Digital Signature

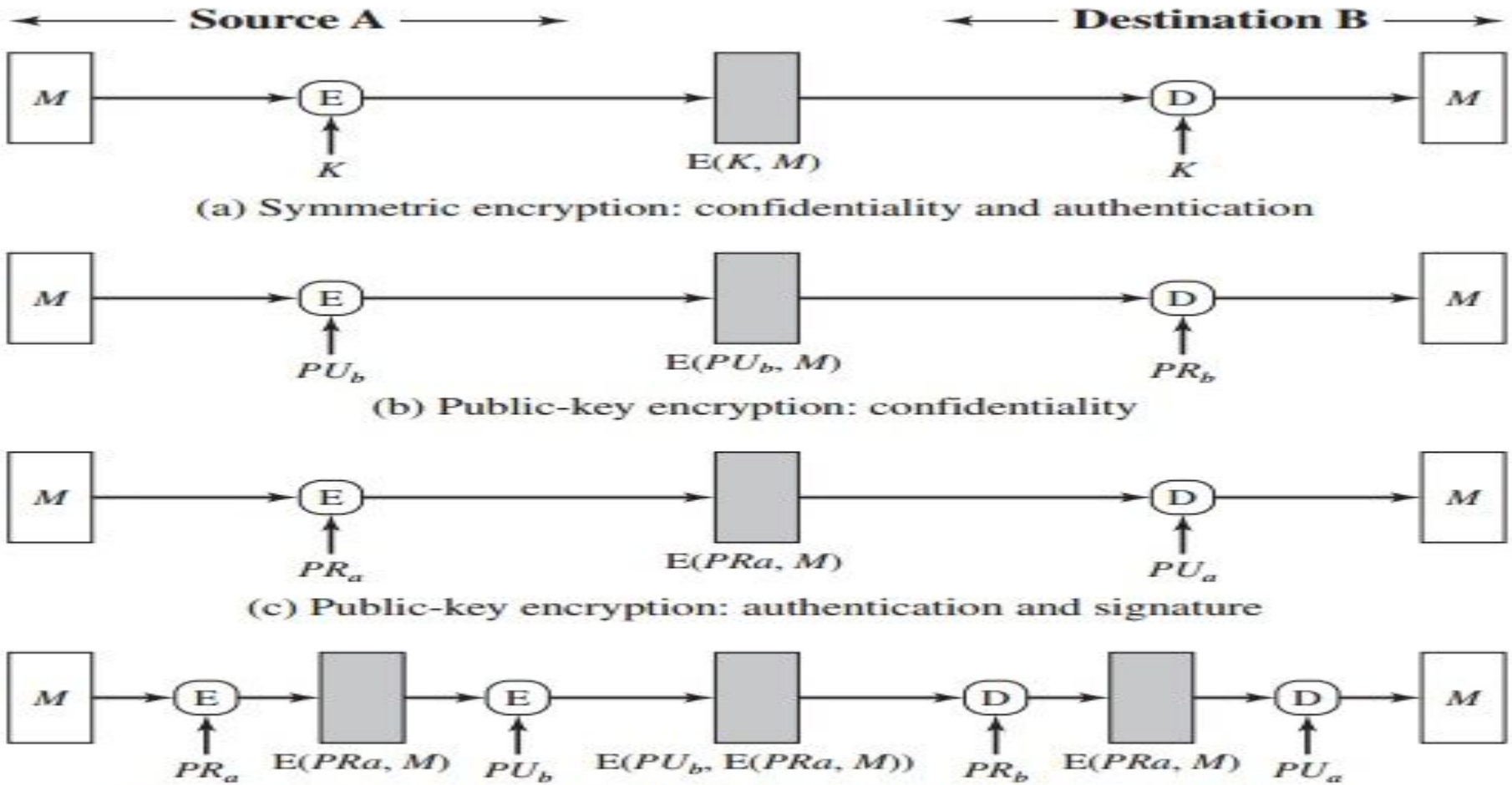


Figure 12.1 Basic Uses of Message Encryption

Issues related to authenticity

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.

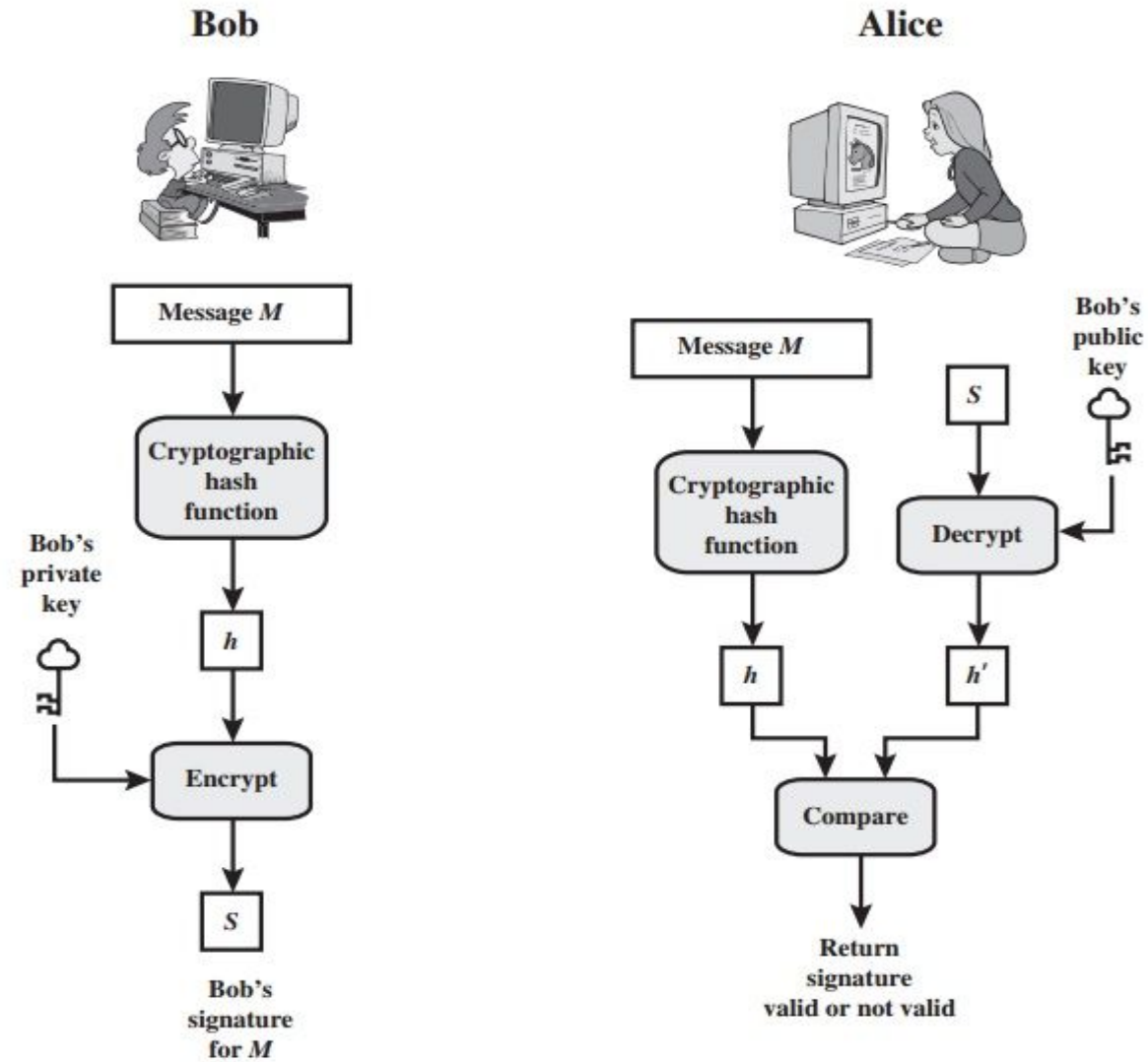
1. Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share.
2. John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

Both scenarios are of legitimate concern. Here is an example of the first sce- nario: 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.

Digital signature

Digital signatures provide the ability to:

- verify author, date & time of signature
- authenticate message contents
- be verified by third parties to resolve disputes
- hence include authentication function with additional capabilities

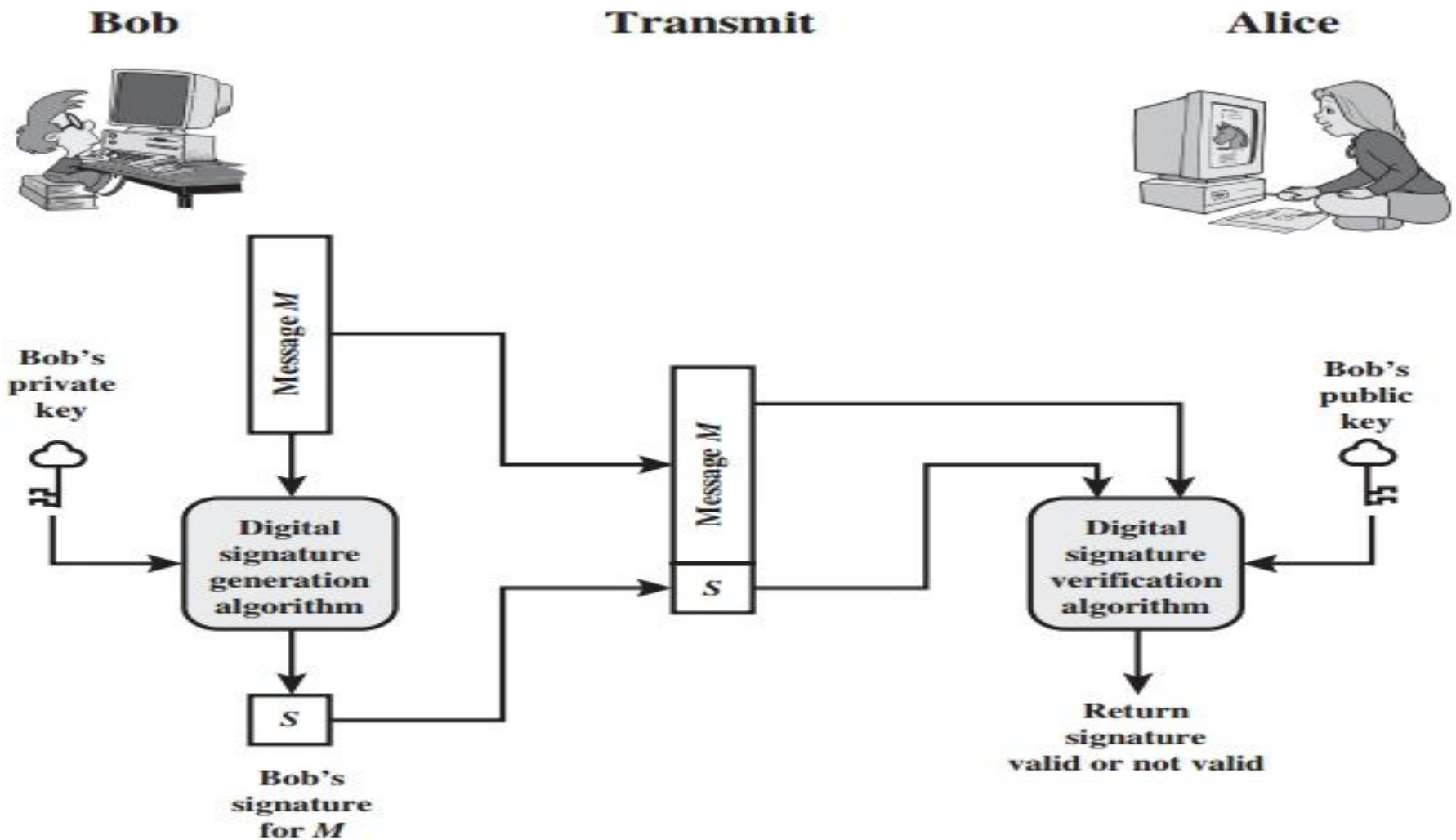

Bob
Alice
Message M
Cryptographic hash function
Bob's private key
h
Encrypt
S
Bob's signature for M
Message M
Cryptographic hash function
S
Bob's public key
Decrypt
h
h'
Compare
Return signature valid or not valid

why digital signature

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.

The digital signature must have the following properties:

- It must verify the author and the date and time of the signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.


Bob
Transmit
Alice
Message M
Bob's private key
Digital signature generation algorithm
S
Bob's signature for M
Message M
S
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid

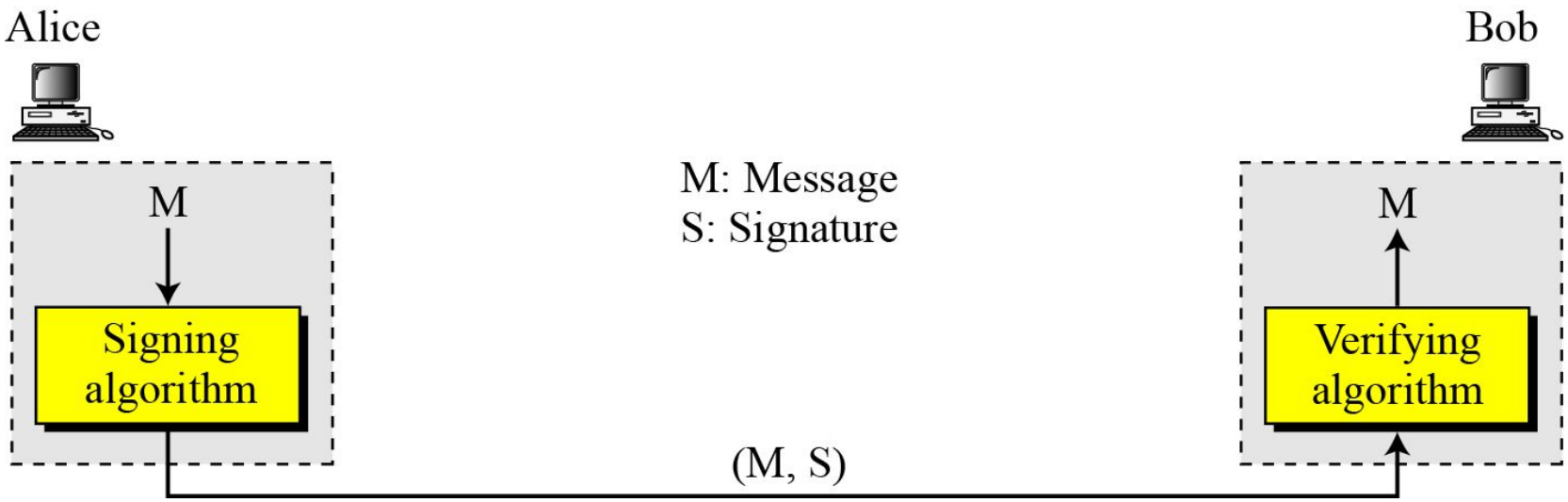
Introduction

- 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.
- 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.

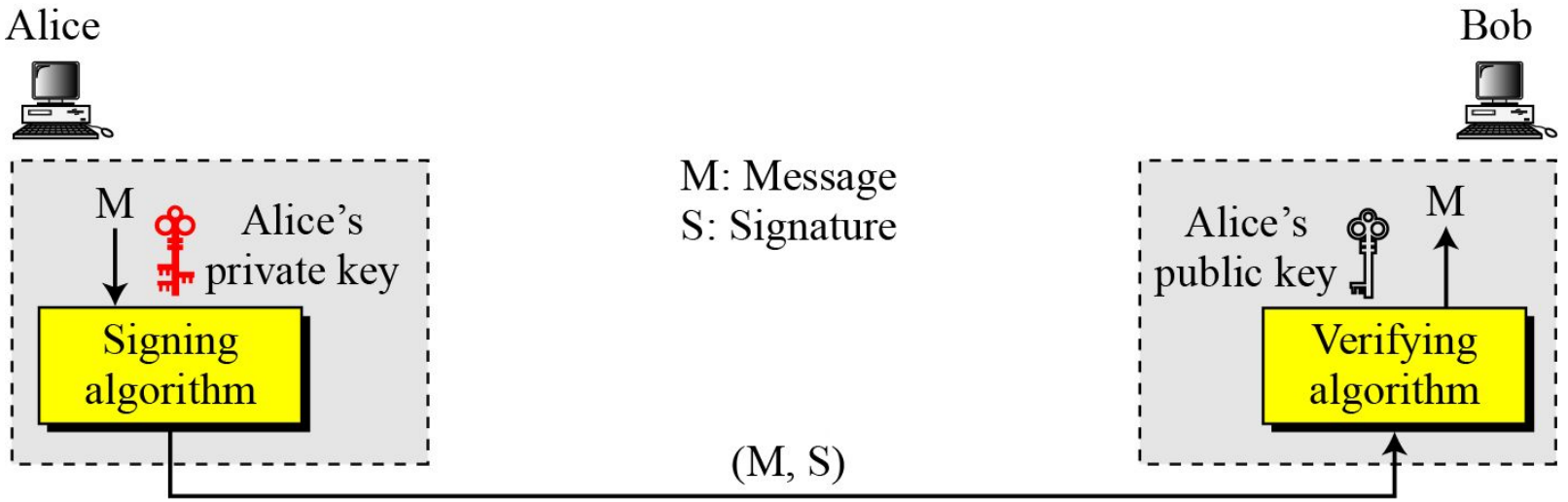
Conventional and digital signature difference

Characteristic	Conventional	Digital
Inclusion	Included in the document as part of the document.	Send the signature as a separate document.
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.
Relationship	Normally a *one-to-many* relationship between a signature and documents	*One-to-one* relationship between a signature and a message.
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

Digital Signature Process



Keys in the Digital Signature



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

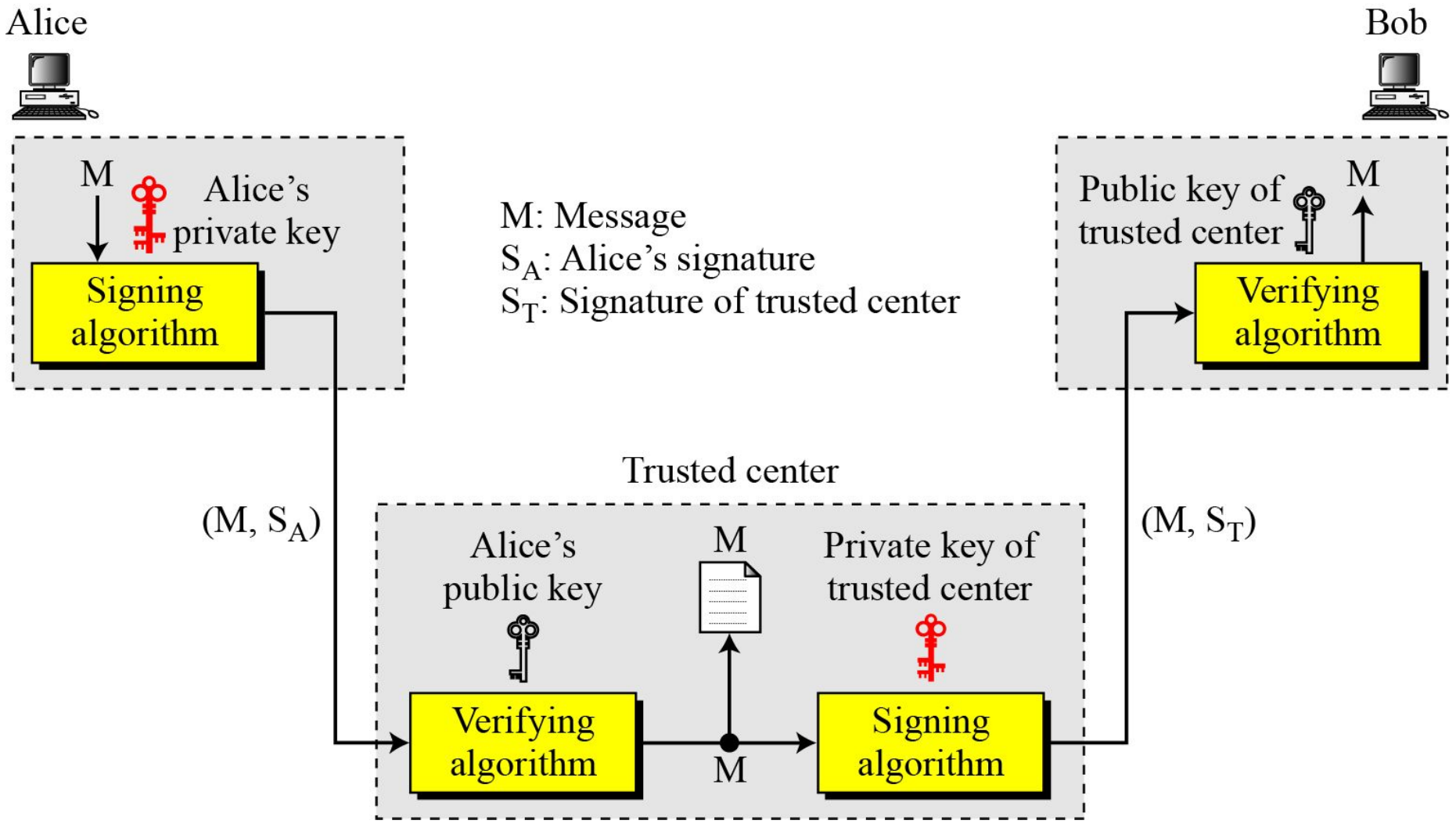
Digital Signature-Services

Services offered by Digital Signatures are

- Message Authentication
- Message Integrity
- Nonrepudiation
- Confidentiality

- A **digital signature** can directly provide the last three.
- For message *confidentiality* we still need encryption/ decryption.

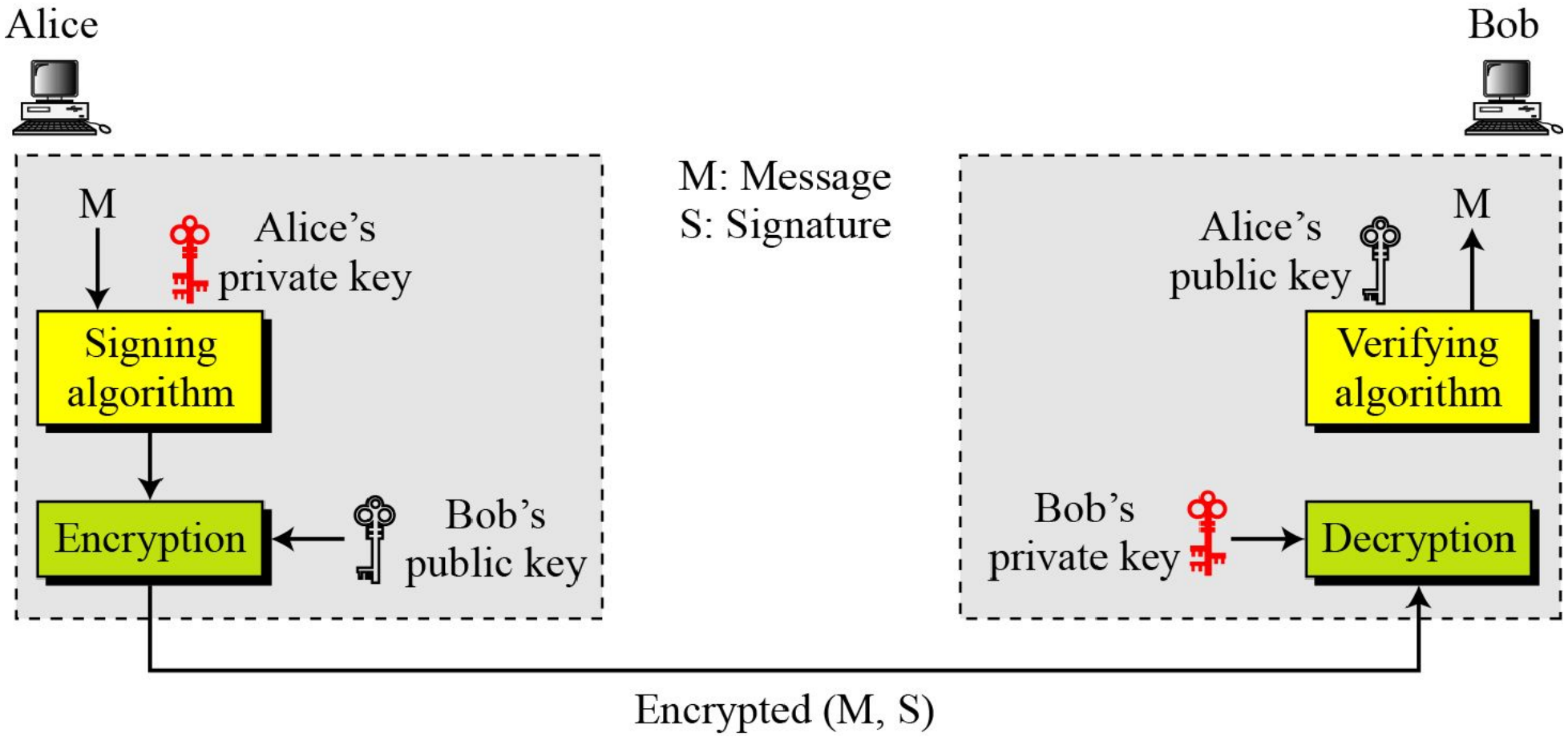
A trusted centre for non repudiation



Message Confidentiality

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

Message Confidentiality



Types of attack on cipher text

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Different types of attack on Digital Signature

- Key-only attack.
- Known-message attack.
- Chosen-message attack.

types of attacks

Key-only attack: C only knows A's public key.

Known message attack: C is given access to a set of messages and their signatures.

Generic chosen message attack: C chooses a list of messages before attempt- ing to breaks A's signature scheme, independent of A's public key. C then obtains from A valid signatures for the chosen messages. The attack is generic, because it does not depend on A's public key; the same attack is used against everyone.

Directed chosen message attack: Similar to the generic attack, except that the list of messages to be signed is chosen after C knows A's public key but before any signatures are seen.

Adaptive chosen message attack: C is allowed to use A as an "oracle." This means the A may request signatures of messages that depend on previously obtained message–signature pairs.

Existential attack

the middle person tries to send a random message with a valid signature

For eg.

I want to update my ubuntu so i contact the ubuntu server. this signature is well known and hence any person can take that signature and attach a random message

when it reaches me i down it as a valid file but it may corrupt the system

Schemes for digital signature

- RSA digital signature scheme.
- ElGamal digital signature scheme.
- Schnorr digital signature scheme.
- Digital Signature Standard (DSS).
- Elliptic Curve digital signature scheme.

Digital Signature Scheme

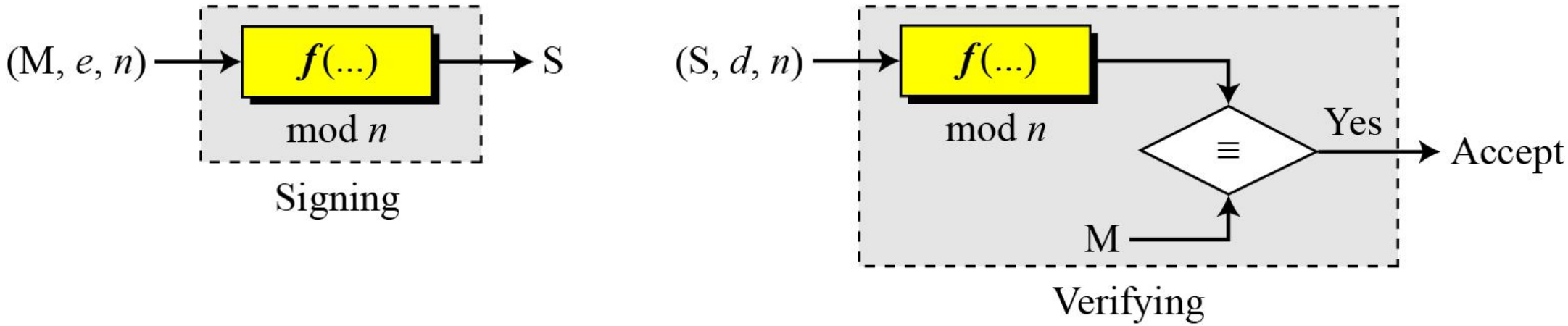
The signing and verifying sites use the same function, but with different parameters.

The verifier compares the message and the output of the function for congruence; If the result is true, the message accepted.

Digital Signature Scheme

M: Message
S: Signature

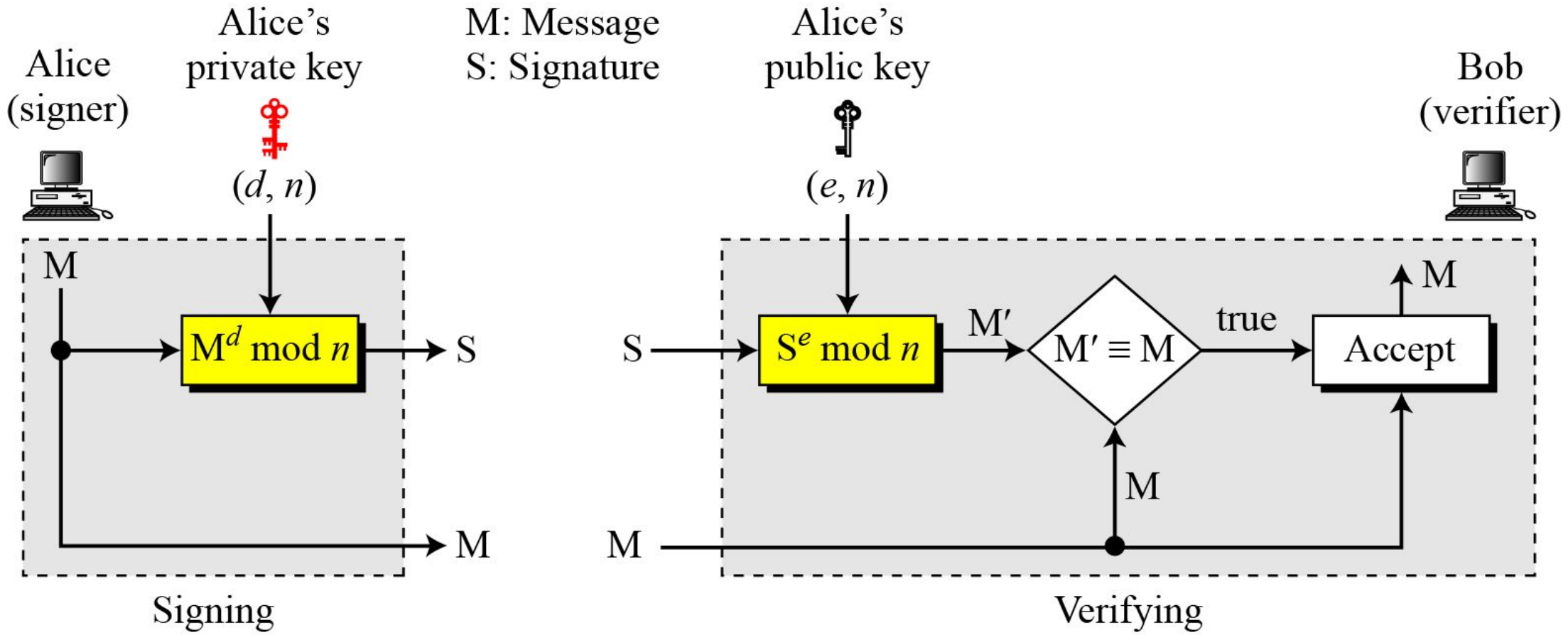
(e, n): Alice's public key
d: Alice's private key



Key generation

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

signing and verifying



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

- The value of φ(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:

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

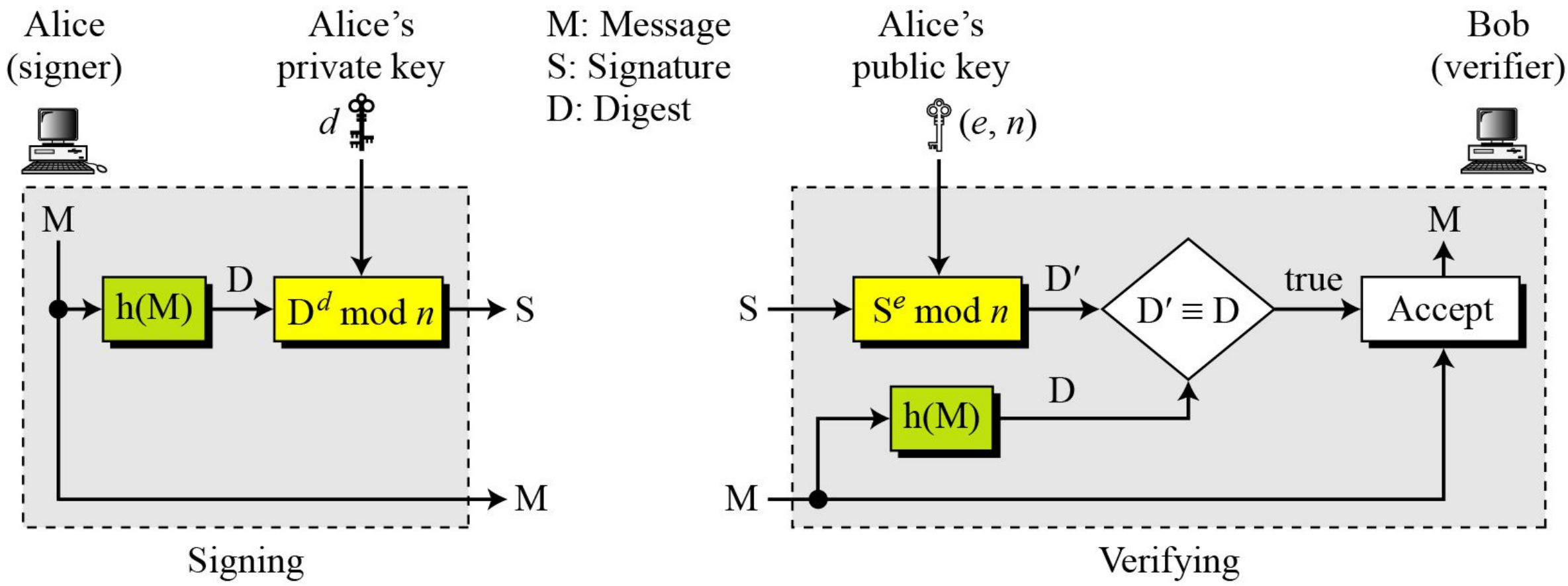
Alice sends the message and the signature to Bob.

- 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 message digest



Schemes for digital signature

- The Direct Digital Signature
  - There are only two parties involved in the passing of the signed information: the sender and the receiver.
  - Direct digital signatures only require these two entities because the receiver of the data (digital signature) knows the public key used by the sender. And the sender of the signature trusts the receiver not to alter the document in any way.
- The Arbitrated Digital Signature
  - Implementing an arbitrated digital signature invites a third party into the process called a "trusted arbiter."
  - The role of the trusted arbiter is usually twofold:
    - third party verifies the integrity of the signed message or data
    - The trusted arbiter dates, or time-stamps, the document, verifying receipt and the passing on of the signed document to its intended final destination.