COMPUTER SECURITY SEGMENT-3

INSTRUCTOR: SAZID ZAMAN KHAN
ASSISTANT PROFESSOR , CSE, IIUC

Euclidean Algorithm

- One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. Two integers are **relatively prime** (or coprime) if there is no integer greater than one that divides them both (that is, their greatest common divisor is one).

Greatest Common Divisor

More formally, the positive integer c is said to be the greatest common divisor of a and b if

1. c is a divisor of a and of b.
2. any divisor of a and b is a divisor of c.

An equivalent definition is the following:

$$\gcd(a, b) = \max[k, \text{such that } k|a \text{ and } k|b]$$

Because we require that the greatest common divisor be positive, $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$. In general, $\gcd(a, b) = \gcd(|a|, |b|)$.

$$\gcd(60, 24) = \gcd(60, -24) = 12$$

Also, because all nonzero integers divide 0, we have $\gcd(a, 0) = |a|$.

We stated that two integers a and b are relatively prime if and only if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if $\gcd(a, b) = 1$.

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

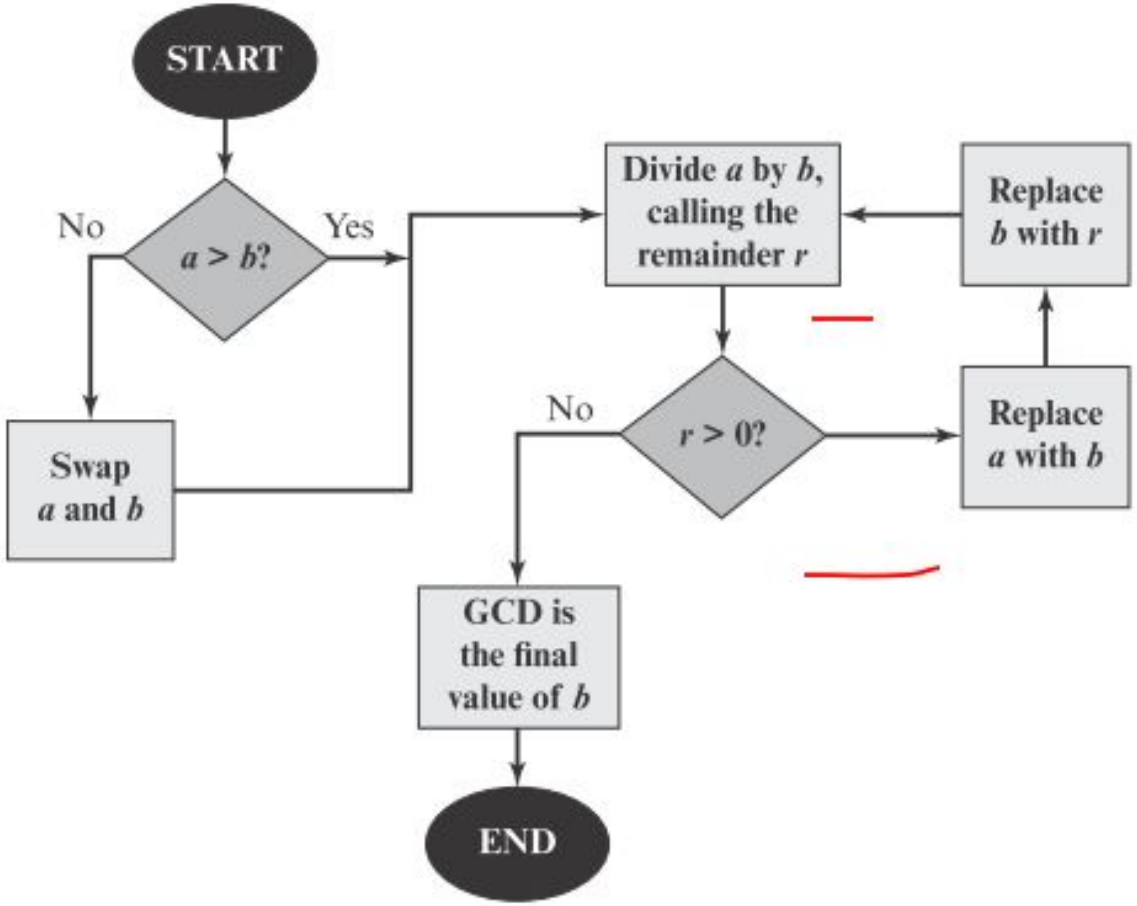


Figure 2.2 Euclidean Algorithm

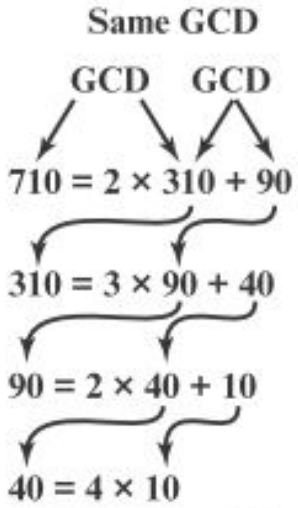


Figure 2.3 Euclidean Algorithm Example: gcd(710, 310)

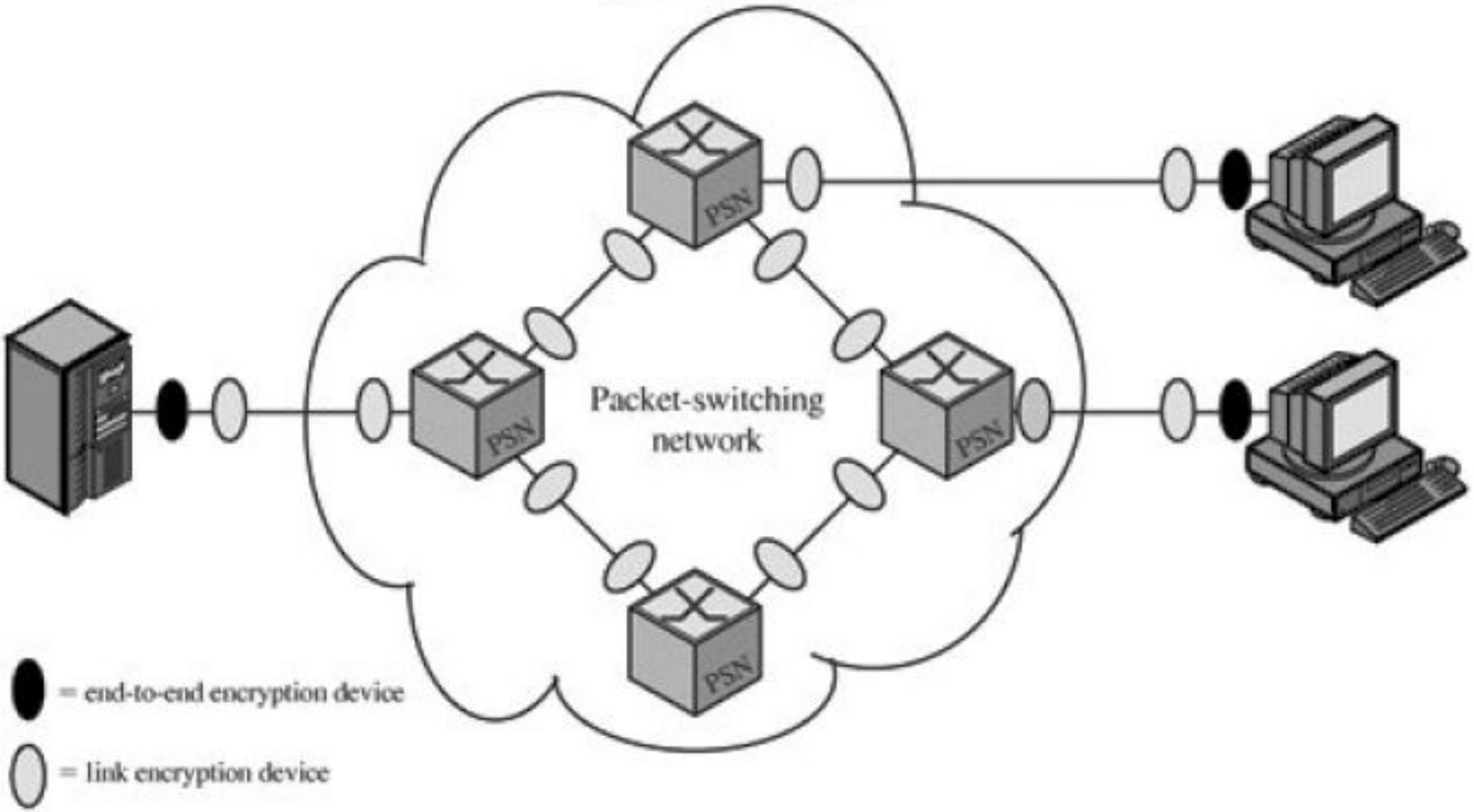
Placement of Encryption Function

- If encryption is to be used to counter attacks on confidentiality, we need to decide what to encrypt and where the encryption function should be located. To begin, this section examines the potential locations of security attacks and then looks at the two major approaches to encryption placement: link and end to end.

Figure 7.2. Encryption Across a Packet-Switching Network

(This item is displayed on page 204 in the print version)

[View full size image]



Link Encryption

- With link encryption, each vulnerable communications link is equipped on both ends with an encryption device. Thus, all traffic over all communications links is secured. Although this requires a lot of encryption devices in a large network, its value is clear.
- One of its disadvantages is that the message must be decrypted each time it enters a switch (such as a frame relay switch) because the switch must read the address (logical connection number) in the packet header in order to route the frame. Thus, the message is vulnerable at each switch. If working with a public network, the user has no control over the security of the nodes.

Link Encryption

- Several implications of link encryption should be noted. For this strategy to be effective, all the potential links in a path from source to destination must use link encryption.
- Each pair of nodes that share a link should share a unique key, with a different key used on each link. Thus, many keys must be provided.

End to End Encryption

- With end-to-end encryption, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data. The data in encrypted form are then transmitted unaltered across the network to the destination terminal or host. The destination shares a key with the source and so is able to decrypt the data.
- This plan seems to secure the transmission against attacks on the network links or switches. Thus, end-to-end encryption relieves the end user of concerns about the degree of security of networks and links that support the communication.

End to End Encryption

- Consider the following situation. A host connects to a frame relay or ATM network, sets up a logical connection to another host, and is prepared to transfer data to that other host by using end-to-end encryption.
- Data are transmitted over such a network in the form of packets that consist of a header and some user data. What part of each packet will the host encrypt? Suppose that the host encrypts the entire packet, including the header. This will not work because, remember, only the other host can perform the decryption. The frame relay or ATM switch will receive an encrypted packet and be unable to read the header.

Using both link and end to end encryption

- To achieve greater security, both link and end-to-end encryption are needed, as is shown in Figure 7.2. When both forms of encryption are employed, the host encrypts the user data portion of a packet using an end-to-end encryption key.
- The entire packet is then encrypted using a link encryption key. As the packet traverses the network, each switch decrypts the packet, using a link encryption key to read the header, and then encrypts the entire packet again for sending it out on the next link.
- Now the entire packet is secure except for the time that the packet is actually in the memory of a packet switch, at which time the packet header is in the clear.

Key Distribution

- For symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protected from access by others. Furthermore, frequent key changes are usually desirable to limit the amount of data compromised if an attacker learns the key.
- Therefore, the strength of any cryptographic system rests with the key distribution technique, a term that refers to the means of delivering a key to two parties who wish to exchange data, without allowing others to see the key. For two parties A and B, key distribution can be achieved in a number of ways, as follows:

Key Distribution

- 1. A can select a key and physically deliver it to B.
- 2. A third party can select the key and physically deliver it to A and B.
- 3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
- 4. If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

Key Distribution

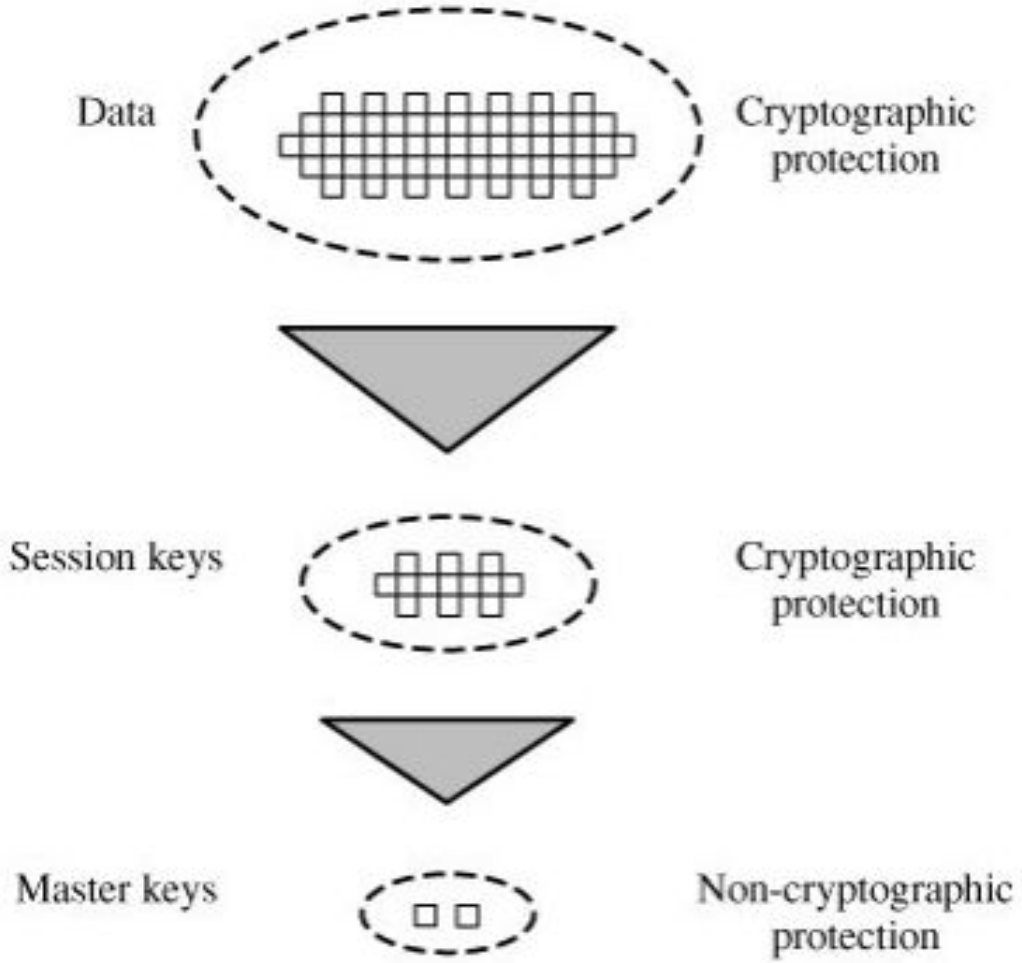
- Manual delivery is often awkward. In a distributed system, any given host or terminal may need to engage in exchanges with many other hosts and terminals over time.
- A network using node-level encryption with 1000 nodes would conceivably need to distribute as many as half a million keys.

Key Distribution

- The use of a key distribution center is based on the use of a hierarchy of keys. At a minimum, two levels of keys are used (Figure 7.8). Communication between end systems is encrypted using a temporary key, often referred to as a session key.
- Typically, the session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then discarded. Each session key is obtained from the key distribution center. Accordingly, session keys are transmitted in encrypted form, using a master key that is shared by the key distribution center and an end system or user.

Key Distribution

Figure 7.8. The Use of a Key Hierarchy



Key Distribution

- For each end system or user, there is a unique master key that it shares with the key distribution center. Of course, these master keys must be distributed in some fashion. However, the scale of the problem is vastly reduced.
- If there are N entities that wish to communicate in pairs, then, as was mentioned, as many as [N(N-1)]/2 session keys are needed at any one time. However, only N master keys are required, one for each entity.

A Key Distribution Scenario

- The key distribution concept can be deployed in a number of ways. A typical scenario is illustrated in Figure 7.9, which is based on a figure in [POPE79]. The scenario assumes that each user shares a unique master key with the key distribution center (KDC).

A Key Distribution Scenario

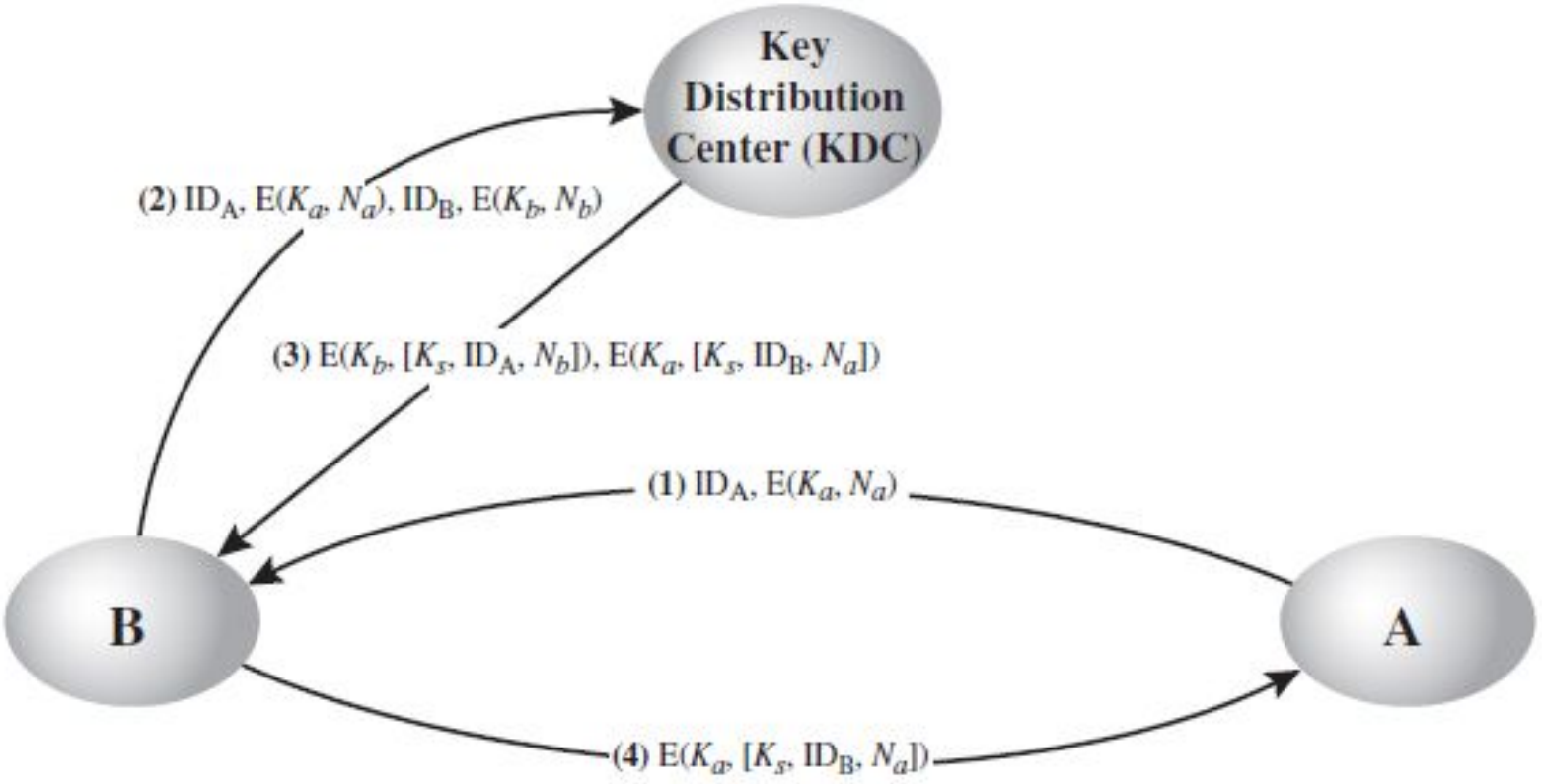


Figure 14.18 Figure for Problem 14.1

A Key Distribution Scenario

- Let us assume that user A wishes to establish a logical connection with B and requires a one-time session key to protect the data transmitted over the connection. A has a master key, K_a, known only to itself and the KDC; similarly, B shares the master key K_b with the KDC. The following steps occur:
- 1. A issues a request to the KDC for a session key to protect a logical connection to B. The message includes the identity of A and B and a unique identifier, N1, for this transaction, which we refer to as a nonce. The nonce may be a timestamp, a counter, or a random number; the minimum requirement is that it differs with each request. Also, to prevent masquerade, it should be difficult for an opponent to guess the nonce.

A Key Distribution Scenario

- The KDC responds with a message encrypted using K_a Thus, A is the only one who can successfully read the message, and A knows that it originated at the KDC. The message includes two items intended for A:
- The one-time session key, K_s, to be used for the session
- The original request message, including the nonce, to enable A to match this response with the appropriate request.

A Key Distribution Scenario

- Thus, A can verify that its original request was not altered before reception by the KDC and, because of the nonce, that this is not a replay of some previous request.
- In addition, the message includes two items intended for B:
- The one-time session key, K_s to be used for the session
- An identifier of A (e.g., its network address), ID_A
- These last two items are encrypted with K_b (the master key that the KDC shares with B). They are to be sent to B to establish the connection and prove A's identity.

A Key Distribution Scenario

- A stores the session key for use in the upcoming session and forwards to B the information that originated at the KDC for B, namely, $E(K_b, [K_s \| ID_A])$. Because this information is encrypted with K_b, it is protected from eavesdropping.
- B now knows the session key (K_s), knows that the other party is A (from ID_A), and knows that the information originated at the KDC (because it is encrypted using K_b).
- At this point, a session key has been securely delivered to A and B, and they may begin their protected exchange.

Session Key Lifetime

- The more frequently session keys are exchanged, the more secure they are, because the opponent has less ciphertext to work with for any given session key. On the other hand, the distribution of session keys delays the start of any exchange and places a burden on network capacity.
- A security manager must try to balance these competing considerations in determining the lifetime of a particular session key.

Groups, Rings and Fields

- See the selected parts from sheet “Lecture4 selected printed” (Prof. Avi Kak lectures).
- After that, for a good explanation of integral domain see the video “zero divisor _integral domain good”.
- See selected parts from “Lecture 5 selected printed”.
- See page 1-12 from “Lecture-6”.

References and disclaimer

- All resources used here are properties of the respective owners. Those are used here for educational purpose.
- **References:**
- 1. Cryptography and Network Security, Principles and Practice (7th Edition)
- -William Stallings.
- Other web sources.