**Chapter 11 Review Questions**

1. What is data called that is to be encrypted by inputting into an encryption algorithm?

a. Plaintext – Pg408

b. Cleartext

c. Opentext

d. Ciphertext

2. Which of the following is not a basic security protection over information that cryptography can provide?

a. Confidentiality

b. Stop loss – Pg410

c. Integrity

d. Authenticity

3. The areas of a file in which steganography can hide data include all of the following except \_\_\_\_\_.

a. in data that is used to describe the content or structure of the actual data

b. in the directory structure of the file system – Pg407

c. in the file header fields that describe the file

d. in areas that contain the content data itself

4. Proving that a user sent an e-mail message is known as \_\_\_\_\_\_\_.

a. repudiation

b. integrity

c. nonrepudiation – Pg410

d. availability"

5. Symmetric cryptographic algorithms are also called \_\_\_\_\_\_\_.

a. private key cryptography – Pg417

b. cipherkey cryptography

c. public/private key cryptography

d. public key cryptography

6. A(n) \_\_\_\_\_\_\_ is not decrypted, but is only used for comparison purposes.

a. stream

b. hash – Pg411

c. algorithm

d. key

7. Each of the following is a characteristic of a secure hash algorithm except \_\_\_\_\_\_.

a. collisions should be rare – Pg412

b. the results of a hash function should not be reversed

c. the hash should always be the same fixed size

d. a message cannot be produced from a predefined hash

8. Hashing would not be used in which of the following examples?

a. bank automatic teller machine (ATM)

b. encrypting and decrypting e-mail attachments – Pgs411-413

c. verifying a user password entered on a Linux system

d. determining the integrity of a message encrypts a hash with a shared secret key.

9. \_\_\_\_\_\_\_\_ encrypts a hash with a shared secret key.

a. Key\_hash

b. WEP

c. MDRIPE

d. Hashed Message Authentication Code (HMAC) – Pg413

10. Which of the following is a protection provided by hashing?

a. Authenticity

b. Confidentiality

c. Integrity – Pg412

d. Availability

11. \_\_\_\_\_\_\_ is a hash that uses two different and independent parallel chains of computation, the results of which are then combined at the end of the process.

a. DES

b. AES

c. RC4

d. RIPEMD – Pg415

12. Which of the following is the strongest symmetric cryptographic algorithm?

a. Advanced Encryption Standard – Pg422

b. Data Encryption Standard

c. Triple Data Encryption Standard

d. Rivest Cipher (RC) 1

13. If Bob wants to send a secure message to Alice using an asymmetric cryptographic algorithm, the key he uses to encrypt the message is \_\_\_\_\_\_\_.

a. Alice’s private key

b. Alice’s public key – Pg424

c. Bob’s public key

d. Bob’s private key

14. A digital signature can provide each of the following benefits except \_\_\_\_\_\_\_.

a. prove the integrity of the message

b. verify the receiver – Pg424

c. verify the sender

d. enforce nonrepudiation

15. Which of the following asymmetric cryptographic algorithms is the most secure?

a. MEC-2

b. RSA

c. MD-17

d. SHA-2 – Pg415

16. Which of the following asymmetric encryption algorithms uses prime numbers?

a. EFS

b. Quantum computing

c. ECC

d. RSA – Pg427

17. \_\_\_\_\_\_\_ uses lattice-based cryptography and may be more resistant to quantum computing attacks.

a. NTRUEncrypt – Pg429

b. ECC

c. RC4

d. SHA-512

18. The Trusted Platform Module (TPM) \_\_\_\_\_\_.

a. allows the user to boot a corrupted disk and repair it

b. is only available on Windows computers running BitLocker

c. includes a pseudorandom number generator (PRNG)

d. provides cryptographic services in hardware instead of software – Pg432

19. Which of the following has an onboard key generator and key storage facility, accelerated symmetric and asymmetric encryption, and can back up sensitive material in encrypted form?

a. Trusted Platform Module (TPM)

b. Self-encrypting hard disk drives (HDDs)

c. Encrypted hardware-based USB devices

d. Hardware Security Module (HSM) – Pg433

20. The Microsoft Windows LAN Manager hash \_\_\_\_\_\_.

a. is weaker than NTLMv2 – Pg416

b. is part of BitLocker

c. is required to be present when using TPM

d. is identical to MD-4

**Chapter 12 Review Questions**

1. The strongest technology that would assure Alice that Bob is the sender of a message is a(n) \_\_\_\_\_\_\_.

a. digital signature

b. encrypted signature

c. hash

d. digital certificate" – Pg453

2. A digital certificate associates \_\_\_\_\_\_\_.

a. a private key with a digital signature

b. the user’s identity with their public key – Pg453

c. a user’s private key with the public key

d. a user’s public key with their private key

3. Digital certificates can be used for each of the following except \_\_\_\_\_\_\_.

a. to verify the authenticity of the Registration Authorizer – Pg457

b. to verify the identity of clients and servers on the Web

c. to encrypt messages for secure e-mail communications

d. to encrypt channels to provide secure communication between clients and servers

4. An entity that issues digital certificates is a \_\_\_\_\_\_\_\_.

a. Certificate Signatory (CS)

b. Signature Authority (SA)

c. Digital Signer (DS)

d. Certificate Authority (CA) – Pg454

5. A centralized directory of digital certificates is called a(n) \_\_\_\_\_\_.

a. Digital Signature Approval List (DSAP)

b. Digital Signature Permitted Authorization (DSPA)

c. Authorized Digital Signature (ADS)

d. Certificate Repository (CR) – Pg456

6. Each of the following is a field of an X.509 certificate except

a. validity period

b. CA expiration code – Pg462

c. serial number

d. Signature

7. In order to ensure a secure cryptographic connection between a Web browser and a Web server, a(n) \_\_\_\_\_\_\_ would be used.

a. e-mail Web certificate

b. server digital certificate – Pg458

c. personal digital certificate

d. Web digital certificate

8. A digital certificate that turns the address bar green is a(n) \_\_\_\_\_\_\_\_.

a. X.509 Certificate

b. Advanced Web Server Certificate (AWSC)

c. Extended Validation SSL Certificate – Pg461

d. Personal Web-Client Certificate

9. The \_\_\_\_\_\_\_\_\_\_ -party trust model supports CA.

a. first

b. second

c. third – Pg465

d. fourth

10. Public-Key Cryptography Standards (PKCS) .

a. are used to create public keys only

b. define how hashing algorithms are created

c. have been replaced by PKI

d. are widely accepted in the industry – Pg463

11. Each of the following is true regarding a hierarchical trust model except \_\_\_\_\_\_\_\_\_.

a. it assigns a signal hierarchy with one master CA

b. it is designed for use on a large scale – Pg466

c. the master CA is called the root

d. the root signs all digital certificate authorities with a single key

12. Dual-sided digital certificates \_\_\_\_\_\_\_\_.

a. are used in military and financial settings when it is necessary for the client to authenticate back to the server – Pg461

b. are the same as dual-key digital certificates

c. are required under PKCS #1

d. require a special browser

13. Which of the following is not where keys can be stored?

a. In hashes – Pg469

b. On the user’s local system

c. Embedded in digital certificates

d. In tokens

14. Public key infrastructure (PKI) \_\_\_\_\_\_\_.

a. creates private key cryptography

b. requires the use of an RA instead of a CA

c. generates public/private keys automatically

d. is the management of digital certificates – Pg462

15. A(n) \_\_\_\_\_\_\_\_ is a published set of rules that govern the operation of a PKI.

a. certificate policy (CP) – Pg468

b. certificate practice statement (CPS)

c. signature resource guide (SRG)

d. enforcement certificate (EF)

16. Which of the following is not part of the certificate life cycle?

a. Authorization – Pg469

b. Creation

c. Expiration

d. Revocation

17. \_\_\_\_\_\_ refers to a situation in which keys are managed by a third party, such as a trusted CA.

a. Remote key administration

b. Trusted key authority

c. Key authorization

d. Key escrow – Pg470

18. \_\_\_\_\_\_\_\_\_ is a protocol for securely accessing a remote computer.

a. Secure Shell (SSH) – Pg472

b. Secure Sockets Layer (SSL)

c. Secure Hypertext Transport Protocol (SHTTP)

d. Transport Layer Security (TLS)

19. What is the cryptographic transport protocol that is used most often to secure Web transactions?

a. SHTTP

b. PPPTPoE

c. HTTPS – Pg473

d. MD-17

20. Which transport encryption algorithm is integrated as part of IPv6?

a. IPsec – Pg474

b. SSH

c. SSL/TLS

d. RSA