

20 Network Security MCQ For IBPS IT Officer Exam

1)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

2)IKE creates SAs for _____.

- A)SSL
- B)PGP
- C)IPSec
- D)VP

3) _____ provides either authentication or encryption, or both, for packets at the IP level.

- A)AH
- B)ESP
- C)PGP
- D)SSL

4)One security protocol for the e-mail system is _____.

- A)IPSec
- B)SSL
- C)PGP
- D)none of the above

5)IPSec defines two protocols: _____ and _____.

- A) AH; SSL
- B) PGP; ESP
- C) AH; ESP
- D) all of the above

6) A modern cipher is usually a complex _____cipher made of a combination of different simple ciphers.

- A)round
- B)circle
- C)square
- D)none of the above

7)_____ is the protocol designed to create security associations, both inbound and outbound.

- A)SA
- B)CA
- C)KDC
- D)IKE

8)The Internet authorities have reserved addresses for _____.

- A)intranets
- B)internets
- C)extranets
- D)none of the above

9) An _____ is a network that allows authorized access from outside users.

- A)intranet
- B)internet
- C)extranet
- D)none of the above

10) _____ 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

11) 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

12)A _____ provides privacy for LANs that must communicate through the global Internet.

A)VPP

B)VNP

C)VNN

D)VPN

13)IPSec in the _____ mode does not protect the IP header.

A)transport

B)tunnel

C)either (a) or (b)

D)neither (a) nor (b)

14) In _____, the cryptographic algorithms and secrets are sent with the message.

A)IPSec

B)SSL

C)TLS

D)PGP

15)A _____ layer security protocol provides end-to-end security services for applications.

A)data link

B)network

C)transport

D)none of the above

16) 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)

17)The _____ method provides a one-time session key for two parties.

- A) Diffie-Hellman
- B) RSA
- C) DES
- D) AES

18) _____ is a round cipher based on the Rijndael algorithm that uses a 128-bit block of data.

- A) AEE
- B) AED
- C) AER
- D) AES

19) AES has _____ different configurations.

- A) two
- B) three
- C) four
- D) five

20) DES uses a key generator to generate sixteen _____ round keys.

- A) 32-bit
- B) 48-bit
- C) 54-bit
- D) 42-bit

[Click Here For Answers](#)

[Network Security MCQ-1](#)

- 1) Network layer firewall has two sub-categories as
a) stateful firewall and stateless firewall

- b) bit oriented firewall and byte oriented firewall
- c) frame firewall and packet firewall
- d) none of the mentioned

2) An..... is a trusted third party that assigns a symmetric key to two parties

- a) KDC
- b) CA
- c) KDD
- d) None of the above

3)..... 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

4) The secret key between members needs to be created as akey when two members contact KDC.

- a) public
- b) session
- c) complimentary
- d) none of the above

5) An..... can be used to reserve the integrity of a document or a message

- a) message digest
- b) message summary
- c) encrypted message
- d) none of the above

6) Message..... means that the data must arrive at the receiver exactly as sent.

- a) confidentiality
- b) integrity
- c) authentication
- d) none of the above

7)A digital signature needs ansystem

- a)symmetric key
- b)asymmetric key
- c)either a or b
- d)neither a or b

8)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

9)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
- e)none of the above

10)To authenticate the data origin, one needs an.....

- a)MAC
- b)MDC
- c)either a or b
- d)neither a or b

Answers:

- 1)a
- 2)a
- 3)b
- 4)a
- 5)a
- 6)b
- 7)b
- 8)b
- 9)c

10) a