CHAPTER 1

Introduction

(Solution to Odd-Numbered Problems)

Review Questions

1. The three security goals are *confidentiality, integrity,* and *availability.*

- *Confidentiality* means protecting confidential information.
- *Integrity* means that changes to the information need to be done only by authorized entities.
- *Availability* means that information needs to be available to authorized entities.

3. We mentioned five security services: *data confidentiality, data integrity, authentication, nonrepudiation,* and *access control*.

- *Data confidentiality* is to protect data from disclosure attack.
- *Data integrity* is to protect data from modification, insertion, deletion, and replaying.
- *Authentication* means to identify and authenticate the party at the other end of the line.
- *Nonrepudiation* protects against repudiation by either the sender or the receiver of the data.
- *Access control* provides protection against unauthorized access to data.

5.

- *Cryptography***,** a word with origin in Greek, means “secret writing.” We used the term to refer to the science and art of transforming messages to make them secure and immune to attacks.
- *Steganography,* a word with origin in Greek, means "covered writing." Steganography refers to concealing the message itself by covering it with something else.

Exercises

7.

a. This is *snooping* (attack to the confidentiality of stored data). Although the contents of the test is not confidential on the day of the test, it is confidential before the test day.

b. This is modification (attack to the integrity of data). The value of the check is changed (from $10 to $100).

c. This is *denial of service* (attack to availability). Sending so many e-mails may crash the server and the service may be interrupted.

9.

a. This is *steganography.* The answers to the test has not been changed; they have been only hidden.

b. This is *cryptography.* The characters in the message are not hidden; they are replaced by another characters.

c. This is *steganography.* The special ink hides the actual writing on the check.

d. This is *steganography.* The water marks hides the actual contents of the thesis.