CWIPEDIA.IN

Network and Information Security

MCQ Question Bank

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

Answer: Option B

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

Answer: Option C

3. A(n) _________function creates a message digest out of a message.

A) encryption

B) decryption

C) hash

D) none of the above

Answer: Option C

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

Answer: Option B

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

Answer: Option B

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

Answer: Option A

7. A witness used in entity authentication is _____________.

A) something known

B) something possessed

C) something inherent

D) all of the above

Answer: Option D

8. A ________ message digest is used as an MDC.

A) keyless

B) keyed

C) either (a) or (b)

D) neither (a) nor (b)

Answer: Option A

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

Answer: Option B

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

Answer: Option B

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)

Answer: Option A

12. If __________ is needed, a cryptosystem must be applied over the scheme.

A) integrity

B) confidentiality

C) nonrepudiation

D) authentication

Answer: Option B

13. Digital signature provides _________.

A) authentication

B) nonrepudiation

C) both (a) and (b)

D) neither (a) nor (b)

Answer: Option C

14. Digital signature cannot provide ________ for the message.

A) integrity

B) confidentiality

C) nonrepudiation

D) authentication

Answer: Option B

15. To authenticate the data origin, one needs a(n) _______.

A) MDC

B) MAC

C) either (a) or (b)

D) neither (a) nor (b)

Answer: Option 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

Answer: Option A

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

Answer: Option D

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

Answer: Option C

19. A digital signature needs a(n)__________ system.

A) symmetric-key

B) asymmetric-key

C) either (a) or (b)

D) neither (a) nor (b)

Answer: Option 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

Answer: Option C

21. Message _________ means that the sender and the receiver expect privacy.

A) confidentiality

B) integrity

C) authentication

D) none of the above

Answer: Option A

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)

Answer: Option 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

Answer: Option B

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

Answer: Option A

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

A) KDC

B) PKI

C) CA

D) none of the above

Answer: Option C

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

Answer: Option D

27. A hash function must meet _________ criteria.

A) two

B) three

C) four

D) none of the above

Answer: Option B

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

Answer: Option B

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

Answer: Option C

30. __________ operates in the transport mode or the tunnel mode.

A) IPSec

B) SSL

C) PGP

D) none of the above

Answer: Option A

31. IKE creates SAs for ______.

A) SSL

B) PGP

C) IPSec

D) VP

Answer: Option C

32. _______ provides either authentication or encryption, or both, for packets at the IP level.

A) AH

B) ESP

C) PGP

D) SSL

Answer: Option B

33. One security protocol for the e-mail system is _________.

A) IPSec

B) SSL

C) PGP

D) none of the above

Answer: Option C

34. Typically, ______ can receive application data from any application layer protocol, but the protocol is normally HTTP.

A) SSL

B) TLS

C) either (a) or (b)

D) both (a) and (b)

Answer: Option D

35. IKE is a complex protocol based on ______ other protocols.

A) two

B) three

C) four

D) five

Answer: Option B

36. IPSec defines two protocols: _______ and ________.

A) AH; SSL

B) PGP; ESP

C) AH; ESP

D) all of the above

Answer: Option C

37. In the ______ mode, IPSec protects information delivered from the transport layer to the network layer.

A) transport

B) tunnel

C) either (a) or (b)

D) neither (a) nor (b)

Answer: Option A

38. ______ is the protocol designed to create security associations, both inbound and outbound.

A) SA

B) CA

C) KDC

D) IKE

Answer: Option D

39. A ________network is used inside an organization.

A) private

B) public

C) semi-private

D) semi-public

Answer: Option A

40. SSL provides __________.

A) message integrity

B) confidentiality

C) compression

D) all of the above

Answer: Option D

41. The Internet authorities have reserved addresses for ________.

A) intranets

B) internets

C) extranets

D) none of the above

Answer: Option D

42. An __________ is a network that allows authorized access from outside users.

A) intranet

B) internet

C) extranet

D) none of the above

Answer: Option C

43. __________ is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level.

A) IPSec

B) SSL

C) PGP

D) none of the above

Answer: Option A

44. IKE uses ________.

A) Oakley

B) SKEME

C) ISAKMP

D) all of the above

Answer: Option D

45. IPSec uses a set of SAs called the _________.

A) SAD

B) SAB

C) SADB

D) none of the above

Answer: Option C

46. An _________ is a private network that uses the Internet model.

A) intranet

B) internet

C) extranet

D) none of the above

Answer: Option A

47. _______ is actually an IETF version of ______.

A) TLS; TSS

B) SSL; TLS

C) TLS; SSL

D) SSL; SLT

Answer: Option C

48. In _______, there is a single path from the fully trusted authority to any certificate.

A) X509

B) PGP

C) KDC

D) none of the above

Answer: Option A

49. The combination of key exchange, hash, and encryption algorithms defines a _________ for each SSL session.

A) list of protocols

B) cipher suite

C) list of keys

D) none of the above

Answer: Option B

50. A _______ provides privacy for LANs that must communicate through the global Internet.

A) VPP

B) VNP

C) VNN

D) VPN

Answer: Option D

51. ________ uses the idea of certificate trust levels.

A) X509

B) PGP

C) KDC

D) none of the above

Answer: Option B

52. IPSec in the _______ mode does not protect the IP header.

A) transport

B) tunnel

C) either (a) or (b)

D) neither (a) nor (b)

Answer: Option A

53. _________ provides privacy, integrity, and authentication in e-mail.

A) IPSec

B) SSL

C) PGP

D) none of the above

Answer: Option C

54. In ______, there can be multiple paths from fully or partially trusted authorities.

A) X509

B) PGP

C) KDC

D) none of the above

Answer: Option B

55. _______ provides authentication at the IP level.

A) AH

B) ESP

C) PGP

D) SSL

Answer: Option A

56. In ________, the cryptographic algorithms and secrets are sent with the message.

A) IPSec

B) SSL

C) TLS

D) PGP

Answer: Option D

57. _______ is designed to provide security and compression services to data generated from the application layer.

A) SSL

B) TLS

C) either (a) or (b)

D) both (a) and (b)

Answer: Option D

58. ________ provide security at the transport layer.

A) SSL

B) TLS

C) either (a) or (b)

D) both (a) and (b)

Answer: Option D

59. The ________ mode is normally used when we need host-to-host (end-to-end) protection of data.

A) transport

B) tunnel

C) either (a) or (b)

D) neither (a) nor (b)

Answer: Option A

60. In the ________ mode, IPSec protects the whole IP packet, including the original IP header.

A) transport

B) tunnel

C) either (a) or (b)

D) neither (a) nor (b)

Answer: Option B

61. _______ was invented by Phil Zimmerman.

A) IPSec

B) SSL

C) PGP

D) none of the above

Answer: Option C

62. A ________ layer security protocol provides end-to-end security services for applications.

A) data link

B) network

C) transport

D) none of the above

Answer: Option C

63. In PGP, to exchange e-mail messages, a user needs a ring of ________ keys.

A) secret

B) public

C) either (a) or (b)

D) both (a) and (b)

Answer: Option B