CHAPTER 16

Security

(Solutions to Odd-Numbered Problems)

Review Questions

1. Three security goals are confidentiality, integrity, and availability. Confidentiality is to protect our confidential information against malicious actions that endanger it. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. Availability means that the information created and stored by an organization needs to be available to authorized entities.

3. Cryptography means concealing the contents of a message by enciphering; steganography means concealing the message itself by covering it with something else.

5. Symmetric-key cryptography is based on sharing secrecy; asymmetric-key cryptography is based on personal secrecy.

7. Message integrity guarantees that the message has not been changed; A message authentication authenticate the sender of the message.

9. A digital signature can provide three security services: message authentication, message integrity, and nonrepudiation.

11. A practical solution to key distribution is the use of a trusted third party, referred to as a key-distribution center (KDC). To reduce the number of keys, each person establishes a shared secret key with the KDC. A secret key is established between the KDC and each member. This is how Alice sends a confidential message to Bob. Alice sends a request to the KDC stating that she needs a session (temporary) secret key between herself and Bob. The KDC informs Bob about Alice's request. If Bob agrees, a session key is created between the two.

Multiple-Choice Questions

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

Exercises

33.

a. Steganography

b. Cryptography

c. Steganography

d. Steganography

35. Range is 0 to 25 (for a total of 26 different key). However, Alice should not use 0 because this means no encryption.

37. Only one character will be changed because transposition does not substitute characters.

39.

Encryption

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e
S	I	H	T	N	A	S	I	R	E	X	E	E	S	I	C
4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1

Decryption

1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
S	I	H	T	N	A	S	I	R	E	X	E	E	S	I	C
t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e
4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1

41. The plaintext is 0708; the ciphertext is 0788 as shown below:

H: 07	→	$C = 70^{13} \bmod 100 = 07$
I: 08	→	$C = 08^{13} \bmod 100 = 88$

43. Numbers associated with each letter is shown in the following table.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

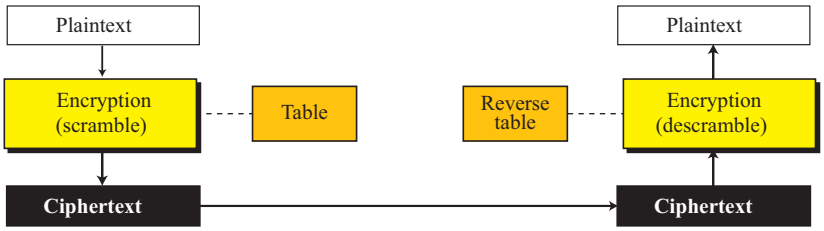
The digest is 21 as shown below.

		H		E		L		L		O		
		7		4		11		11		14		
		↓		↓		↓		↓		↓		
0	→	7	→	11	→	22	→	7	→	21	→	21

45. The system can request the user to use a long password and something which is not normally guessed (such as a birth date or a common name). The system can also allow the user to enter the password a limited number of times. If the user fails, the system may request for other type of information such as mother maiden name. The bank can use the policy to confiscate the bank card if a user enters a wrong PIN a number of times.

47. The diagram is shown in Figure S16.47.

Figure S16.47 *Exercise 47*



One possible key is the following scrambling table. The eight bits in each character are scrambled in encryption site and de-scrambled in the decryption site.

Encryption ↓	1	2	3	4	5	6	7	8	↑ Decryption
	3	7	5	1	8	2	4	6	

49. Encryption is $C = 7^3 \bmod 15 = 13$. Decryption is $P = 13^{11} \bmod 15 = 7$.

51. In symmetric-key cryptography only Alice and Bob have the secrete key. If Alice sends a message to Bob, only Bob can read the message. If later Alice denies that she has sent the message, no one can verify that she has actually sent it because no one except Bob has the duplicate key.

53. Figure S16.53 shows the solution.

Figure S16.53 *Exercise 53*