CRYPTOGRAPHY
and
NETWORK SECURITY

PEC-CS801B, UNIT 2

By
CHINMOY GHOSH
Assntt. Professor,
Deptt. Of CSE, JGEC

Introduction

- Security is about how to prevent attacks, or -- if prevention is not possible -- how to detect attacks and recover from them

- An attack is a *deliberate attempt* to compromise a system; it usually exploits weaknesses in the system's design, implementation, operation, or management

- attacks can be
  - passive
    - attempts to learn or make use of information from the system but does not affect system resources
    - examples: eavesdropping message contents, traffic analysis
    - difficult to detect, should be prevented
  - active
    - attempts to alter system resources or affect their operation
    - examples: masquerade (spoofing), replay, modification (substitution, insertion, destruction), denial of service
    - difficult to prevent, should be detected

Cryptography

Cryptography is the art and science of achieving security by encoding message to make them non-readable.

Cryptography issues:

1. Confidentiality: only sender, intended receiver should "understand" message contents
   - sender encrypts message
   - receiver decrypts message
2. End-Point Authentication: sender, receiver want to confirm identity of each other
3. Message Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Basic Terminologies

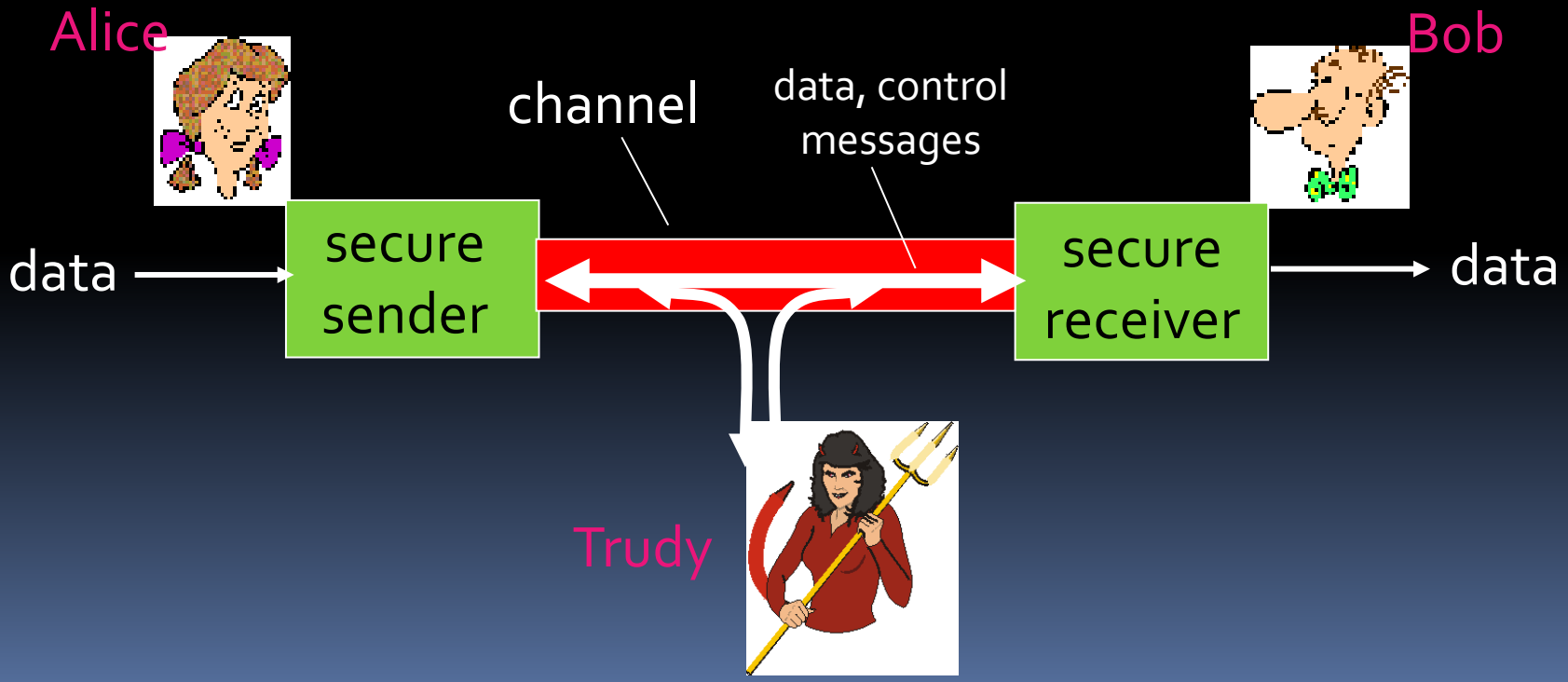
- Cryptography deals with creating documents that can be shared secretly over public communication channels
- Cryptographic documents are decrypted with the key associated with encryption, with the knowledge of the encryptor.
- The word cryptography comes from the Greek words: Krypto (secret) and graphein (write).
- Cryptanalysis deals with finding the encryption key without the knowledge of the encryptor.

Basic Terminologies

- Keys are rules used in algorithms to convert a document into a secret document
- Keys are of two types:
  - Symmetric
  - Asymmetric
- A key is symmetric if the same key is used both for encryption and decryption
- A key is asymmetric if different keys are used for encryption and decryption
- Plaintext is text that is in readable form
- Ciphertext results from plaintext by applying the encryption key

Friends and enemies: Alice, Bob, Trudy

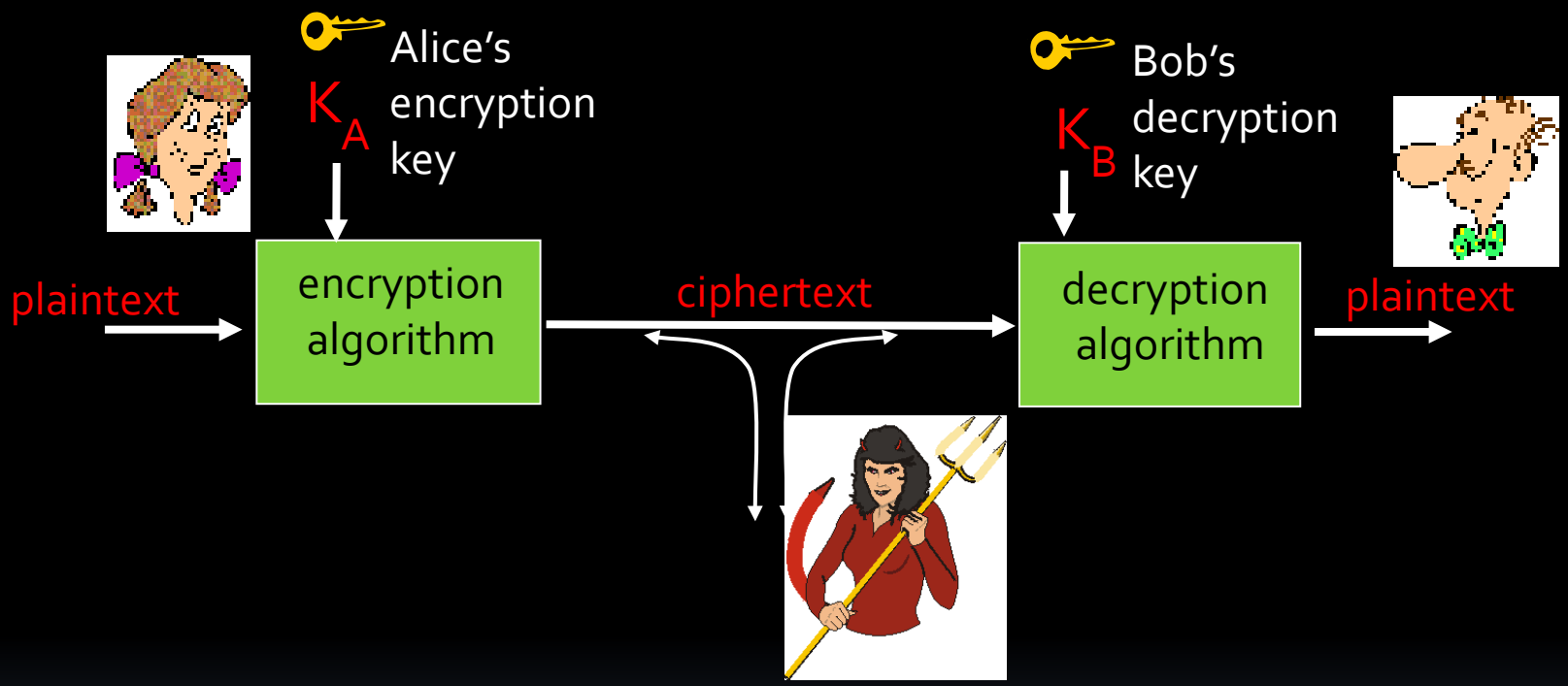
- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

- … well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates

The language of cryptography

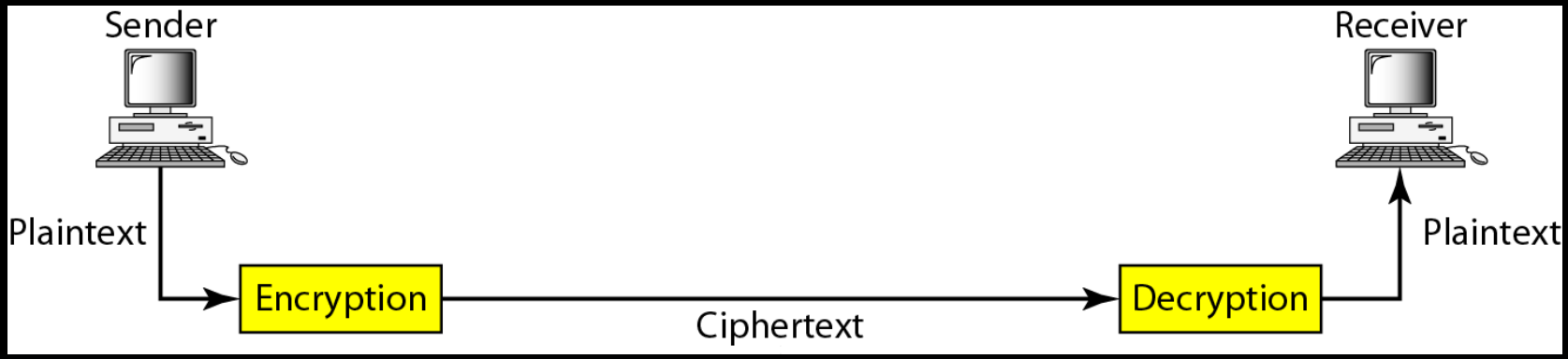


m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Cryptography components



Categories of cryptography

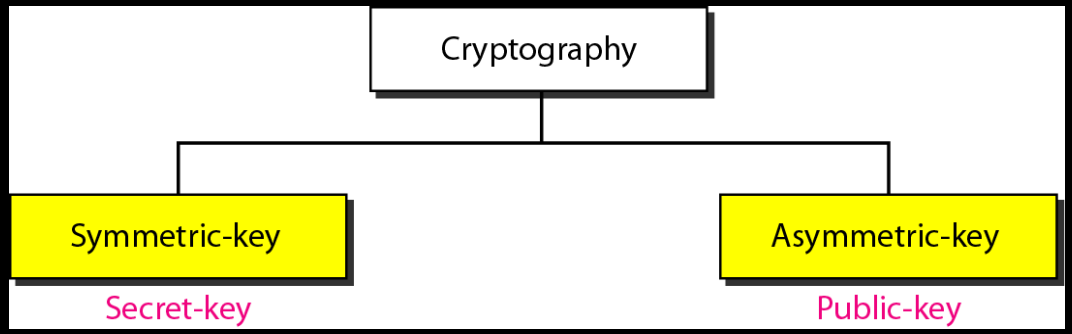
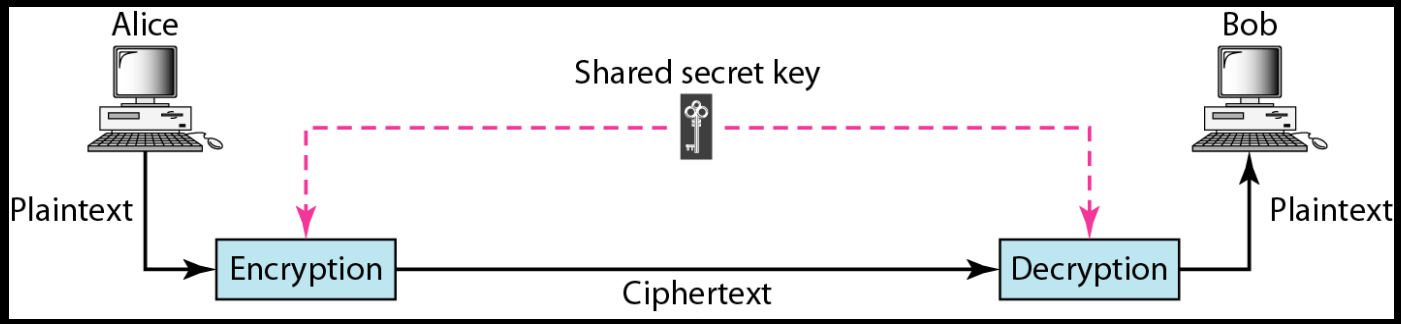


Figure 30.3 *Symmetric-key cryptography*



In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Figure 30.4 *Asymmetric-key cryptography*

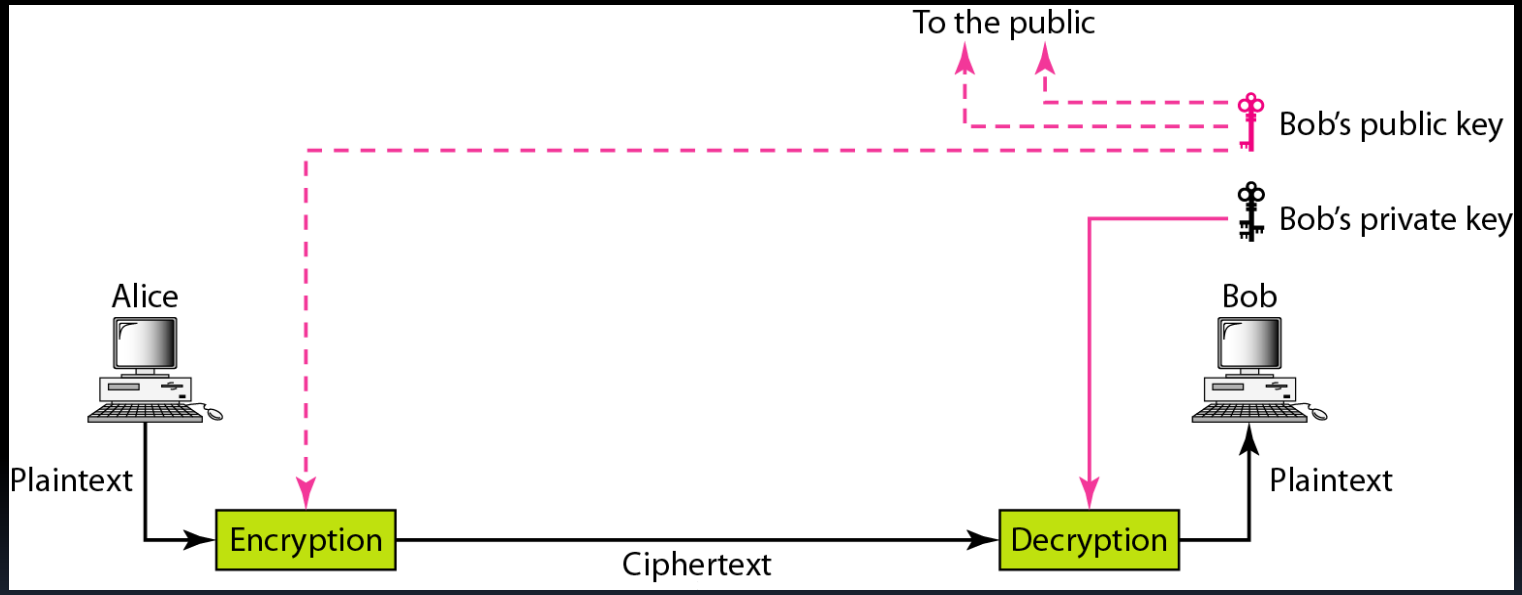


Figure 30.5 *Keys used in cryptography*

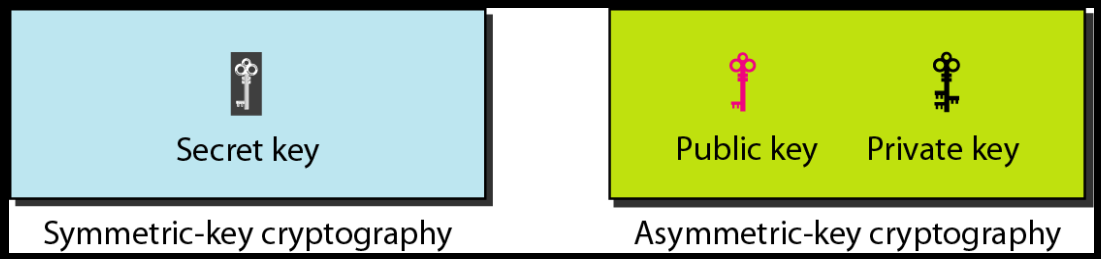
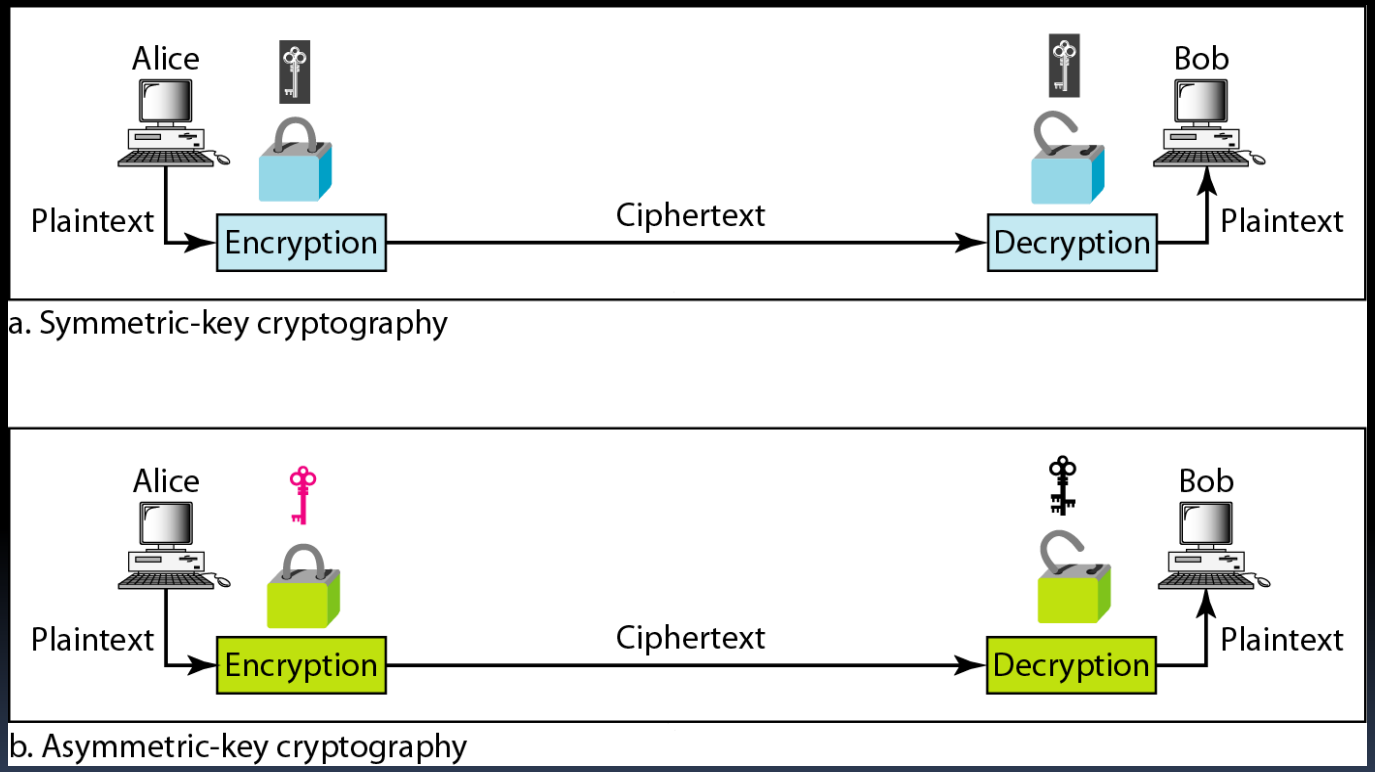


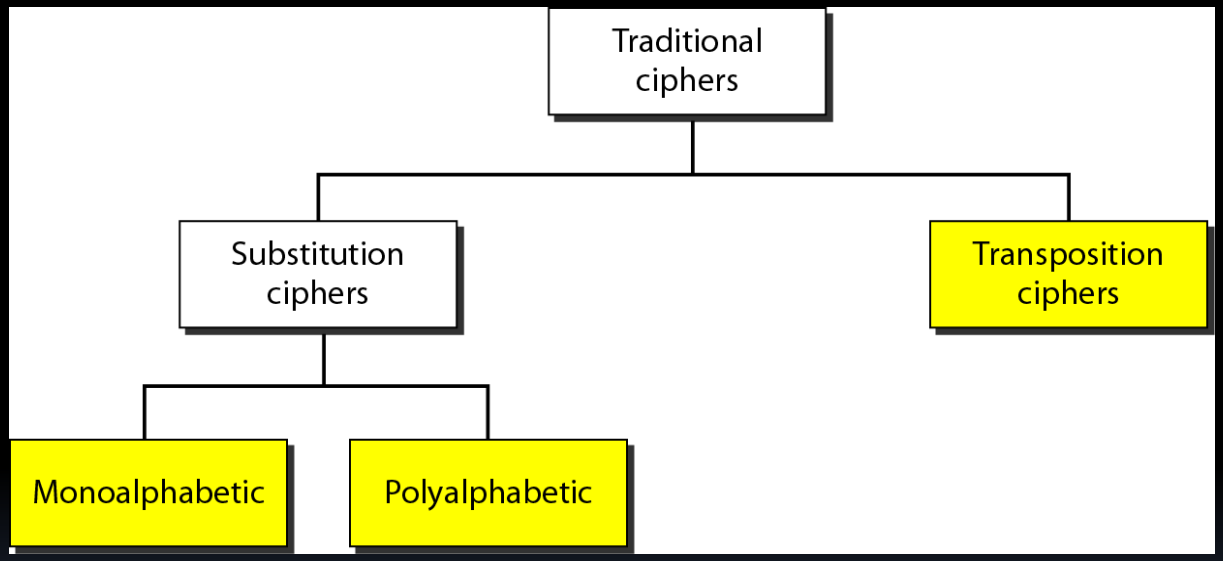
Figure 30.6 *Comparison between two categories of cryptography*



SYMMETRIC-KEY CRYPTOGRAPHY

- Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.
- There are two ways in which a plain text message can be codified to obtain the corresponding cipher text:
  - Substitution
  - Transposition

Figure 30.7 *Traditional ciphers*



Substitution Cipher

- A substitution cipher replaces one symbol with another.
  - Mono-alphabetic (Caesar Cipher)
  - Homophonic
  - Polygram
  - * Playfair Cipher

Polygram substitution technique replaces one block of plain text with a block of cipher text, it does not work on a character-by-character basis.

Example 30.1

The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: KHOOR

Solution

The cipher is probably monoalphabetic because both occurrences of L's are encrypted as O's.

Example 30.2

The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: ABNZF

Solution

The cipher is not monoalphabetic because each occurrence of L is encrypted by a different character. The first L is encrypted as N; the second as Z.

Example 30.3

Use the shift cipher with key = 15 to encrypt the message "HELLO."

Solution

We encrypt one character at a time. Each character is shifted 15 characters down. Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And O is encrypted to D. The cipher text is WTAAD.

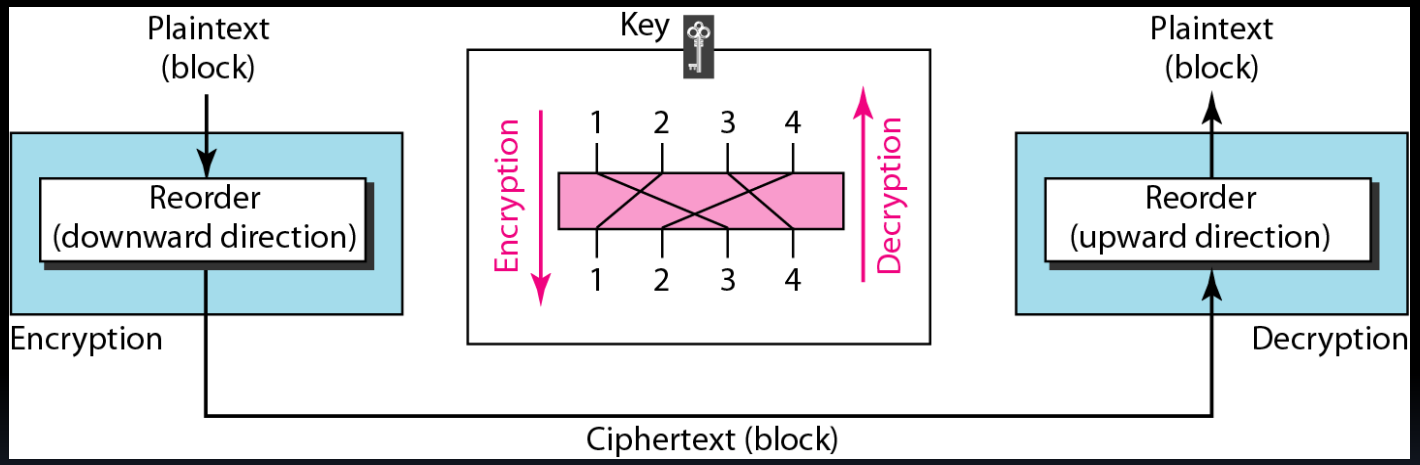
Example 30.4

Use the shift cipher with key = 15 to decrypt the message "WTAAD."

Solution

We decrypt one character at a time. Each character is shifted 15 characters up. Letter W is decrypted to H. Letter T is decrypted to E. The first A is decrypted to L. The second A is decrypted to L. And, finally, D is decrypted to O. The plaintext is HELLO.

Figure 30.8 *Transposition cipher*



Transposition Cipher

- In transposition Cipher, there is no substitution of character; instead their location change.
  - Rail Fence Techniques.
  - Simple Columnar transposition Technique.
  - Vernum Cipher (One time pad) .

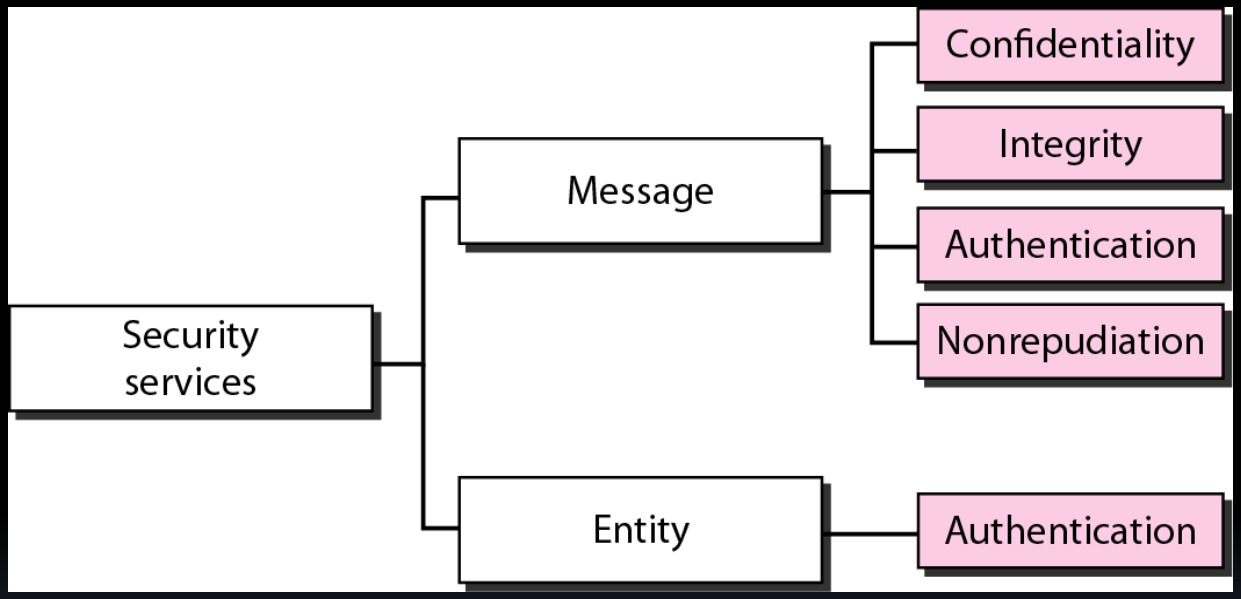
31-1 SECURITY SERVICES

Network security can provide five services. Four of these services are related to the message exchanged using the network. The fifth service provides entity authentication or identification.

Topics discussed in this section:

Message Confidentiality
Message Integrity
Message Authentication
Message Nonrepudiation
Entity Authentication

Figure 31.1 *Security services related to the message or entity*



31-2 MESSAGE CONFIDENTIALITY

The concept of how to achieve message confidentiality or privacy has not changed for thousands of years. The message must be encrypted at the sender site and decrypted at the receiver site. This can be done using either symmetric-key cryptography or asymmetric-key cryptography.

Topics discussed in this section:

Confidentiality with Symmetric-Key Cryptography
Confidentiality with Asymmetric-Key Cryptography

31-3 MESSAGE INTEGRITY

Encryption and decryption provide secrecy, or confidentiality, but not integrity. However, on occasion we may not even need secrecy, but instead must have integrity.

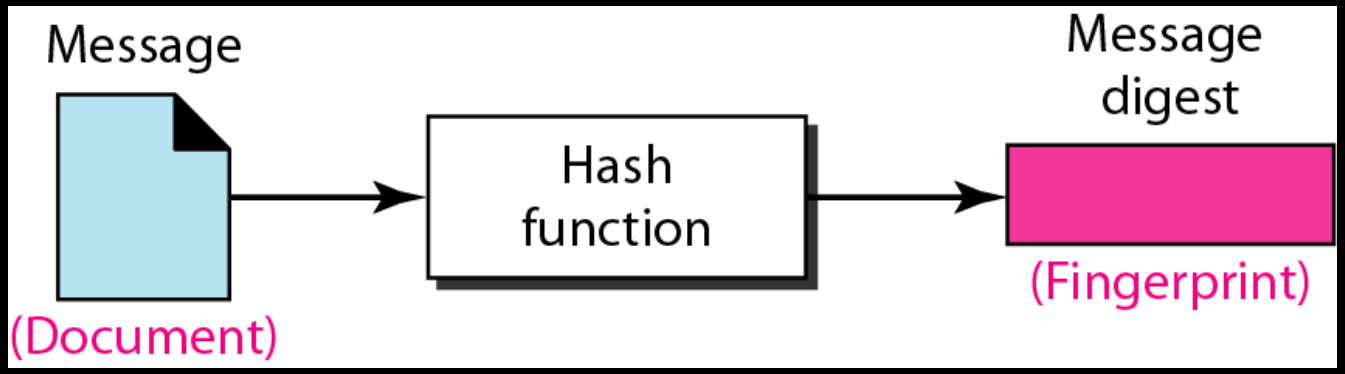
Topics discussed in this section:

Document and Fingerprint
Message and Message Digest
Creating and Checking the Digest
Hash Function Criteria
Hash Algorithms: SHA-1

Note

To preserve the integrity of a document, both the document and the fingerprint are needed.

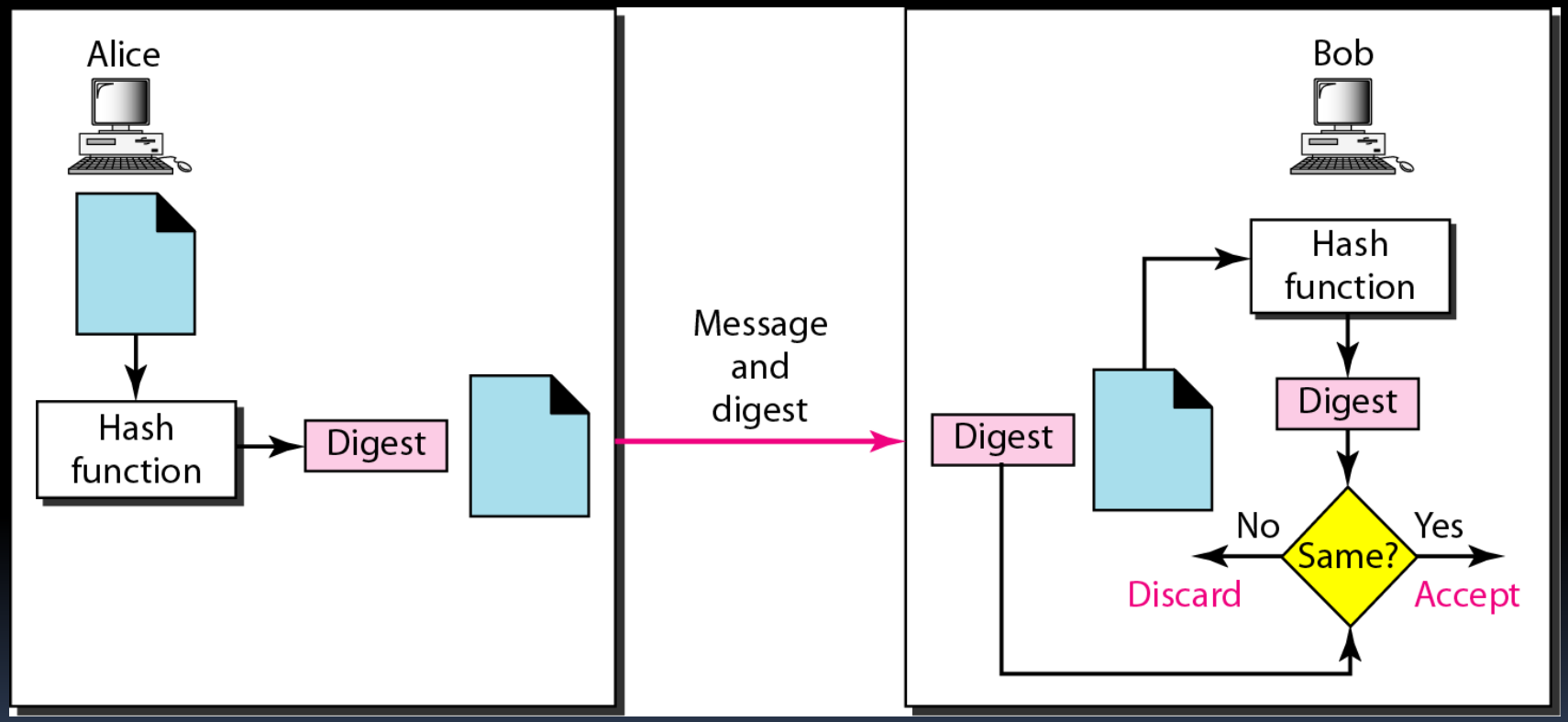
Figure 31.4 *Message and message digest*



Note

The message digest needs to be kept secret.

Figure 31.5 *Checking integrity*



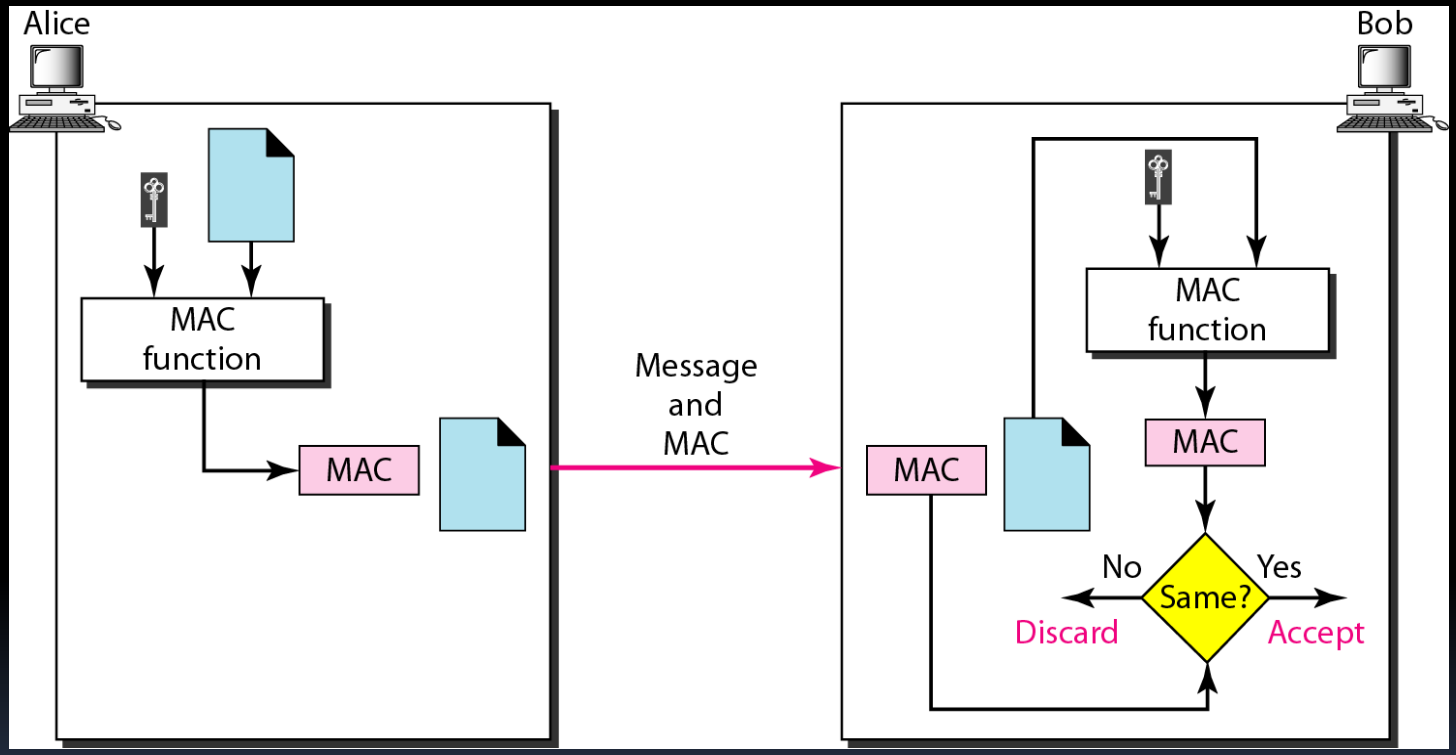
31-4 MESSAGE AUTHENTICATION

A hash function cannot provide authentication. The digest created by a hash function can detect any modification in the message, but not authentication.

Topics discussed in this section:

MAC (Message authentication code)

Figure 31.9 *MAC, created by Alice and checked by Bob*



31-5 DIGITAL SIGNATURE

When Alice sends a message to Bob, Bob needs to check the authenticity of the sender; he needs to be sure that the message comes from Alice and not Eve. Bob can ask Alice to sign the message electronically. In other words, an electronic signature can prove the authenticity of Alice as the sender of the message. We refer to this type of signature as a digital signature.

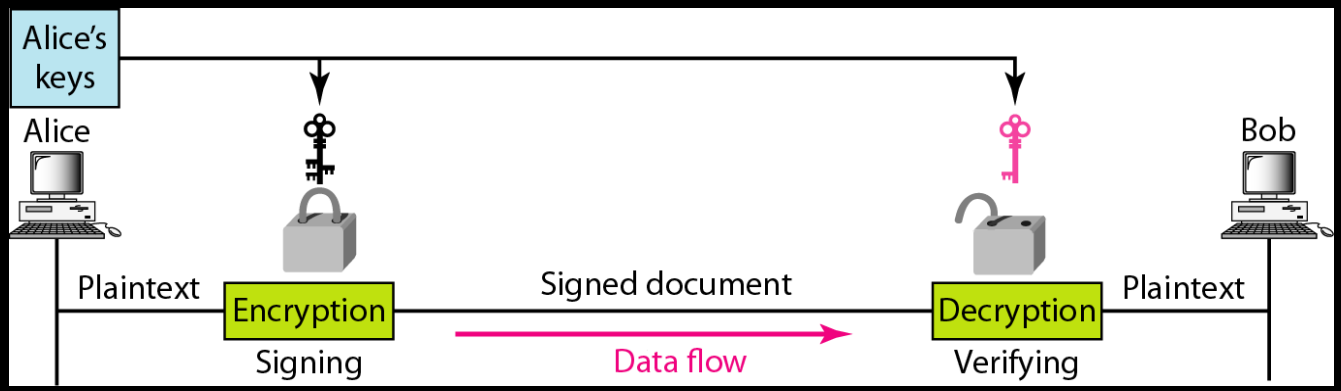
Topics discussed in this section:

Comparison
Need for Keys
Process

Note

A digital signature needs a public-key system.

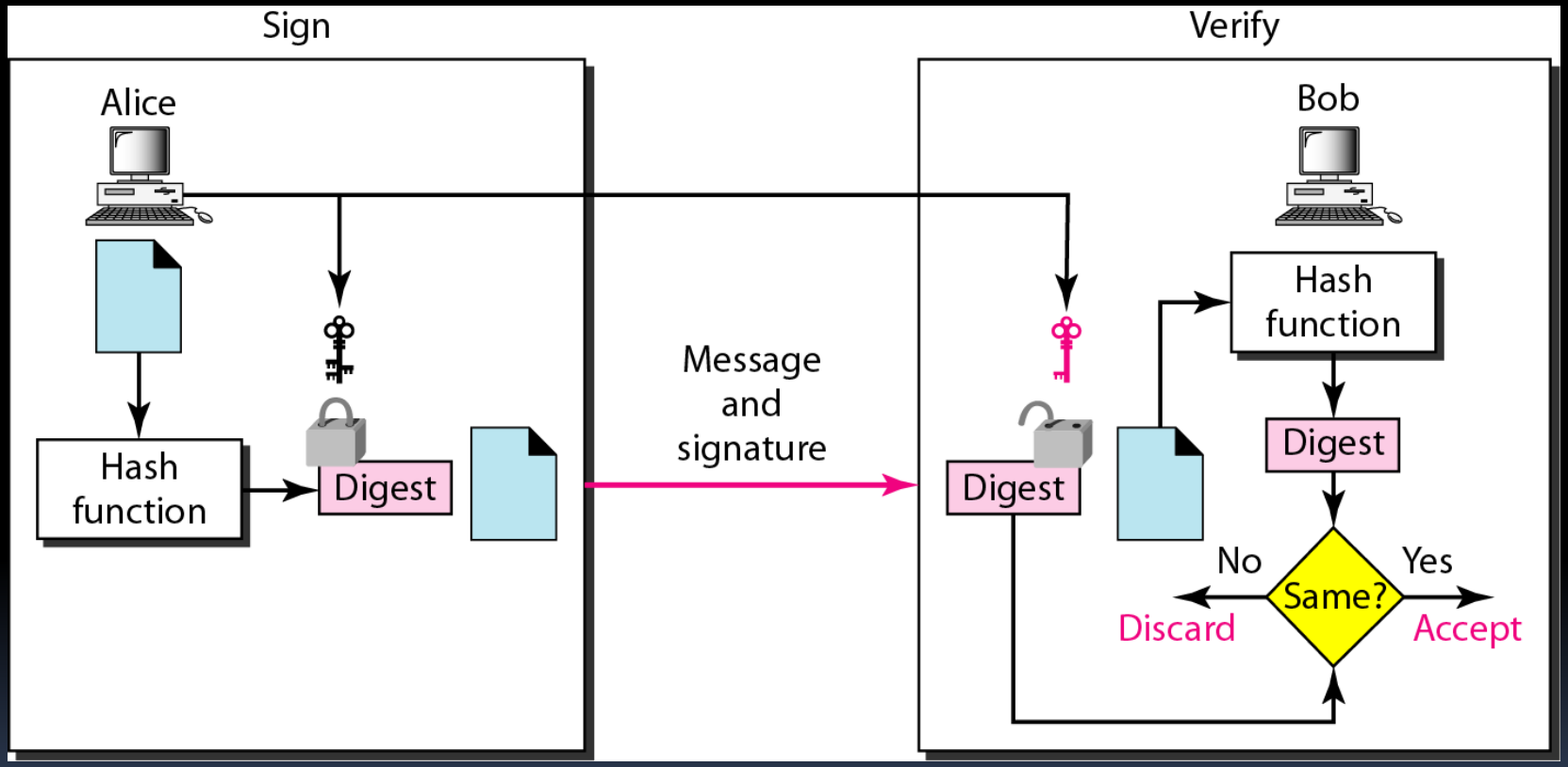
Figure 31.11 *Signing the message itself in digital signature*



Note

In a cryptosystem, we use the private and public keys of the receiver;
in digital signature, we use the private and public keys of the sender.

Figure 31.12 *Signing the digest in a digital signature*



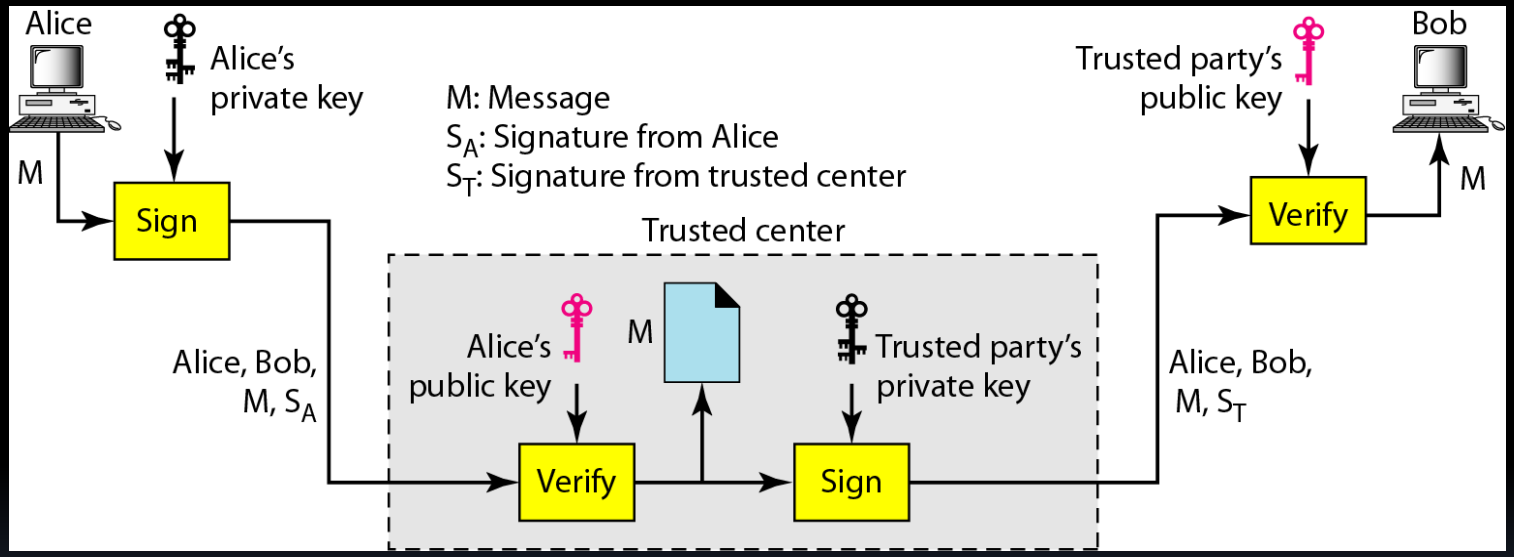
Note

A digital signature today provides message integrity.

Note

Digital signature provides message authentication.

Figure 31.13 *Using a trusted center for nonrepudiation*



Note

Nonrepudiation can be provided using a trusted party.

31-6 ENTITY AUTHENTICATION

Entity authentication is a technique designed to let one party prove the identity of another party. An entity can be a person, a process, a client, or a server. The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier.

Topics discussed in this section:

Passwords