CHAPTER 16

Security

(Solutions to Review Questions and Problems)

Review Questions

Q16-1. Only snooping is a threat to confidentiality. Masquerading and repudiation are threats to integrity.

Q16-3. Only denial of service is a threat to availability. Repudiation and modification are threats to integrity.

Q16-5. This is an example of steganography because the letter is covered by the seal.

Q16-7. This is an example of steganography because the message is hidden inside the essay.

Q16-9. This is an example of symmetric-key cryptography because the same key is used both for encryption and decryption. In asymmetric-key cryptography, a public key should be used for encryption and a private key for decryption.

Q16-11. This is a monoalphabetic substitution cipher because changing depends on what the character is, not on the position of the character.

Q16-13. The key in this case needs to be between 0 and 25 (although there is no cipher if the key is 0). on average Eve needs to test 26/2 = 13 keys to break the code.

Q16-15. All are examples of stream ciphers. In the additive cipher, the key stream is repeated values of the key. In the monoalphabetic cipher, each key in the stream is a mapping from the plaintext to ciphertext. In the autokey cipher, each key is the previous plaintext character.

Q16-17. To be safe, the keys used in asymmetric-key cryptography should be very large. This makes the calculation very long if the message is also long. Compare the short key of DES (56 bits) with the long key of RSA (500 to 1000 bits).

Q16-19. If e = 1, there is no encryption: C = P1 = P. If Eve intercepts the ciphertext, she has the plaintext.

Q16-21. Message authentication and entity authentication both authenticate the sender for the receiver. As their names indicate, however, message authentication authenticates the sender for a particular message, while entity authentication authenticates the sender for the entire session in which several messages can be sent. If the sender is sending only a single message, message authentication has the same effect as entity authentication; if a sender is sending several messages, one entity authentication authenticates the sender for all messages.

Q16-23. The first choice is actually very inefficient and not practical because Alice needs to have a shared secret key between herself and each of the recipients. She also needs to create fifty separate MACs, one for each secret key. Alice can use digital signature and sign only one message with her own private key. She then sends a copy of the message to each recipient. Each recipient needs to use Alice's public key to verify the message.

Problems

P16-1.

a. This is **snooping** (an attack to confidentiality). Although the contents of the test are not confidential on the day of the test, they are confidential before the test day.

b. This is **modification** (an attack to integrity). The value of the check is changed (from $10 to $100).

c. This is **denial of service** (an attack to availability). Sending so many e-mails may crash the server and the service may be interrupted.

P16-3.

a. The ciphertext is **NBCMCMUHYRYLWCMY** as shown below:

Plaintext	Encryption	Ciphertext
t → 19	(19 + 20) mod 26	13 → N
h → 07	(07 + 20) mod 26	01 → B
i → 08	(08 + 20) mod 26	02 → C
s → 18	(18 + 20) mod 26	12 → M
i → 08	(08 + 20) mod 26	02 → C
s → 18	(18 + 20) mod 26	12 → M
a → 00	(00 + 20) mod 26	20 → U
n → 13	(13 + 20) mod 26	07 → H
e → 04	(04 + 20) mod 26	24 → Y
x → 23	(23 + 20) mod 26	17 → R
e → 04	(04 + 20) mod 26	24 → Y
r → 17	(17 + 20) mod 26	11 → L
c → 02	(02 + 20) mod 26	22 → W
i → 08	(08 + 20) mod 26	02 → C
s → 18	(18 + 20) mod 26	12 → M
e → 04	(04 + 20) mod 26	24 → Y

b. We can retrieve the plaintext by subtracting 20 from each ciphertext character using modulo 26 arithmetic as shown below:

Ciphertext	Decryption	Plaintext
N → 13	(13 – 20) mod 26	19 → t
B → 01	(01 – 20) mod 26	07→ h
C → 02	(02 – 20) mod 26	08 → i

M → 12	(12 – 20) mod 26	18 → s
C → 02	(02 – 20) mod 26	08 → i
M → 12	(12 – 20) mod 26	18 → s
U → 20	(20 – 20) mod 26	00 → a
H → 07	(07 – 20) mod 26	13 → n
Y → 24	(24 – 20) mod 26	04 → e
R → 17	(17 – 20) mod 26	23 → x
Y → 24	(24 – 20) mod 26	04 → e
L → 11	(11 – 20) mod 26	17 → r
W → 22	(22 – 20) mod 26	02 → c
C → 02	(02 – 20) mod 26	08 → i
M → 12	(12 – 20) mod 26	18 → s
Y → 24	(24 – 20) mod 26	04 → e

P16-5. The plaintext and ciphertext are shown below, ignoring the space:

Plaintext	Ciphertext
an exercise	**(5, 5), (3, 3), (1, 5), (3, 1), (1, 5), (2, 2), (3, 5), (4, 4), (3, 2), (1, 5)**

P16-7. We apply the key = 1, 2, 3, 4, 5, 6, and 7 to find the plaintext.

Ciphertext	Key	Plaintext
UVACLYZLJBL	1	tuzbkxeykiaxy
UVACLYZLJBL	2	styajwdxjhzwj
UVACLYZLJBL	3	rsxzivcwigyvi
UVACLYZLJBL	4	qrwyhubvhfxuh
UVACLYZLJBL	5	pqvxgtaugewtg
UVACLYZLJBL	6	opuwfsztfdvsf
UVACLYZLJBL	7	notverysecure

P16-9. We first find the value of $\Phi = (p - 1) \times (q - 1) = 120$. We then need to see which of the e values satisfies the relation $(d \times e) \bmod 120 = 1$. We will find that 103 is the answer.

a. $(7 \times 11) \bmod 120 = 77$

b. $(7 \times 103) \bmod 120 = 721 \bmod 120 = 1$ **(Answer is 103)**

c. $(7 \times 19) \bmod 120 = 133 \bmod 120 = 13$

P16-11. The key that is concatenated with the message in a MAC should be a secret between Alice and Bob; no one else should know this secret. When Alice sends a MAC to Bob, the key cannot be the public key of Bob or the private key of Alice. If the key is the public key of Bob, everyone (including Eve) knows this key and can use it to create a MAC to pretend that she is Alice. If the key is the private key of Alice, no one (including Bob) knows the key. So Bob cannot verify that a MAC was truly created by Alice.