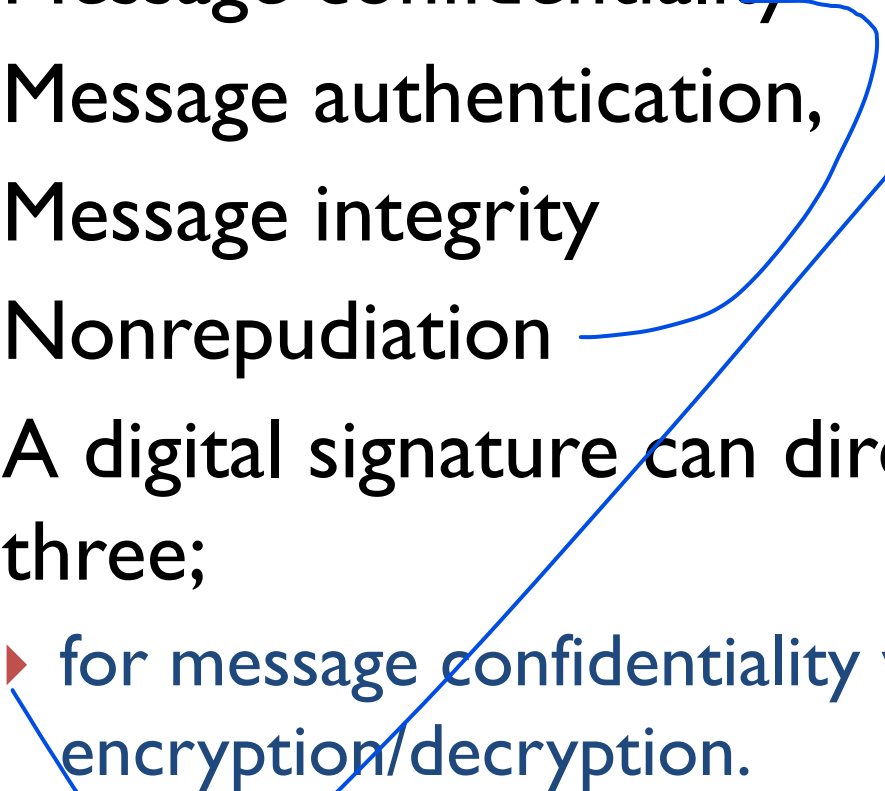
Need for Keys...

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

Signing the digest



Security Services offered by digital signature

- ▶ Message confidentiality
 - ▶ Message authentication,
 - ▶ Message integrity
 - ▶ Nonrepudiation
 - ▶ A digital signature can directly provide the last three;
 - ▶ for message confidentiality we still need encryption/decryption.
- 

Message Authentication

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

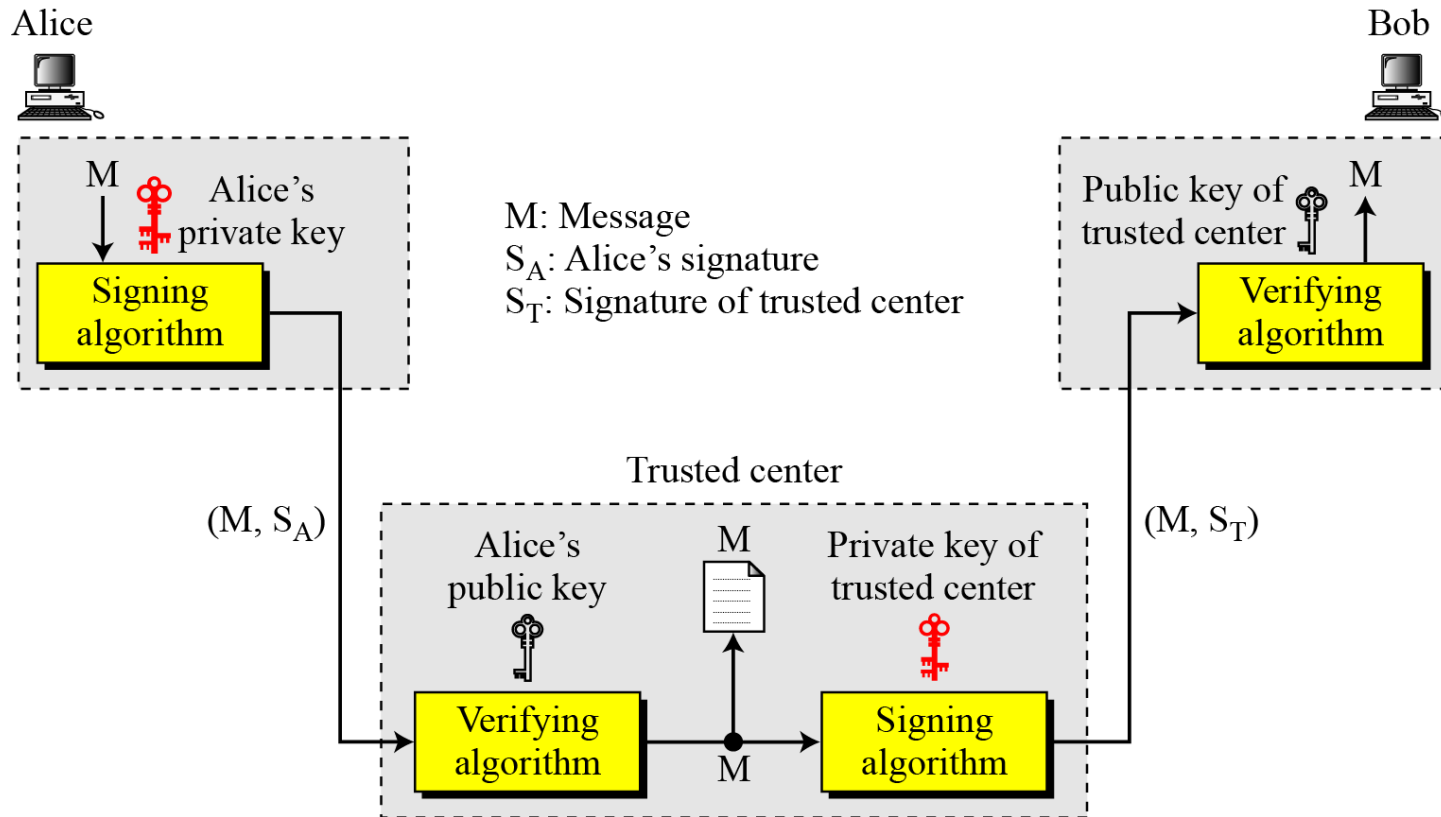
A digital signature provides message authentication.

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.

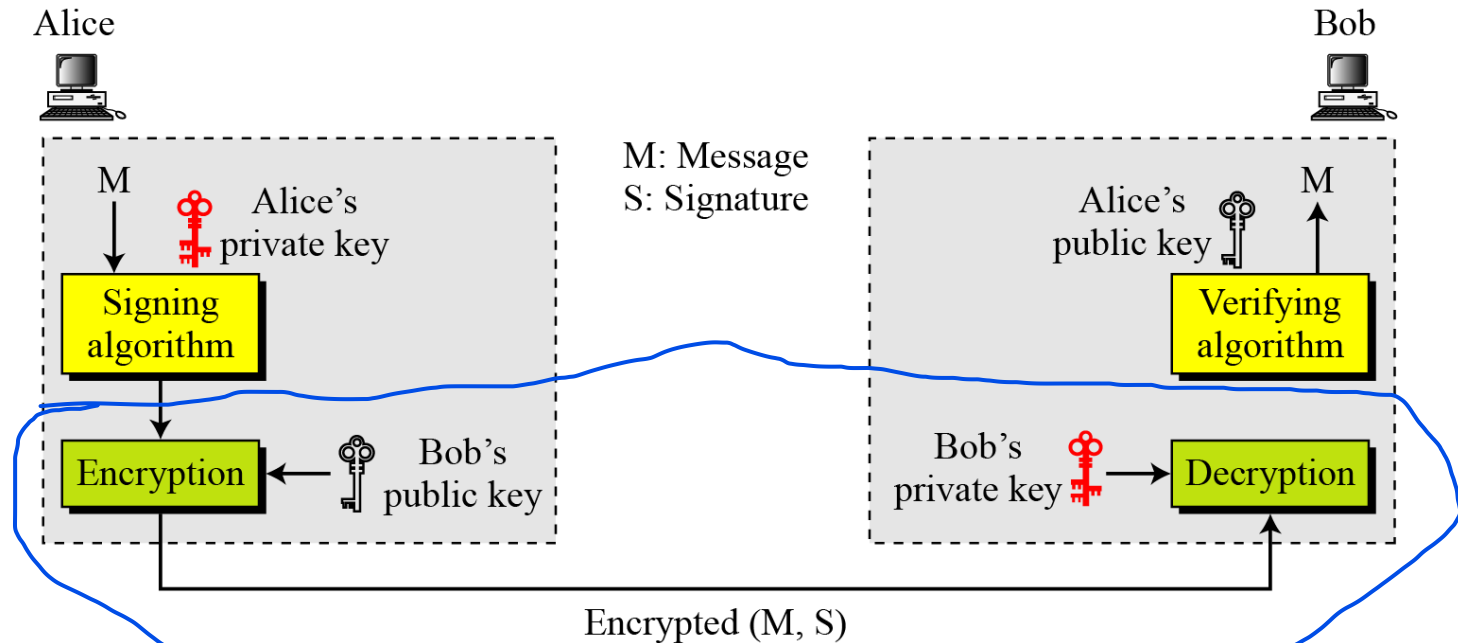
A digital signature provides message integrity.

Nonrepudiation



Nonrepudiation can be provided using a trusted party.

Confidentiality



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

Attack types

- ▶ **Key-Only Attack**

- ▶ the attacker is only given the public verification key.

- ▶ **Known-Message Attack**

- ▶ the attacker is given valid signatures for a variety of messages known by the attacker but not chosen by the attacker.

- ▶ **Chosen-Message Attack**

- ▶ the attacker first learns signatures on arbitrary messages of the attacker's choice.

Forgery Types

▶ Existential Forgery

- ▶ Existential forgery is the creation (by an adversary) of any message/signature pair (m, σ) , where σ was not produced by the legitimate signer.

▶ Selective Forgery

- ▶ Selective forgery is the creation (by an adversary) of a message/signature pair (m, σ) where m has been chosen by the adversary prior to the attack.

Digital Signature Schemes

Digital Signature Schemes

- ▶ RSA Digital Signature Scheme
- ▶ Digital Signature Standard (DSS)
- ▶ Elliptic Curve Digital Signature Scheme

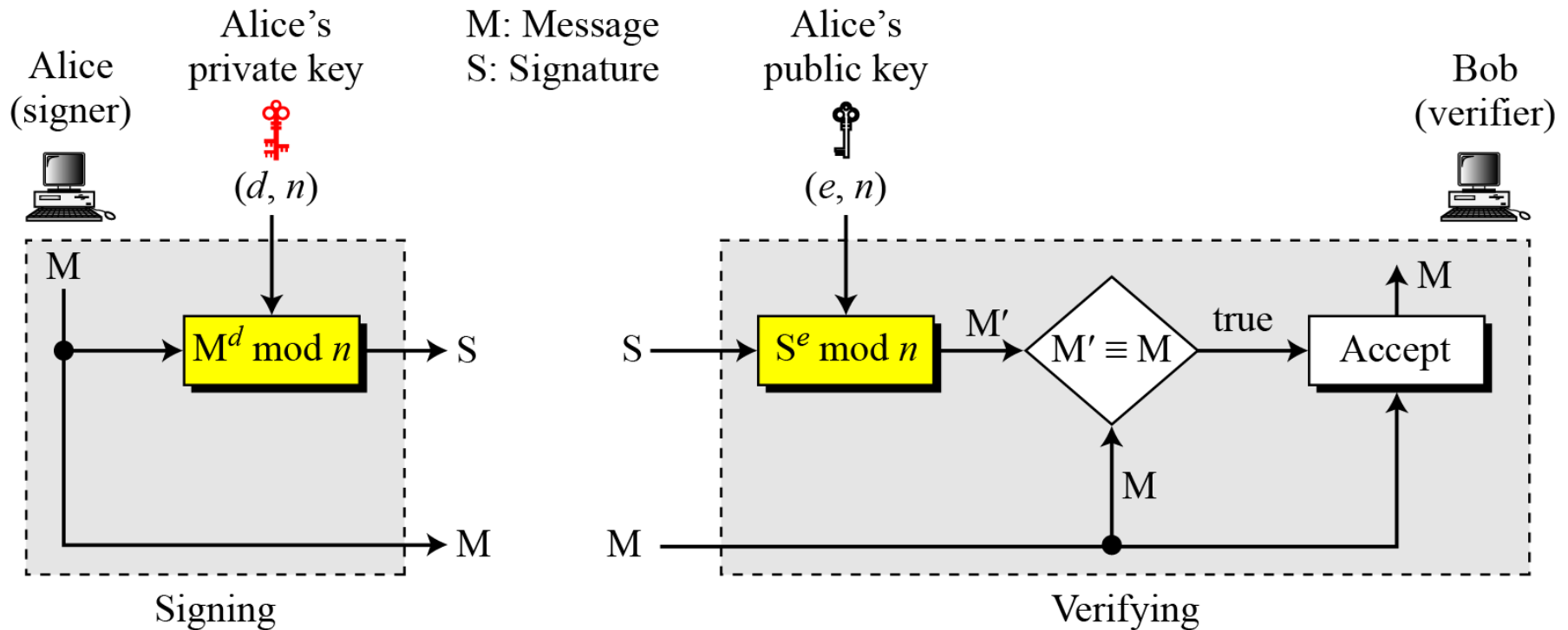
RSA Digital Signature Scheme

▶ Key Generation

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

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

RSA Digital Signature Scheme...



RSA Digital Signature Scheme...

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.



RSA Digital Signature Scheme...

▶ Key only attack:

- ▶ Eve has access only to Alice's public key. Eve intercepts the pair (M, S) and tries to create another message M' such that it generates the same S

▶ Known-message attack:

- ▶ Eve intercepts two message signature pairs (M_1, S_1) and (M_2, S_2) that have been created using same private key. Can Eve find Signature on the message $M_1 \times M_2$?

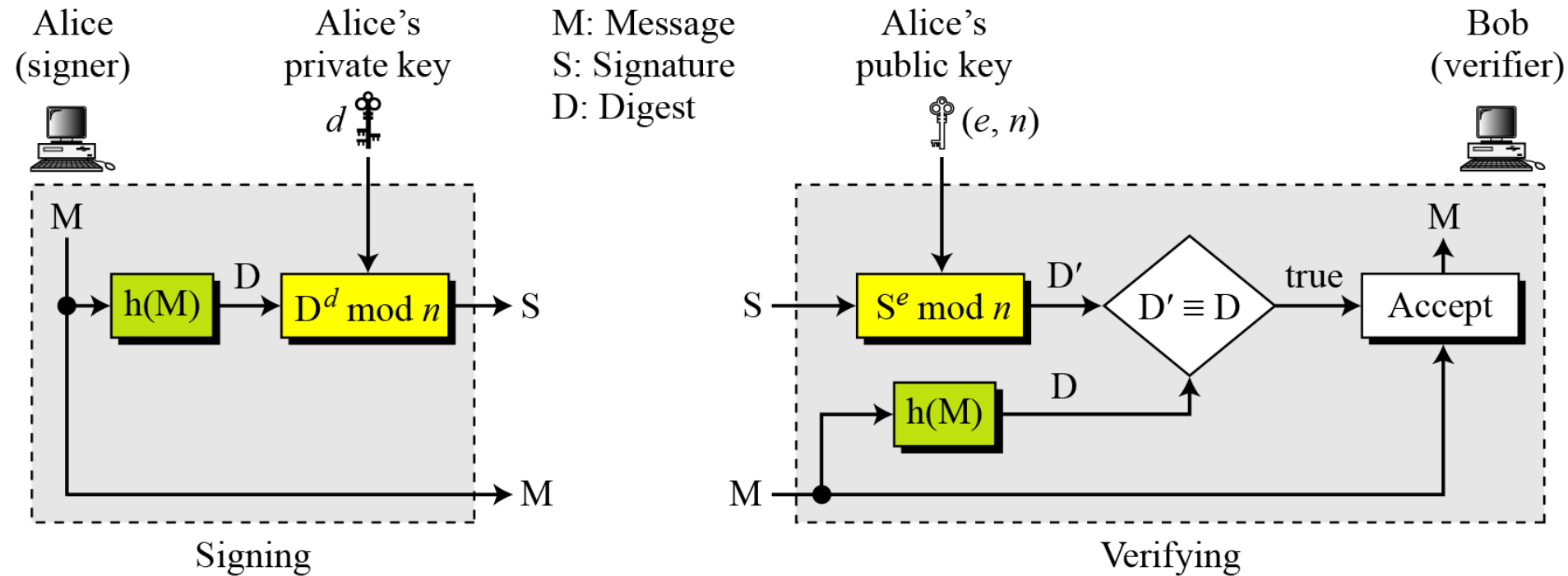
▶ Chosen-message attack: aene khabar je ke hu to M1 and M2 thi kaik alag message banavi lais.

- ▶ What if Eve convince Alice to sign M_1 and M_2 chosen by her? Is this selective forgery or existential ?

So, selective forgery is like Eve picking specific notes for you to sign, then using those signatures to make a note you never actually approved. It's like pretending you said something you didn't.

RSA Digital Signature Scheme...

RSA Signature on the Message Digest



RSA Digital Signature Scheme...

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.

Can you justify the above statement?

RSA Digital Signature Scheme...

▶ Key only attack:

- ▶ Eve intercepts the pair (M, S) and tries to create another message M' such that it creates the same digest !!!
- ▶ Eve finds two messages M_1 and M_2 such that they hash to same value !!! **collision attack**.

▶ Known-message attack:

- ▶ Eve intercepts two message signature pairs (M_1, S_1) and (M_2, S_2) that have been created using same private key. Can Eve find Signature on the message $M_1 \times M_2$?
- ▶ Can Eve calculate the message $M = M_1 \times M_2$ and its signature ?

▶ Chosen-message attack:

- ▶ What if Eve convince Alice to sign M_1 and M_2 chosen by her?
- ▶ Can Eve calculate the message $M = M_1 \times M_2$ and its signature ?

Digital Signature Standard (DSS)

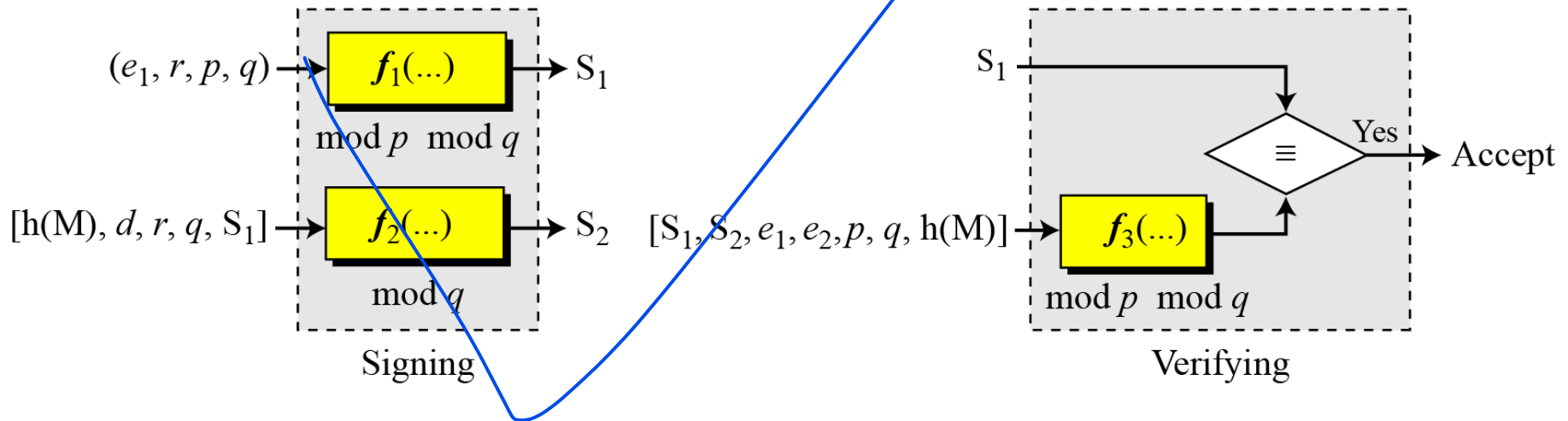
S_1, S_2 : Signatures

M : Message

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

d : Alice's private key

r : Random secret



Digital Signature Standard (DSS)...

Key Generation.

- 1) Alice chooses primes p and q .
- 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 .
- 4) Alice chooses d and calculates $e_2 = e_1^d$.
- 5) Alice's public key is (e_1, e_2, p, q) ; her private key is (d) .

Digital Signature Standard (DSS)...

M: Message

r : Random secret

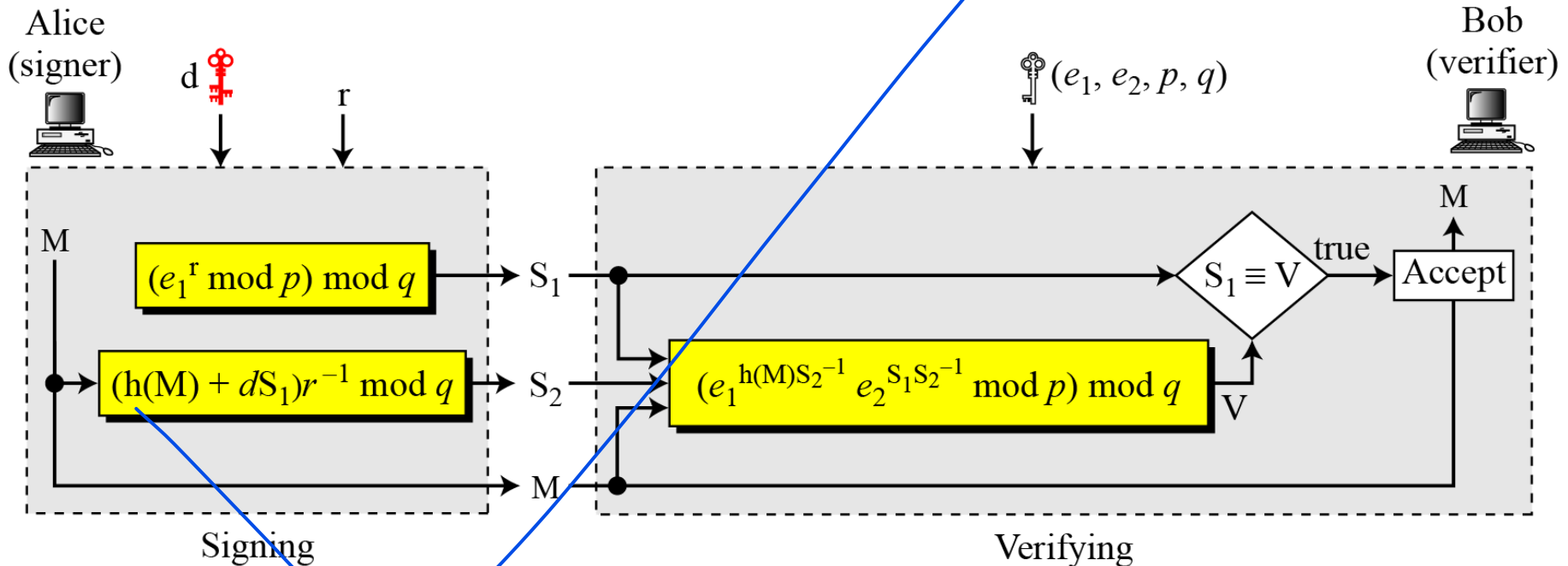
$h(M)$: Message digest

S_1, S_2 : Signatures

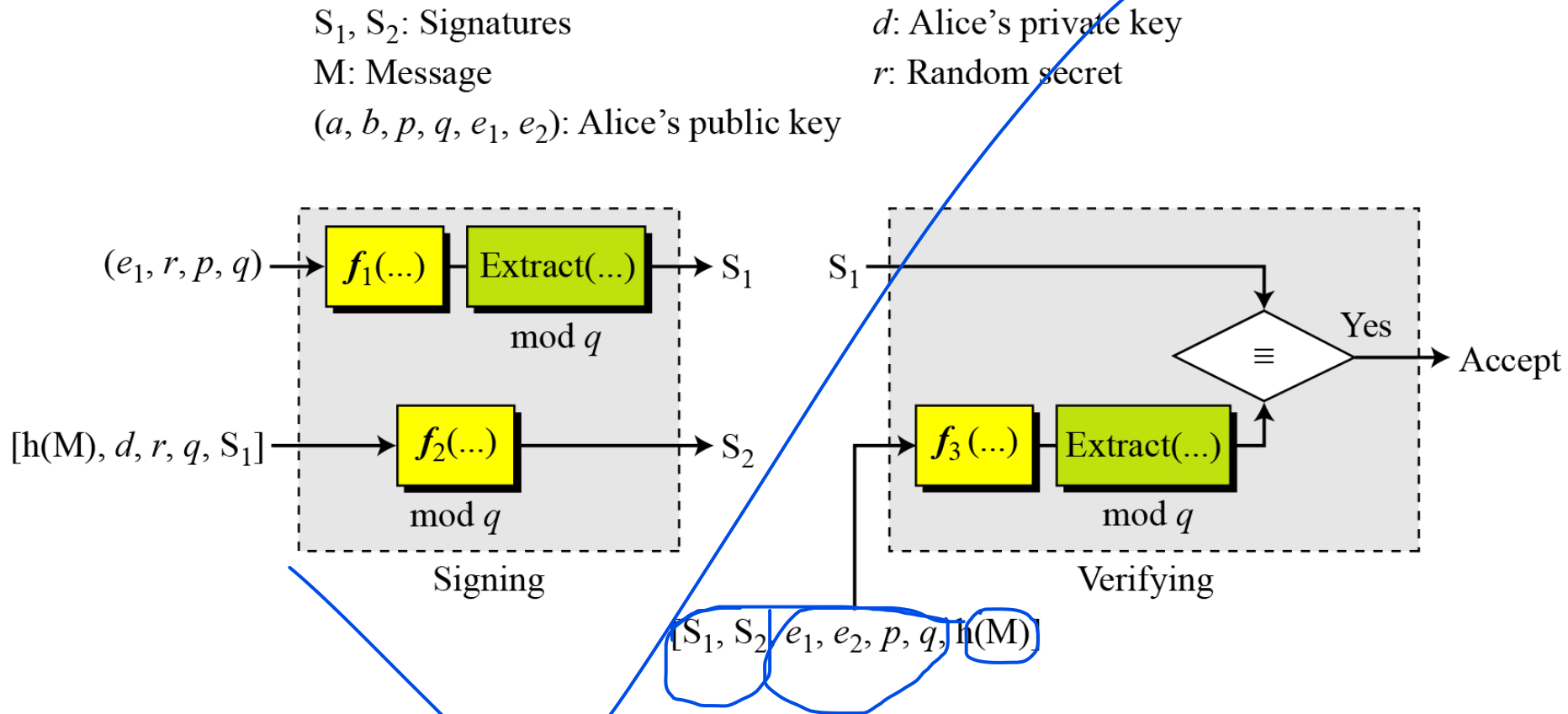
d : Alice's private key

V: Verification

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



Elliptic Curve Digital Signature Scheme



Elliptic Curve Digital Signature Scheme...

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, e_1, e_2) ; her private key is d .

Elliptic Curve Digital Signature Scheme...

M: Message

r : Random secret

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

S_1, S_2 : Signatures

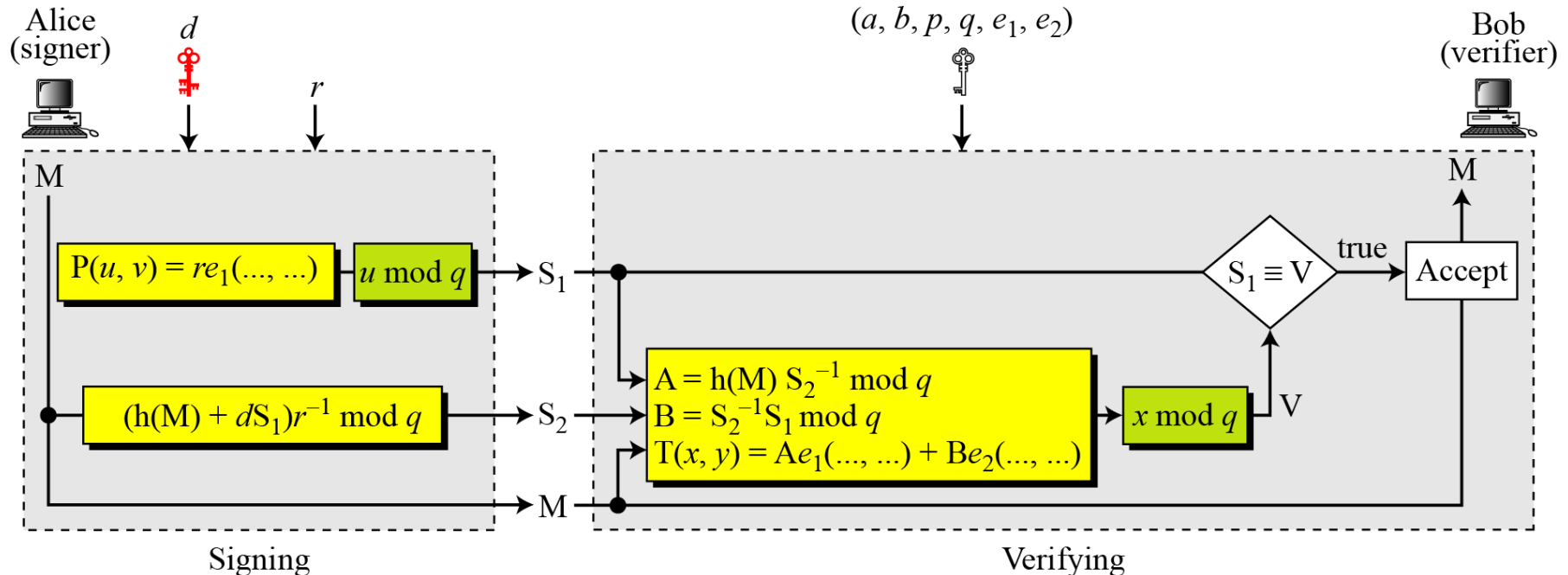
d : Alice's private key

$h(M)$: Message digest

V: Verification

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

A, B: Intermediate results



Variations

▶ Time Stamped Signatures

- ▶ 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.

▶ Blind Signatures

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