Multiple Choice Questions in Data Communications and Networking

A Complete Chapter Quiz

Network Security

Compilation of all the quizzes (MCQs) for each and every chapters in the book of Data Communications and Networking 4th Edition by Behrouz A. Forouzan.

1. Message_____ means that the data must arrive at the receiver exactly as sent.
A) confidentiality
B) integrity
C) authentication
D) none of the above

2. Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
A) confidentiality
B) integrity
C) authentication
D) none of the above

3. A(n) _____function creates a message digest out of a message.
A) encryption
B) decryption
C) hash
D) none of the above

4. The secret key between members needs to be created as a _____ key when two members contact KDC.
A) public
B) session
C) complimentary
D) none of the above

5. The _____ criterion ensures that a message cannot easily be forged.
A) one-wayness
B) weak-collision-resistance
C) strong-collision-resistance
D) none of the above

6. A(n) _____ is a trusted third party that assigns a symmetric key to two parties.
A) KDC
B) CA
C) KDD
D) none of the above

7. A witness used in entity authentication is _____.
A) something known
B) something possessed
C) something inherent
D) all of the above

8. A _____ message digest is used as an MDC.
A) keyless
B) keyed
C) either (a) or (b)
D) neither (a) nor (b)

9. A(n)_____ creates a secret key only between a member and the center.
A) CA
B) KDC
C) KDD
D) none of the above

10. _____ means to prove the identity of the entity that tries to access the system's resources.
A) Message authentication
B) Entity authentication
C) Message confidentiality
D) none of the above

11. A _____ signature is included in the document; a _____ signature is a separate entity.
A) conventional; digital
B) digital; digital
C) either (a) or (b)
D) neither (a) nor (b)

12. If _____ is needed, a cryptosystem must be applied over the scheme.
A) integrity

B) confidentiality
C) nonrepudiation
D) authentication

13. Digital signature provides _____.
A) authentication
B) nonrepudiation
C) both (a) and (b)
D) neither (a) nor (b)

14. Digital signature cannot provide _____ for the message.
A) integrity
B) confidentiality
C) nonrepudiation
D) authentication

15. To authenticate the data origin, one needs a(n) _____.
A) MDC
B) MAC
C) either (a) or (b)
D) neither (a) nor (b)

16. A(n) _____ can be used to preserve the integrity of a document or a message.
A) message digest
B) message summary
C) encrypted message
D) none of the above

17. Challenge-response authentication can be done using _____.
A) symmetric-key ciphers
B) asymmetric-key ciphers
C) keyed-hash functions
D) all of the above

18. The _____criterion ensures that we cannot find two messages that hash to the same digest.
A) one-wayness
B) weak-collision-resistance
C) strong-collision-resistance
D) none of the above

19. A digital signature needs a(n)_____ system.
A) symmetric-key
B) asymmetric-key
C) either (a) or (b)
D) neither (a) nor (b)

20. A(n) _____is a federal or state organization that binds a public key to an entity and issues a certificate.
A) KDC
B) Kerberos
C) CA
D) none of the above

21. Message _____ means that the sender and the receiver expect privacy.
A) confidentiality
B) integrity
C) authentication
D) none of the above

22. In _____ authentication, the claimant proves that she knows a secret without actually sending it.
A) password-based
B) challenge-response
C) either (a) or (b)
D) neither (a) nor (b)

23. In _____, a claimant proves her identity to the verifier by using one of the three kinds of witnesses.
A) message authentication
B) entity authentication
C) message confidentiality
D) message integrity

24. The _____ criterion states that it must be extremely difficult or impossible

to create the message if the message digest is given.

A) one-wayness
B) weak-collision-resistance
C) strong-collision-resistance
D) none of the above

25. A(n) _____ is a hierarchical system that answers queries about key certification.

A) KDC
B) PKI
C) CA
D) none of the above

26. _____ means that a sender must not be able to deny sending a message that he sent.

A) Confidentiality
B) Integrity
C) Authentication
D) Nonrepudiation

27. A hash function must meet _____ criteria.

A) two
B) three
C) four
D) none of the above

28. _____ is a popular session key creator protocol that requires an authentication server and a ticket-granting server.

A) KDC
B) Kerberos
C) CA
D) none of the above

29. Password-based authentication can be divided into two broad categories: _____ and _____.

A) fixed; variable
B) time-stamped; fixed
C) fixed; one-time
D) none of the above