CHAPTER 16

Security

(Solutions to Practice Set)

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.
2. Five security services are: Data confidentiality, data integrity, authentication, nonrepudiation, and access control. Data confidentiality is designed to protect data from snooping and traffic analysis. Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary. Authentication identifies the party at the other end of the line. It provides authentication of the sender or receiver and authenticates the source of the data. Nonrepudiation service protects against repudiation by either the sender or the receiver of the data. Access control protects against unauthorized access to data.
3. Cryptography means concealing the contents of a message by enciphering; steganography means concealing the message itself by covering it with something else.
4. A substitution cipher replaces one symbol with another; A transposition cipher reorders symbols.
5. Symmetric-key cryptography is based on sharing secrecy; asymmetric-key cryptography is based on personal secrecy.
6. Asymmetric-key cryptography uses two distinctive keys: a private key and a public key. Bob first creates a pair of keys; he keeps the private key and publicly announces the public key. If anyone needs to send a message to Bob, she encrypts the message with Bob's public key. To read the message, Bob decrypts the message with his private key.
7. Message integrity guarantees that the message has not been changed; A message authentication authenticate the sender of the message.

8.

a. A conventional signature is included in the document; a digital signature is sent as a separate document.

b. For a conventional signature, the signature on the document is verified against a signature on a file. For a digital signature, the recipient receives the message and the signature. The recipient needs to apply the verification technique to the combination of the message and the signature to verify the authenticity.

c. For a conventional signature, there is normally a one-to-many relationship between a signature and documents. A person uses the same signature to sign many documents. For a digital signature, there is a one-to-one relationship between a signature and a message. Each message has its own signature.

d. In a conventional signature, a copy of the signed document can be distinguished from the original one on file. In a digital signature, there is no such distinction unless there is a factor of time (such as a timestamp).

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

10. Three kinds of identification witnesses discussed in this chapter: something known, something possessed, and something inherent. Something known is a secret known only by the claimant that can be checked by the verifier. Something possessed is something that can prove the claimant's identity. Something inherent is an inherent characteristic of the claimant.

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.

12. Certification authority (CA) is a federal or state organization that binds a public key to an entity and issues a certificate. The CA has a well-known public key itself that cannot be forged. The CA checks Bob's identification. It then asks for Bob's public key and writes it on the certificate. Now Bob can upload the signed certificate.

Multiple-Choice Questions

13. a	14. b	15. c	16. c	17. c	18. b
19. a	20. c	21. a	22. a	23. b	24. c
25. d	26. a	27. a	28. a	29. b	30. c
31. a	32. b				

Exercises

33.

a. Steganography

b. Cryptography

c. Steganography

d. Steganography

34.

a. $(100 \times 99) / 2 = 4950 \approx 5000$.

b. 100 (assuming the president is not a club member).

c. 99 (assuming the president is not a club member).

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

36. Only one character will be changed because in this type of encryption each character is independently encrypted.

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

38. In Encryption, each letter is shifted 7 positions towards the end of the alphabet. When we reach the end of the alphabet, we wrap the shifting toward the beginning. In decryption, each letter is shifted 7 position towards the beginning of the alphabet. When we reach the beginning, we wrap the shifting toward the end.

Encryption

Plaintext	t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Ciphertext	A	O	P	Z	P	Z	H	U	L	E	L	Y	J	P	Z	L

Decryption

Ciphertext	A	O	P	Z	P	Z	H	U	L	E	L	Y	J	P	Z	L
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Plaintext	t	h	i	s	i	s	a	n	e	x	e	r	c	i	s	e

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

40. Using number theory and cryptography (see reference), it is not difficult to find d in this case ($d = 113$). This means that if Bob chooses such a small n, it is very easy for Eve to find d. In practice, n is a very large number (more than 1000 bits)

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

$$\text{H: 07} \rightarrow C = 70^{13} \bmod 100 = 07$$

$$\text{I: 08} \rightarrow C = 08^{13} \bmod 100 = 88$$

42. If $e = 1$, the ciphertext is same as the plaintext. If Eve intercept the ciphertext, she has actually has the plaintext.

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

44. When the system defines a password for a user, there is an expiration period; after that, the system defines a new password and the old password is no longer valid. The advantage of this scheme is that if the password is stolen, it is valid only for a while. The disadvantage is the inconvenience of changing the password frequently.

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.

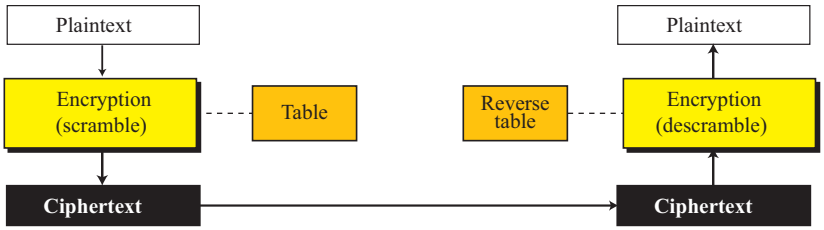
46. The Caesar cipher is so primitive that can easily be attacked:

    a. The intruder can use a brute-force attack by exhaustive search using keys from 1 to 25.

b. The intruder can use frequency of characters in the ciphertext to find the plaintext.

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.

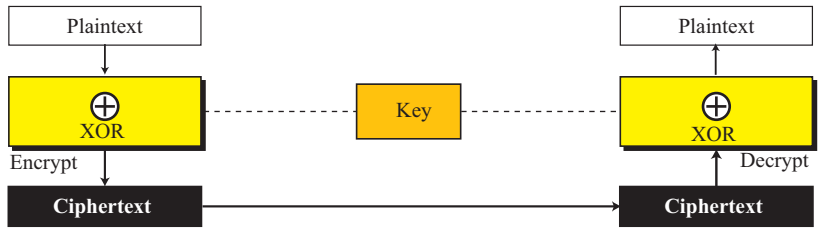
Encryption ↓

1	2	3	4	5	6	7	8
3	7	5	1	8	2	4	6

↑ Decryption

48. The encryption and decryption are shown in Figure S16.48

Figure S16.48 *Exercise 48*



For example if plain text is 1001000 and the key is 00110101 then

Encryption		
	10011000	Plaintext
⊕	00110101	Key
	10101101	Ciphertext

Decryption		
	10101101	Ciphertext
⊕	00110101	Key
	10011000	Plaintext

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

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

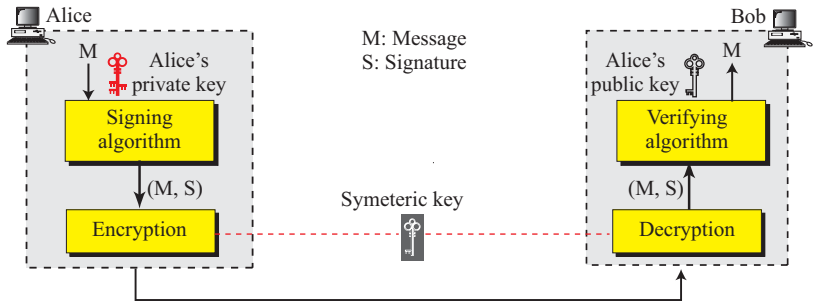
51. In symmetric-key cryptography only Alice and Bob have the secrete key. If Alice sends a message to Bob, only Bob can read the message. If later Alice denies that

she has sent the message, no one can verify that she has actually sent it because no one except Bob has the duplicate key.

52. Authentication is required when two parties don't know each other. Two parties who don't know each other do not have a shared secret key.

53. Figure S16.53 shows the solution.

Figure S16.53 *Exercise 53*



54. Figure S16.54 shows the solution.

Figure S16.54 *Exercise 54*