CHAPTER 27

Network Security

Review Questions

1. We need privacy, authentication, integrity, and nonrepudiation for a secure network.
3. In secret key encryption, the sender and the receiver share a secret key. In public key encryption, the public key is known to everyone but the private key is known only to the receiver.
5. Secret key encryption requires fewer keys than public key encryption. For public key encryption, one key (public) encrypts the message; a different key (private) decrypts the message. For secret key encryption only one key is needed.
7. Digital signature provides authentication, integrity, and nonrepudiation.
9. PGP uses one hash function, one secret key, and 2 private-public key pairs.
11. A nonce is a number used in access authorization.

Multiple-Choice Questions

13. a
15. d
17. b
19. c
21. d
23. d
25. d

Exercises

27. Encryption algorithm:
    a. Replace character by its numerical order in the alphabet
    b. Add 6

c. Replace number with the corresponding character

Decryption algorithm:

a. Replace character by its numerical order in the alphabet

b. Subtract 6

c. Replace number with the corresponding character

29. The Caesar cipher is not very effective since the character frequencies can be guessed by looking at the ciphertext.

31. The encryption algorithm:

Perform the XOR operation on the plaintext and a block of bits that is the same size.

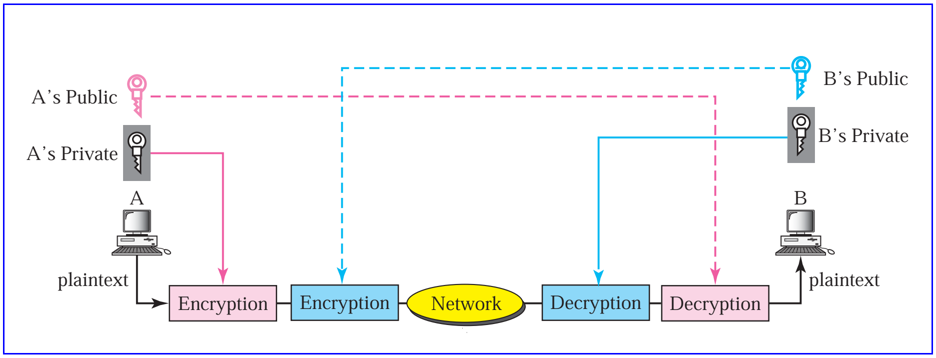
The decryption algorithm:

Perform the XOR operation on the ciphertext and the same block of bits used in the encryption process.

33. To be effective, a secret key should be used only once (one-time key). In other words, in each session, the secret key should be changed. Something, which is changing in every session cannot be used for authentication. Authentication must be provided by a robust protocol before using a secret key for other aspects of security.

35. See Figure 27.1.

Figure 27.1 *Exercise 35*


A's Public
A's Private
A
plaintext
Encryption
Encryption
Network
Decryption
Decryption
B's Public
B's Private
B
plaintext