From the CISSP and SSCP Open Study GROUP Online Quizzer

1. PGP uses which of the following to encrypt data?
   a) An asymmetric key distribution
   b) An asymmetric scheme
   c) A symmetric key distribution system
   d) A symmetric scheme

2. Which of the following algorithms is used today for encryption in PGP?
   a) RSA
   b) Blowfish
   c) RC5
   d) IDEA

3. Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?
   a) Digital watermarking
   b) Steganography
   c) Digital signature
   d) Digital enveloping

4. Which of the following keys has the shortest lifespan?
   a) Private key
   b) Session key
   c) Public key
   d) Secret key

5. Secure Sockets Layer (SSL) provides security services at which layer of the OSI model?
   a) Session Layer
   b) Network Layer
   c) Transport Layer
   d) Application Layer

6. Which of the following is *NOT* a symmetric key algorithm?
   a) Blowfish
   b) RC5
   c) Digital Signature Standard (DSS)
   d) Triple DES (3DES)

7. What encryption algorithm is best suited for communication with handheld wireless devices?
   a) RC4

b) ECC
c) SHA
d) RSA

8. Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?
a) Key Exchange Algorithm
b) Security Association Authentication Protocol
c) Simple Key-management for Internet Protocols
d) IPsec Key exchange

9. In which phase of IKE protocol (IPsec) is peer authentication performed?
a) Pre Initialization Phase
b) No peer authentication performed
c) Phase 2
d) Phase 1

10. Which of the following threats is not addressed by digital signature and token technologies?
a) spoofing
b) password compromise
c) denial-of-service
d) replay attacks

11. Which of the following concerning the Rijndael block cipher algorithm is false?
a) The design of Rijndael was strongly influenced by the design of the block cipher Square.
b) The cipher has a variable block length and key length.
c) Both block and key length can be extended to multiples of 64 bits.
d) A total of nine combinations of key length and block length are possible

12. Which of the following techniques is used in the encryption of data between a web browser and server?
a) Kerberos
b) IPSec
c) SSL
d) PGP

13. Which of the following best provides e-mail message authenticity and confidentiality?
a) Signing the message using the sender's private key and encrypting the message using the receiver's public key
b) Signing the message using the receiver's public key and encrypting the message using the sender's private key

c) Signing the message using the receiver's private key and encrypting the message using the sender's public key
d) Signing the message using the sender's public key and encrypting the message using the receiver's private key

14. Which of the following is not an encryption algorithm?
a) SHA-1
b) DEA
c) Twofish
d) Skipjack

15. What is the result of a hash algorithm being applied to a message ?
a) A digital signature
b) A ciphertext
c) A message digest
d) A plaintext

16. Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?
a) Differential cryptanalysis
b) Birthday attack
c) Differential linear cryptanalysis
d) Statistical attack

17. Which of the following statements pertaining to link encryption is false?
a) User information, header, trailers, addresses and routing data that are part of the packets are encrypted.
b) It provides protection against packet sniffers and eavesdroppers.
c) Information stays encrypted from one end of its journey to the other.
d) It encrypts all the data along a specific communication path.

18. Why is public key cryptography recommended for use in the process of securing facsimiles during transmission?
a) The key is securely passed to the receiving machine.
b) Key data is not recognizable from facsimile data.
c) Data compression decreases key change frequency.
d) Keys are never transmitted over the network.

19. What algorithm was DES derived from?
a) Skipjack
b) Twofish
c) Lucifer
d) Brooks-Aldeman

20. What kind of Encryption technoloy VeriSIGN's SSL utilize?
a) Secret key

b) Public Key
c) Hybrid: Symmetric and asymmetric cryptography
d) Asymmetric key

21. What is the role of IKE within the IPsec protocol?
a) data encryption
b) peer authentication and key exchange
c) data signature
d) enforcing quality of service

22. What is the effective key size of DES?
a) 1024 bits
b) 56 bits
c) 64 bits
d) 128 bits

23. What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?
a) Untrusted certificate list
b) Certificate revocation tree
c) Certificate revocation list
d) Authority revocation list

24. Which of the following statements is true about data encryption as a method of protecting data?
a) It makes few demands on system resources.
b) It requires careful key management.
c) It is usually easily administered.
d) It verifies the accuracy of the data.

25. What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?
a) Key collision
b) Hashing
c) Ciphertext collision
d) Key clustering