Chapter 8 Study Guide

Indicate whether the statement is true or false.

1. The S-HTTP security solution provides six services: authentication by digital signatures, message encryption, compression, e-mail compatibility, segmentation, and key management.
   a. True
   b. False

2. Secure Electronic Transactions was developed by MasterCard and VISA in 1997 to protect against electronic payment fraud.
   a. True
   b. False

3. A cryptovariable is a value representing the application of a hash algorithm on a message.
   a. True
   b. False

4. The asymmetric encryption systems use a single key to both encrypt and decrypt a message.
   a. True
   b. False

5. Nonrepudiation means that customers or partners can be held accountable for transactions, such as online purchases, which they cannot later deny.
   a. True
   b. False

6. Popular cryptosystems use a hybrid combination of symmetric and asymmetric algorithms.
   a. True
   b. False

7. Bluetooth is a de facto industry standard for short-range wireless communications between devices.
   a. True
   b. False

8. A brute force function is a mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm message identity and integrity.
   a. True
   b. False

9. The permutation cipher simply rearranges the values within a block to create the ciphertext.
   a. True
   b. False

10. You cannot combine the XOR operation with a block cipher operation.
    a. True
    b. False

Chapter 8 Study Guide

11. The encapsulating security payload protocol provides secrecy for the contents of network communications as well as system-to-system authentication and data integrity verification.

a. True

b. False

12. In 1917, Gilbert S.Vernam, an AT&T employee, invented a polyalphabetic cipher machine that used a non-repeating random key.

a. True

b. False

13. To perform the Caesar cipher encryption operation, the pad values are added to numeric values that represent the plaintext that needs to be encrypted.

a. True

b. False

14. PKI systems are based on public key cryptosystems and include digital certificates and certificate authorities.

a. True

b. False

15. In addition to being credited with inventing a substitution cipher, Julius Caesar was associated with an early version of the transposition cipher.

a. True

b. False

16. Sequence encryption is a series of encryptions and decryptions between a number of systems, wherein each system in a network decrypts the message sent to it and then reencrypts it using different keys and sends it to the next neighbor, and this process continues until the message reaches the final destination.

a. True

b. False

17. Standard-HTTP (S-HTTP) is an extended version of the Hypertext Transfer Protocol that provides for the encryption of individual messages transmitted via the Internet between a client and server.

a. True

b. False

18. When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message.

a. True

b. False

19. 3DES was created to offer the same strength as the DES algorithm but ran three times as fast, thus saving time.

a. True

b. False

Chapter 8 Study Guide

20. The most common hybrid system is based on the Diffie-Hellman key exchange, which is a method for exchanging private keys using public key encryption.

a. True

b. False

21. The AES algorithm was the first public key encryption algorithm to use a 256 bit key length.

a. True

b. False

22. Steganography is a data hiding method that involves embedding information within other files, such as digital pictures or other images.

a. True

b. False

23. One encryption method made popular by spy movies involves using the text in a book as the key to decrypt a message.

a. True

b. False

24. SSL builds on the encoding format of the Multipurpose Internet Mail Extensions protocol and uses digital signatures based on public key cryptosystems to secure e-mail.

a. True

b. False

25. Usually, as the length of a crytpovariable increases, the number of random guesses that have to be made in order to break the code is reduced.

a. True

b. False

26. Common implementations of a Registration Authority (RA) include functions to issue digital certificates to users and servers.

a. True

b. False

27. Adopted by NIST in 1976 as a federal standard, DES uses a 64-bit block size and key.

a. True

b. False

28. Hashing functions require the use of keys.

a. True

b. False

29. Internet Protocol Security (IPSec) is an open-source protocol framework for security development within the TCP/IP family of protocol.

a. True

b. False

Chapter 8 Study Guide

30. In 1953, Giovan Batista Bellaso introduced the idea of the passphrase (password) as a key for encryption.
    a. True
    b. False

Indicate the answer choice that best completes the statement or answers the question.

31. _____ are encrypted messages that can be mathematically proven to be authentic.
    a. Digital signatures b. MAC
    c. Message certificates d. Message digests

32. _____ is the information used in conjunction with an algorithm to create the ciphertext from the plaintext or derive the plaintext from the ciphertext.
    a. Password b. Cipher
    c. Key d. Passphrase

33. _____ is the entire range of values that can possibly be used to construct an individual key.
    a. Code b. Keyspace
    c. Algorithm d. Cryptogram

34. _____ is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.
    a. MAC b. PKI
    c. DES d. AES

35. More advanced substitution ciphers use two or more alphabets, and are referred to as _____ substitutions.
    a. multialphabetic b. monoalphabetic
    c. polyalphabetic d. polynomic

36. _____ is the current federal information processing standard that specifies a cryptographic algorithm used within the U.S. government to protect information in federal agencies that are not a part of the national defense infrastructure.
    a. DES b. 2DES
    c. AES d. 3DES

37. The _____ protocol provides system-to-system authentication and data integrity verification, but does not provide secrecy for the content of a network communication.
    a. ESP b. AH
    c. HA d. SEP

38. The _____ is responsible for the fragmentation, compression, encryption, and attachment of an SSL header to the cleartext prior to transmission.
    a. Standard HTTP b. SFTP
    c. S-HTTP d. SSL Record Protocol

Chapter 8 Study Guide

39. _____ is a protocol that can be used to secure communications across any IP-based network such as LANs, WANs, and the Internet.

a. PEM b. SSH

c. IPSec d. SET

40. _____ is a hybrid cryptosystem that combines some of the best available cryptographic algorithms and has become the open-source de facto standard for encryption and authentication of e-mail and file storage applications.

a. PGP b. DES

c. AH d. ESP

41. SHA-1 produces a(n) _____-bit message digest, which can then be used as an input to a digital signature algorithm.

a. 48 b. 56

c. 160 d. 256

42. Using a database of precomputed hashes from sequentially calculated passwords called a(n) _____, an attacker can simply look up a hashed password and read out the text version.

a. timing matrix b. agile scrum

c. rainbow table d. smurf list

43. _____ functions are mathematical algorithms that generate a message summary or digest to confirm the identity of a specific message and to confirm that there have not been any changes to the content.

a. Hash b. Map

c. Key d. Encryption

44. _____ is the amount of effort (usually in hours) required to perform cryptanalysis to decode an encrypted message when the key or algorithm (or both) are unknown.

a. Code b. Algorithm

c. Key d. Work factor

45. Digital signatures should be created using processes and products that are based on the _____.

a. DSS b. NIST

c. SSL d. HTTPS

46. At the World Championships in Athletics in Helsinki in August of 2005, a virus called Cabir infected dozens of _____, the first time this occurred in a public setting.

a. Ipad tablets b. Bluetooth mobile phones

c. WiFi routers d. laptop Macintosh computers

47. Bit stream methods commonly use algorithm functions like the exclusive OR operation (_____).

a. XOR b. EOR

c. NOR d. OR

48. _____ was developed by Phil Zimmermann and uses the IDEA Cipher for message encoding.

a. PEM b. PGP

c. S/MIME d. SSL

Chapter 8 Study Guide

49. An X.509 v3 certificate binds a _____, which uniquely identifies a certificate entity, to a user's public key.
a. message digest b. fingerprint
c. distinguished name d. digital signature

50. The CA periodically distributes a(n) _____ to all users that identifies all revoked certificates.
a. CRL b. RA
c. MAC d. RDL

51. A _____ is a key-dependent, one-way hash function that allows only specific recipients (symmetric key holders) to access the message digest.
a. signature b. MAC
c. fingerprint d. digest

52. _____ is the process of converting an original message into a form that is unreadable to unauthorized individuals.
a. Encryption b. Decryption
c. Cryptology d. Cryptography

53. A method of encryption that requires the same secret key to encipher and decipher the message is known as _____ encryption.
a. asymmetric b. symmetric
c. public d. private

54. The _____ algorithm, developed in 1977, was the first public key encryption algorithm published for commercial use.
a. DES b. RSA
c. MAC d. AES

55. DES uses a(n) _____-bit block size.
a. 32 b. 64
c. 128 d. 256