Quizzes: Chapter 16

1. Three security goals are _____.
   a. confidentiality, cryptography, and nonrepudiation
   b. confidentiality, encryption, and decryption
   c. confidentiality, integrity, and availability
   d. confidentiality, denial of service, and masquerading
   Correct Answer: (c)

2. Which of the following attacks is threatening integrity?
   a. Masquerading
   b. Traffic Analysis
   c. Denial of service
   d. Encoding
   Correct Answer: (a)

3. Which of the following attacks is threatening availability?
   a. Replaying
   b. Modification
   c. Denial of service
   d. Decoding
   Correct Answer: (c)

4. _____ means concealing the contents of a message by enciphering.
   a. Steganography
   b. Cryptography
   c. Compressing
   d. Authentication

Correct Answer: (b)

5. _____means concealing the message by covering it with something else.
   a. Cryptography
   b. Steganography
   c. Compressing
   d. Authentication

   Correct Answer: (b)

6. In _____cryptography, the same key is used by the sender and the receiver.
   a. symmetric-key
   b. asymmetric-key
   c. public-key
   d. open-key

   Correct Answer: (a)

7. In _____ cryptography, the same key is used in both directions.
   a. symmetric-key
   b. asymmetric-key
   c. public-key
   d. open-key

   Correct Answer: (a)

8. _____ cryptography is often used for long messages.
   a. Symmetric-key
   b. Asymmetric-key
   c. Public-key
   d. Open-key

   Correct Answer: (a)

9. _____ cryptography is often used for short messages.
   a. Symmetric-key
   b. Asymmetric-key
   c. Secret-key
   d. Open-key

Correct Answer: (b)

10. _____means that the sender and the receiver expect confidentiality.
    a. Nonrepudiation
    b. Integrity
    c. Authentication
    d. encryption and decryption
    Correct Answer: (d)

11. _____ means that the data must arrive at the receiver exactly as they were sent.
    a. Nonrepudiation
    b. Message integrity
    c. Authentication
    d. Secrecy
    Correct Answer: (b)

12. _____ can provide authentication, integrity, and nonrepudiation for a message.
    a. Encryption/decryption
    b. Digital signature
    c. Compression
    d. Key-exchange
    Correct Answer: (b)

13. In _____, the identity of a party is verified once for the entire duration of system access.
    a. entity authentication
    b. message integrity
    c. message authentication
    d. message encryption
    Correct Answer: (a)

14. In _____ cryptography, everyone has access to everyone's public key.

a. symmetric-key
b. asymmetric-key
c. secret-key
d. private-key
Correct Answer: (b)

15. In the asymmetric-key method used for confidentiality, which key(s) is (are) publicly known?
a. encryption key only
b. decryption key only
c. both encryption and decryption keys
d. neither encryption key nor decryption key
Correct Answer: (b)

16. The RSA algorithm for confidentiality uses _____ cryptography.
a. asymmetric-key
b. symmetric-key
c. substitution
d. transposition
Correct Answer: (a)

17. In RSA, if user A wants to send an encrypted message to user B, the plaintext is encrypted with the public key of _____.
a. user A
b. user B
c. the network
d. a third party.
Correct Answer: (b)

6

8

10