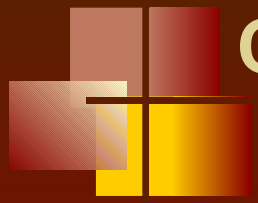
# Cryptography and Network Security

## Chapter 1

## Introduction

**Vijay Katta**



# Chapter 1

## Objectives

- To define three security goals
- To define security attacks that threaten security goals
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To introduce two techniques, cryptography and steganography, to implement security mechanisms.

# Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

# 1-1 SECURITY GOALS

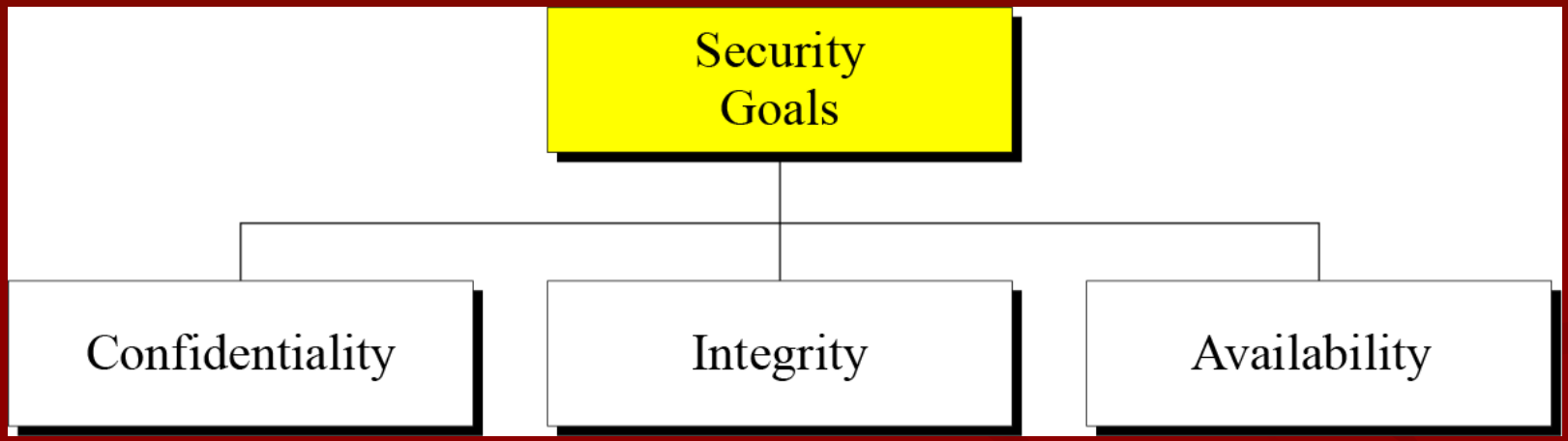
*This section defines three security goals.*

***Topics discussed in this section:***

**1.1.1 Confidentiality**
**1.1.2 Integrity**
**1.1.3 Security**

# 1.1 Continued

**Figure 1.1** *Taxonomy of security goals*



# 1.1.1 Confidentiality

*Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.*

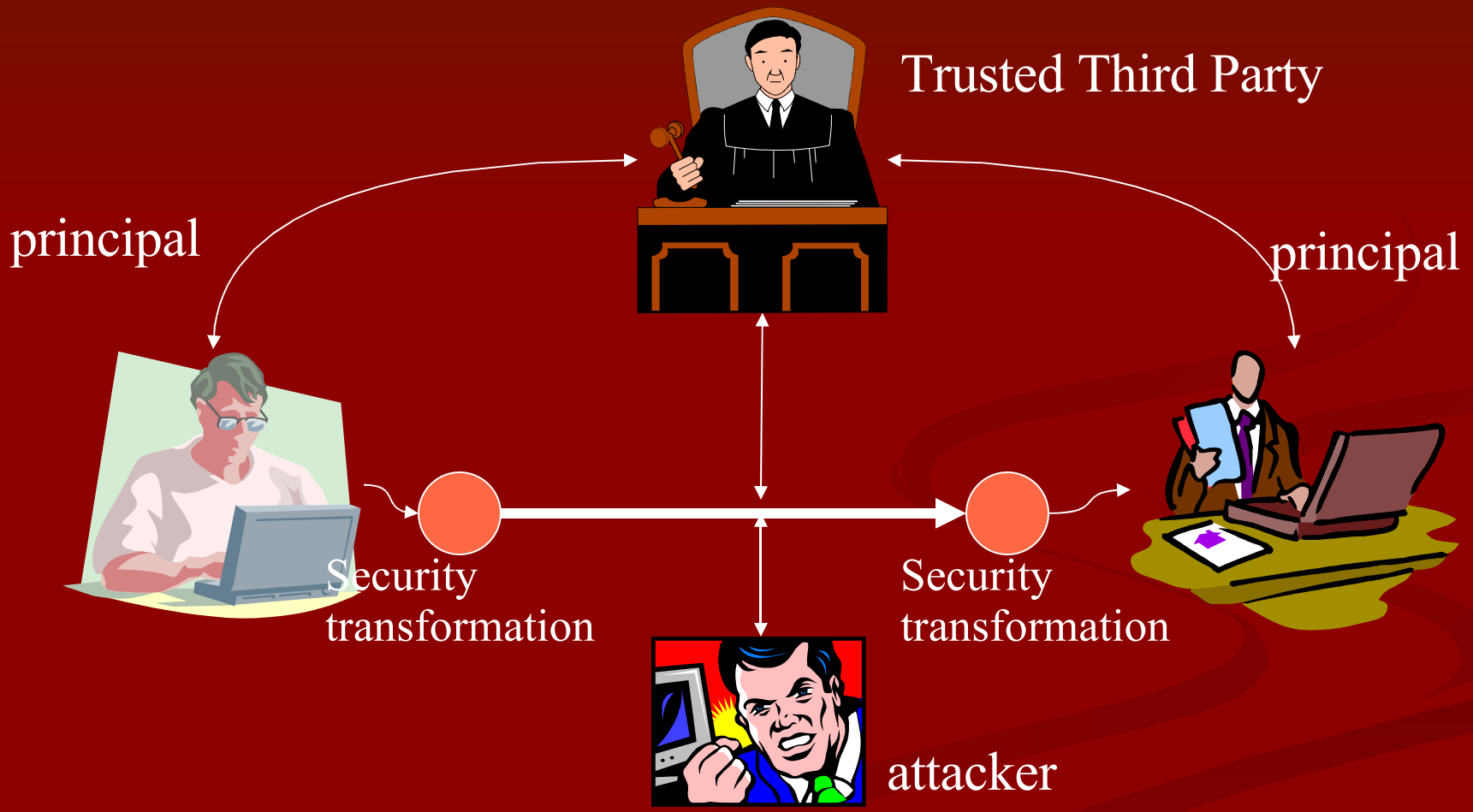
# *1.1.2 Integrity*

***Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.***

# 1.1.3 Availability

***The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.***

# Network Security Model



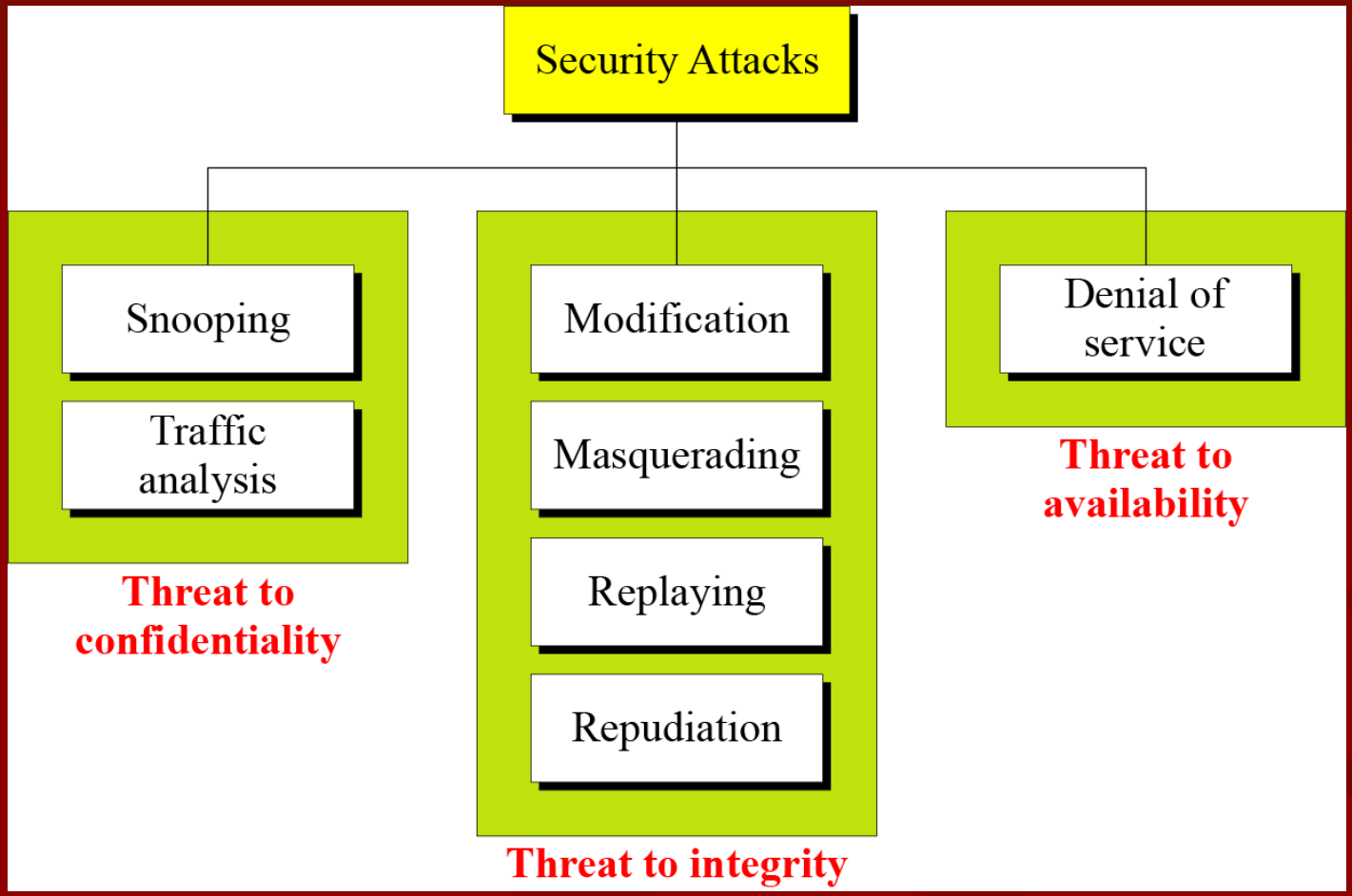
# 1-2 ATTACKS

*The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.*

***Topics discussed in this section:***

**1.2.1 Attacks Threatening Confidentiality**
**1.2.2 Attacks Threatening Integrity**
**1.2.3 Attacks Threatening Availability**
**1.2.4 Passive versus Active Attacks**

**Figure 1.2** *Taxonomy of attacks with relation to security goals*



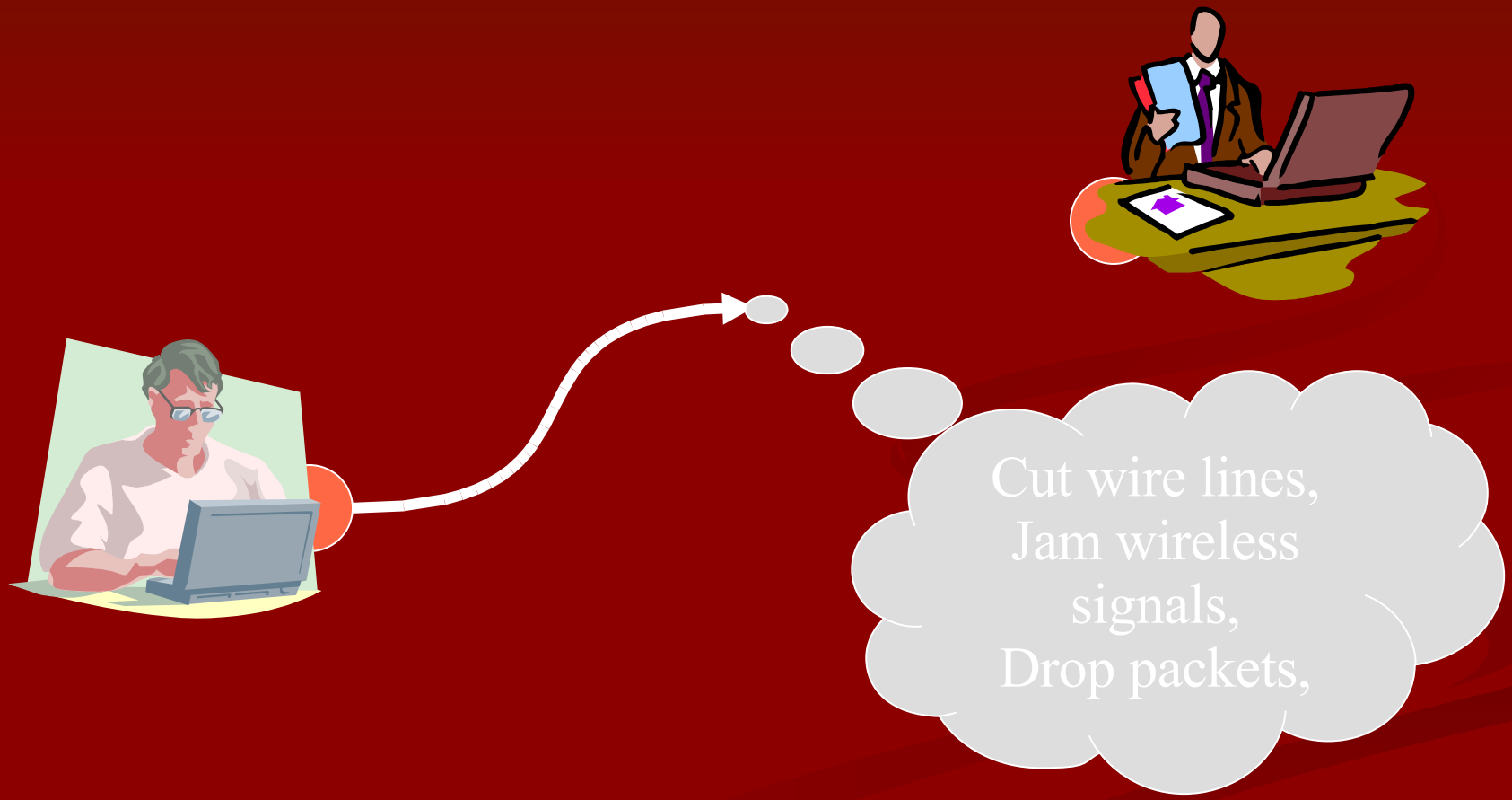
# 1.2.1 Attacks Threatening Confidentiality

***Snooping*** *refers to unauthorized access to or interception of data.*

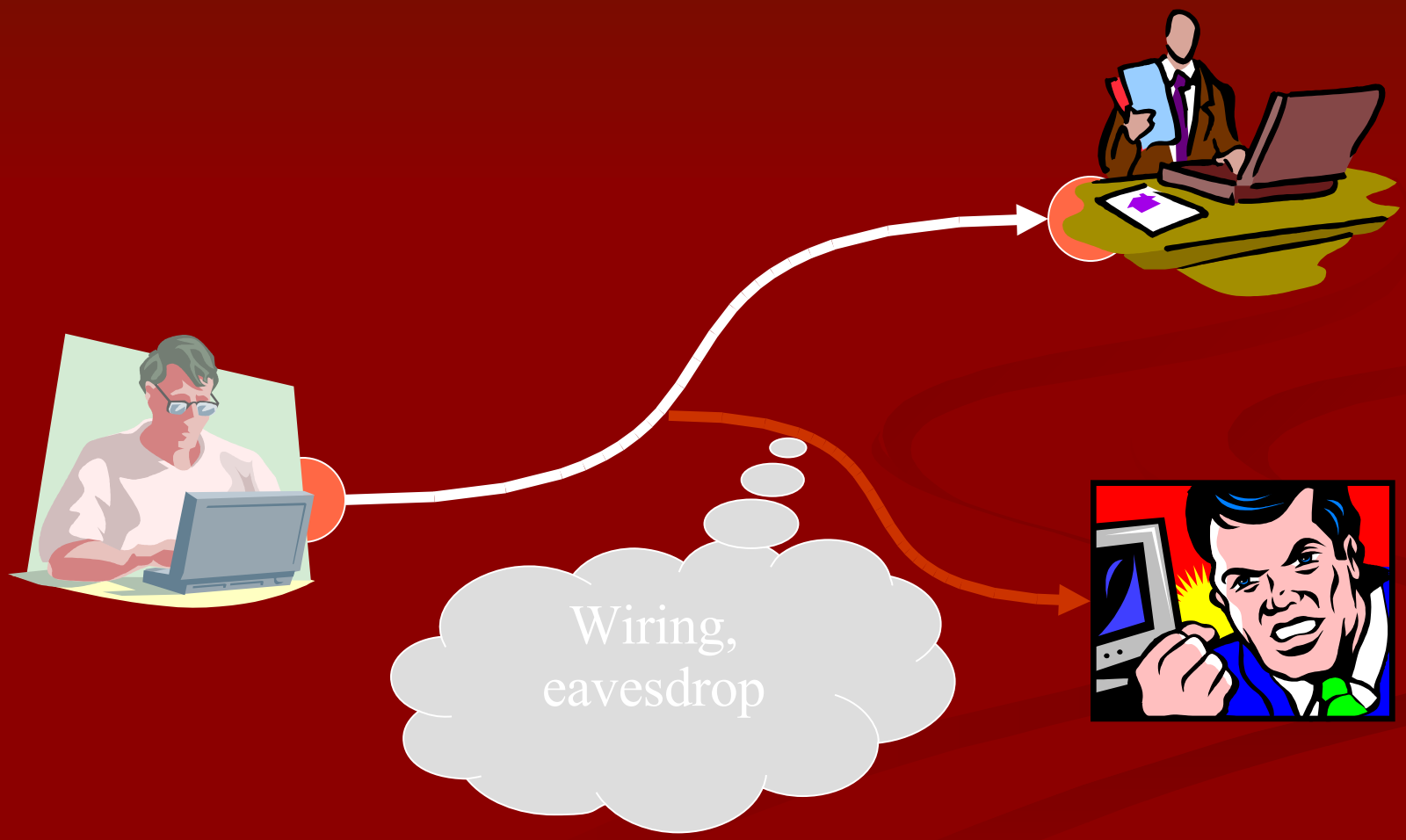
***Traffic analysis*** *refers to obtaining some other type of information by monitoring online traffic.*

# Information Transferring

# Attack: Interruption



# Attack: Interception



# 1.2.2 Attacks Threatening Integrity

***Modification*** *means that the attacker intercepts the message and changes it.*

***Masquerading*** *or* ***spoofing*** *happens when the attacker impersonates somebody else.*

***Replaying*** *means the attacker obtains a copy of a message sent by a user and later tries to replay it.*

***Repudiation*** *means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.*

# Attack: Modification

intercept

Replaced info

# Attack: Fabrication

Also called impersonation

# 1.2.3 Attacks Threatening Availability

***Denial of service*** ***(DoS) is a very common attack. It may slow down or totally interrupt the service of a system.***

# 1.2.4 Passive Versus Active Attacks

**Table 1.1** *Categorization of passive and active attacks*

| *Attacks* | *Passive/Active* | *Threatening* |
|---|---|---|
| Snooping<br>Traffic analysis | Passive | Confidentiality |
| Modification<br>Masquerading<br>Replaying<br>Repudiation | Active | Integrity |
| Denial of service | Active | Availability |

# 1-3 SERVICES AND MECHANISMS

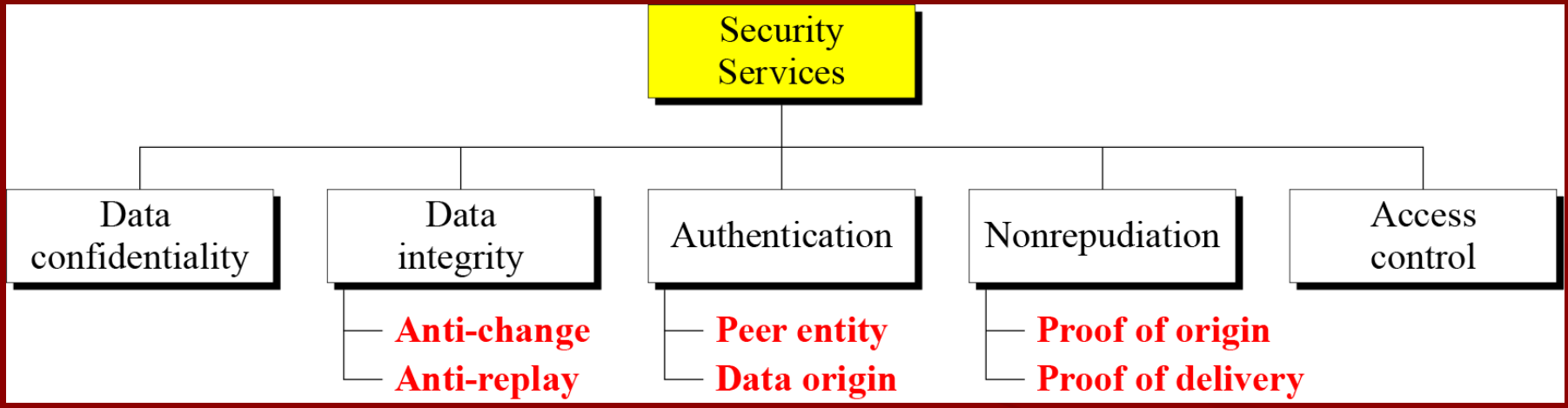
***ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..***

***Topics discussed in this section:***

**1.3.1 Security Services**
**1.3.2 Security Mechanism**
**1.3.3 Relation between Services and Mechanisms**

# 1.3.1 Security Services

## Figure 1.3 *Security services*



# Security Services (X.800)

1) Authentication-

--- Peer Entity authentication.

--- Data Origin authentication.

2)Data Confidentiality-

---Connection Confidentiality.

---Connectionless confidentiality.

---Selected Field confidentiality.

---Traffic Flow Confidentiality.

# Security Services (X.800)

3)Data Integrity.

-Connection integrity with recovery.

- Connection integrity without recovery.

- Connectionless integrity.

-Selected field connection Integrity.

- Selected field connectionless Integrity.

# Security Services (X.800)

4)Nonrepuditation

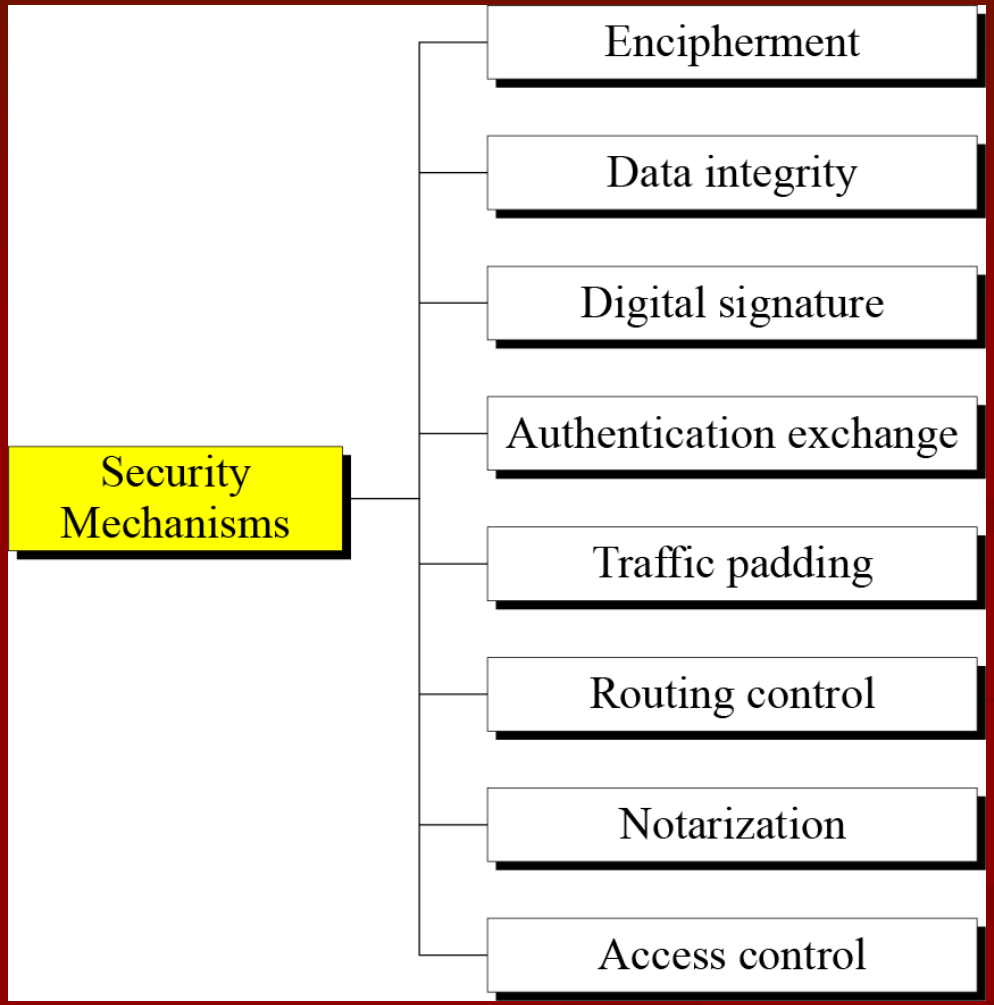
-nonrepuditation Origin.

- nonrepuditation destination.

5) Access Control

# 1.3.2 Security Mechanism

**Figure 1.4** *Security mechanisms*

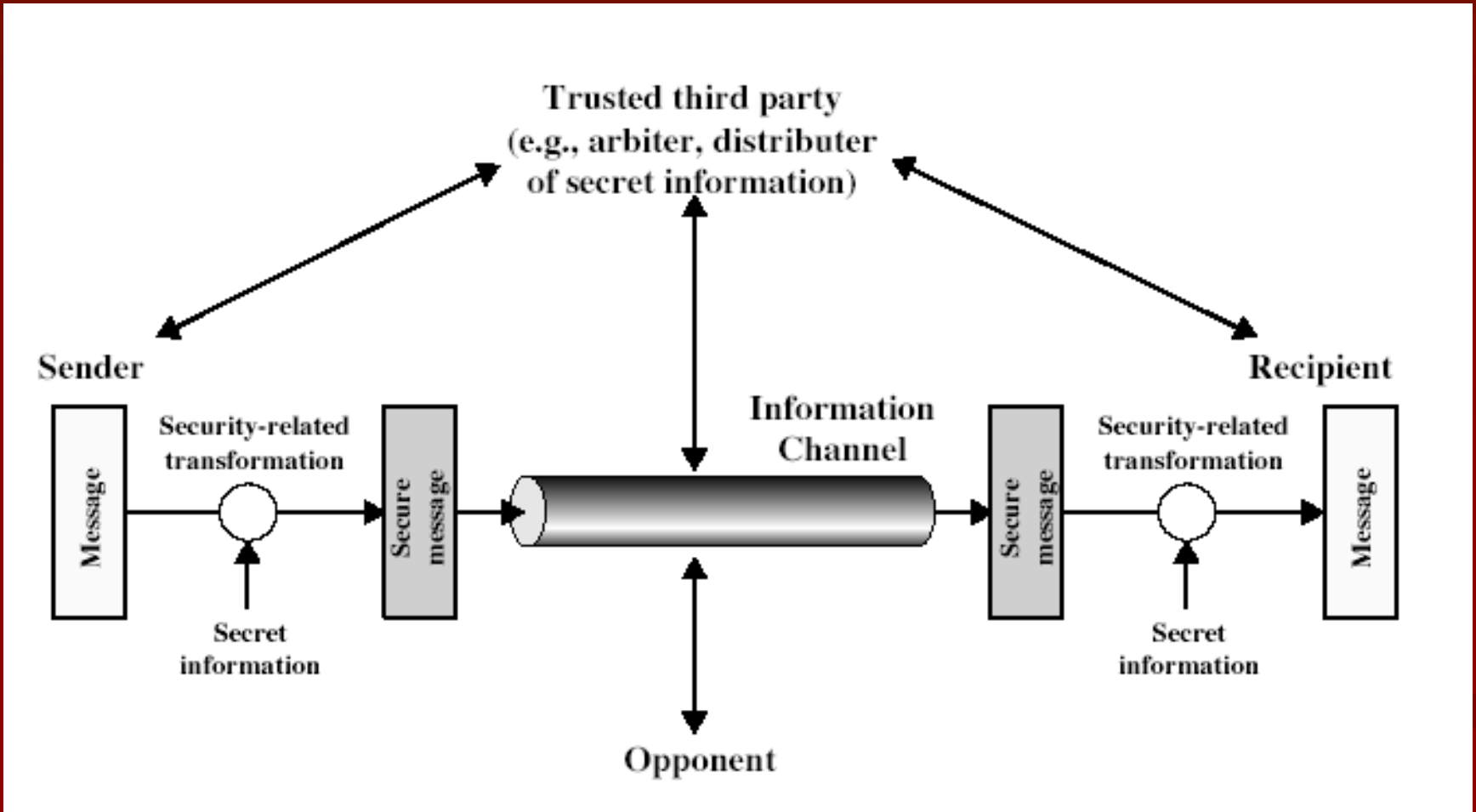


# 1.3.3 Relation between Services and Mechanisms

**Table 1.2** *Relation between security services and mechanisms*

| *Security Service* | *Security Mechanism* |
|---|---|
| Data confidentiality | Encipherment and routing control |
| Data integrity | Encipherment, digital signature, data integrity |
| Authentication | Encipherment, digital signature, authentication exchanges |
| Nonrepudiation | Digital signature, data integrity, and notarization |
| Access control | Access control mechanism |

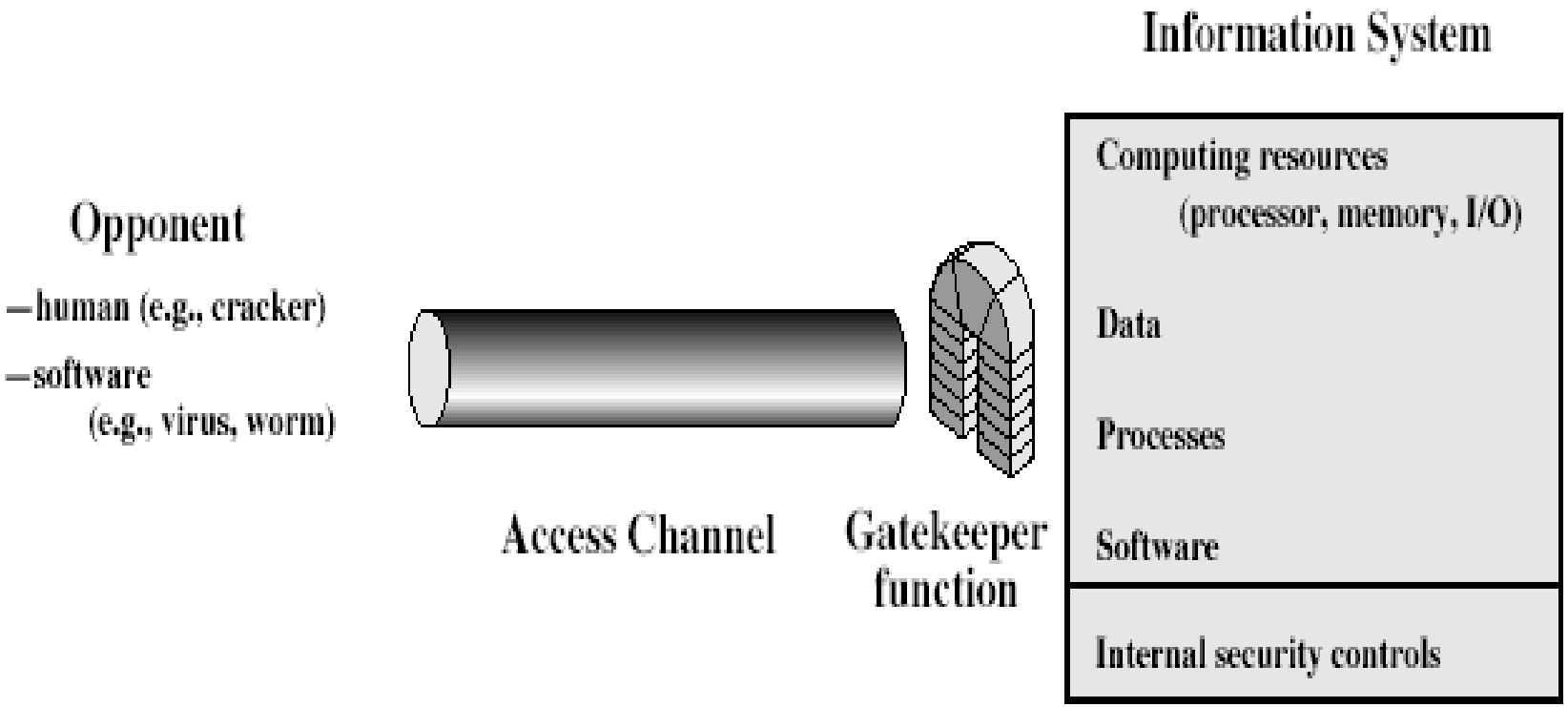
# Model for Network Security



# Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

# Model for Network Access Security



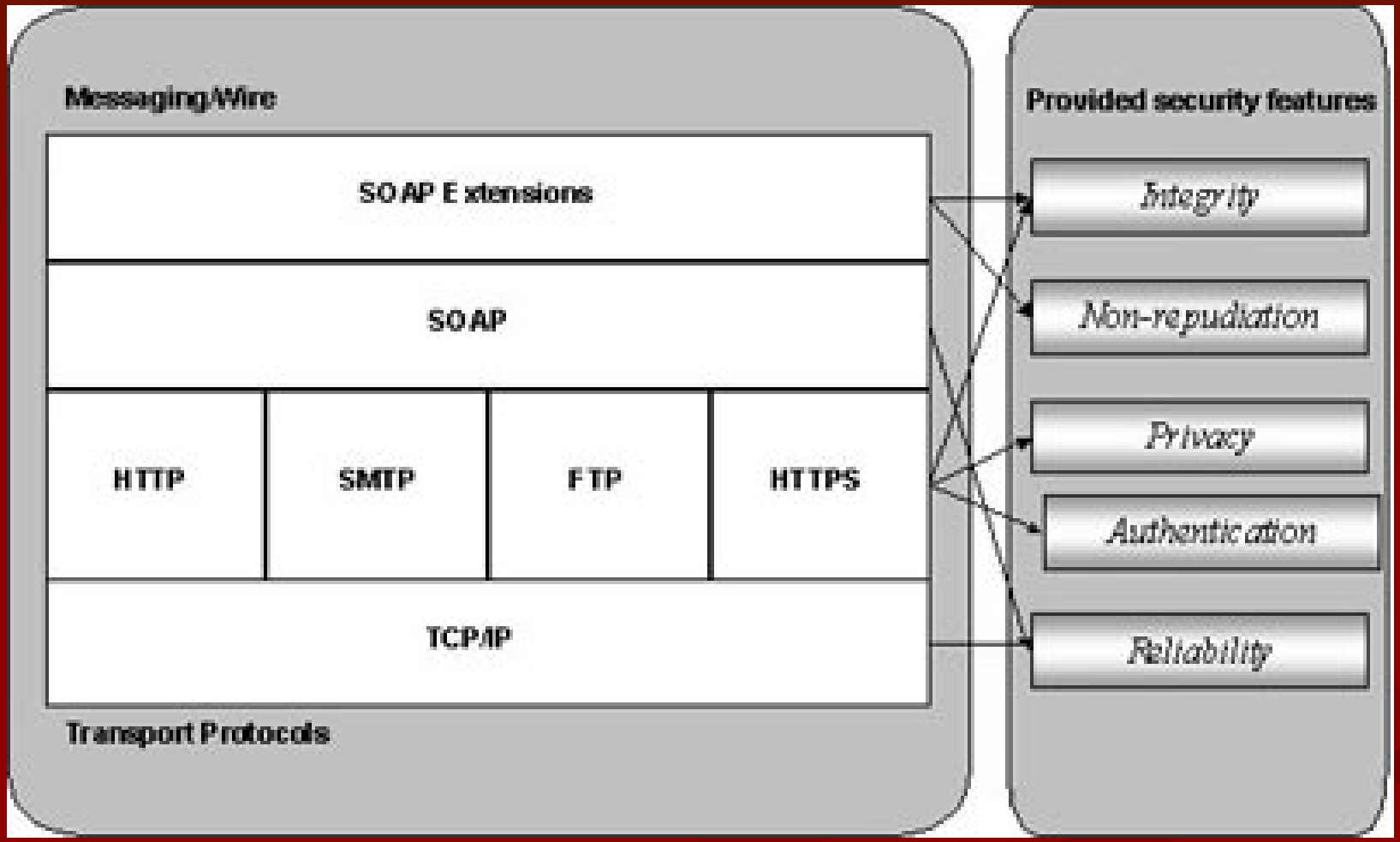
# Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems can be used to implement this model

# Secure Communication

- protecting data locally only solves a minor part of the problem. The major challenge that is introduced by the Web Service security requirements is to secure data transport between the different components. Combining mechanisms at different levels of the Web Services protocol stack can help secure data transport (see figure next page).

# Secure Communication



# Secure Communication

- The combined protocol HTTP/TLS or SSL is often referred to as HTTPS (see figure). SSL was originally developed by Netscape for secure communication on the Internet, and was built into their browsers. SSL version 3 was then adopted by IETF and standardized as the Transport Layer Security (TLS) protocol.
- Use of Public Key Infrastructure (PKI) for session key exchange during the handshake phase of TLS has been quite successful in enabling Web commerce in recent years.
- TLS also has some known vulnerabilities: it is susceptible to man-in-the-middle attacks and denial-of-service attacks.

# SOAP security

- SOAP (Simple Object Access Protocol) is designed to pass through firewalls as HTTP. This is disquieting from a security point of view. Today, the only way we can recognize a SOAP message is by parsing XML at the firewall. The SOAP protocol makes no distinction between reads and writes on a method level, making it impossible to filter away potentially dangerous writes. This means that a method either needs to be fully trusted or not trusted at all.
- The SOAP specification does not address security issues directly, but allows for them to be implemented as extensions.
  - As an example, the extension SOAP-DSIG defines the syntax and processing rules for digitally signing SOAP messages and validating signatures. Digital signatures in SOAP messages provide integrity and non-repudiation mechanisms.

# PKI

- PKI key management provides a sophisticated framework for securely exchanging and managing keys. The two main technological features, which a PKI can provide to Web Services, are:
  - **Encryption of messages**: by using the public key of the recipient
  - **Digital signatures**: non-repudiation mechanisms provided by PKI and defined in SOAP standards may provide Web Services applications with legal protection mechanisms
- Note that the features provided by PKI address the same basic needs as those that are recognized by the standardization organizations as being important in a Web Services context.
- In Web Services, PKI mainly intervenes at two levels:
  - At the SOAP level (non-repudiation, integrity)
  - At the HTTPS level (TLS session negotiation, eventually assuring authentication, integrity and privacy)

# 1-4 TECHNIQUES

*Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.*

***Topics discussed in this section:***

**1.4.1 Cryptography**
**1.4.2 Steganography**

# 1.4.1 Cryptography

*Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.*

# 1.4.2 Steganography

*The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing."*

*Example: covering data with text*

This book is mostly about cryptography, not steganography.

□ □□□ □ □ □ □ □□

0 1 0 0 0 0 1

# 1.4.2 Continued

*Example: using dictionary*

| A | friend | called | a | doctor. |
|---|---|---|---|---|
| 0 | 10010 | 0001 | 0 | 01001 |

*Example: covering data under color image*

| | | |
|---|---|---|
| 01010011 | 10111100 | 01010101 |
| 01011110 | 10111100 | 01100101 |
| 01111110 | 01001010 | 00010101 |

# 1-5 THE REST OF THE BOOK

*The rest of this book is divided into four parts.*

*Part One: Symmetric-Key Enciphermen*

*Part Two: Asymmetric-Key Encipherment*

*Part Three: Integrity, Authentication, and Key Management*

*Part Four: Network Security*