CHAPTER 29

Internet Security

29.1 MULTIPLE-CHOICE QUESTIONS

1. a	3. b	5. a	7. b	9. d
11. d	13. b	15. d	17. c	19. a
21. b	23. a			

29.2 EXERCISES

25. h k k y c g d

27. The encryption algorithm:

OLD ==>	NEW
1	6
2	5
3	8
4	2
5	1
6	7
7	3
8	4

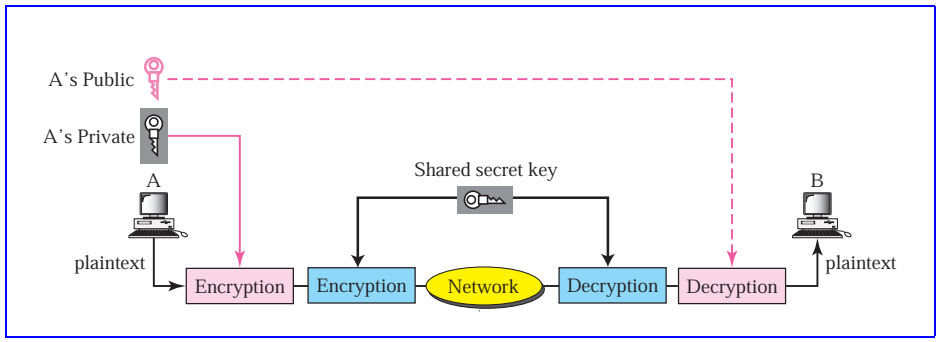
The decryption algorithm is just the opposite; for example, bit 6 is bit 1.

29. The receiver cannot prove that the message has been sent by the sender because the key used to encrypt the message is shared. The sender can claim that the receiver has created the message, encrypted, and decrypted.

31. See Figure 29.1.

33. Kerberos is an authentication system that uses shared secret key and a key distribution center (KDC). There is an authentication server (AS) that plays the role of the

Figure 29.1 *Exercise 31*



KDC. The following shows a brief descriptions of the steps in communication between A and B:

a. A contacts AS and shows that she needs to communicate with B. The communication between A and AS is done using a secret key that is stablished between A and AS.

b. AS authenticates A and creates a one-time secrete key (R). AS also sends a message to B, using secret key between B and AS, which includes A's name and R.

c. A now sends an encrypted message, using R, which includes a one-time communication key between A and B (A-B secret key).

d. B decrypts the message using R, obtains the A-B shared key and sends a message to A, using R, to show that she has received the A-B shared key.

e. Now A and B can communicate using A-B shared key.

35. See Figure 29.2.

Figure 29.2 *Exercise 35*