QUESTIONS Q

1. Which of the following describes the major difference between SSL and S-HTTP?
   - A. SSL operates at the network layer, and S-HTTP operates at the application layer.
   - B. SSL operates at the application layer, and S-HTTP operates at the network layer.
   - C. SSL operates at the transport layer, and S-HTTP operates at the application layer.
   - D. SSL operates at the application layer, and S-HTTP operates at the transport layer.
2. Which of the following would be the best choice to guarantee the integrity of messages in transit or storage?
   - A. Block cipher
   - B. Symmetric algorithm
   - C. Asymmetric algorithm
   - D. Hash algorithm
3. Which of the following are true regarding a PKI system? (Choose two.)
   - A. The CA encrypts all messages.
   - B. The CA is the trusted root that issues certificates.
   - C. The CA is the recovery agent for lost certificates.
   - D. The RA verifies an applicant to the system.
   - E. The RA issues all certificates.
   - F. The RA encrypts all messages.
4. A person approaches a network administrator and wants advice on how to send encrypted e-mail from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following offers a method for sending encrypted e-mail without having to pay for license fees or to manage a server?
   - A. IP Security (IPSec)
   - B. Multipurpose Internet Mail Extensions (MIME)
   - C. Pretty Good Privacy (PGP)
   - D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

5. Which of the following encryption algorithms is your best choice if your primary need is bulk encryption and you need fast, strong encryption?

   A. AES

   B. ECC

   C. RSA

   D. MD5

6. You're describing a basic PKI system to a new member of the team. He asks how the public key can be distributed within the system in an orderly, controlled fashion so that the users can be sure of the sender's identity. Which of the following would be your answer?

   A. Digital signature

   B. Hash value

   C. Private key

   D. Digital certificate

   E. Nonrepudiation

7. You are discussing hash values with a CEH instructor. Immediately after telling you the hash is a one-way algorithm and cannot be reversed, he explains that you can still discover the value entered into the hash, given enough time and resources. Which of the following hash anomalies might allow this?

   A. L0phtCrack

   B. Hash value compromise

   C. Chosen plain text

   D. Collision

8. What is the standard format for digital certificates?

   A. X.500

   B. X.25

   C. XOR

   D. X.509

9. An organization is concerned about corporate espionage and has evidence suggesting an internal employee has been communicating trade secrets to a competitor. After some investigation, the employee trading secrets was identified. Monitoring of the employee's previous communications outside the company revealed nothing out of the ordinary, save for some large unencrypted e-mails

containing image files of humorous pictures to external addresses. Which of the following is the most logical conclusion based on these facts?

A. E-mail encryption allowed the user to hide files.

B. The user hid information in the image files using steganography.

C. Logical watermarking of images and e-mails fed the sensitive files piece by piece to the competitor.

D. SMTP transport fuzzing was used.

10. A hacker has gained access to several files. Many are encrypted, but one is not, and it happens to be an unencrypted version of an encrypted file. Which of the following is the best choice for possibly providing a successful break into the encrypted files?

A. Cipher text only

B. Known plain text

C. Chosen cipher text

D. Replay

11. You are discussing a steganography tool that takes advantage of the nature of "white space" to conceal information. Which tool are you referring to?

A. Snow

B. GifShuffle

C. White Wipe

D. Tripwire

12. At the basic core of encryption approaches, two main methods are in play: substitution and transposition. Which of the following best describes transposition?

A. Bits are replaced with a different value.

B. Bits are removed.

C. The order of bits is changed.

D. The parity bits are changed.

13. Jack and Jill work in an organization that has a PKI system in place for securing messaging. Jack encrypts a message for Jill and sends it on. Jill receives the message and decrypts it. Within a PKI system, which of the following statements is true?

A. Jack encrypts with his private key. Jill decrypts with her private key.

B. Jack encrypts with his public key. Jill decrypts with her public key.

C. Jack encrypts with Jill's private key. Jill decrypts with her public key.

D. Jack encrypts with Jill's public key. Jill decrypts with her private key.

14. Which of the following would you find in an X.509 digital certificate? (Choose all that apply.)

A. Version

B. Algorithm ID

C. Private key

D. Public key

E. Key usage

F. PTR record

15. Which of the following is a secure substitute for Telnet?

A. SHA-1

B. RSA

C. SSL

D. SSH

16. An SSL session requires a client and a server to handshake information between each other and agree on a secured channel. Which of the following best describes the session key creation during the setup of an SSL session?

A. The server creates the key after verifying the client's identity.

B. The server creates the key immediately on the client connection.

C. The client creates the key using the server's public key.

D. The client creates the key after verifying the server's identity.

17. Which encryption algorithm uses variable block sizes (from 32 to 128 bits)?

A. SHA-1

B. RC5

C. 3DES

D. AES

18. Which hash algorithm was developed by the NSA and produces output values up to 512 bits?

A. MD5

B. SHA-1

C. SHA-2

D. SSL

19. A hacker is attempting to uncover the key used in a cryptographic encryption scheme. Which attack vector is the most resource intensive and usually takes the longest amount of time?

    A. Social engineering

    B. Known plain text

    C. Frequency analysis

    D. Brute force

20. Which of the following best describes session key creation in SSL?

    A. It is created by the server after verifying the user's identity.

    B. It is created by the server as soon as the client connects.

    C. It is created by the client using the server's public key.

    D. It is created by the client after verifying the server's identity.

21. In a discussion on symmetric encryption, a friend mentions that one of the drawbacks with this system is scalability. He goes on to say that for every person you add to the mix, the number of keys increases dramatically. If seven people are in a symmetric encryption pool, how many keys are necessary?

    A. 7

    B. 14

    C. 21

    D. 28

22. Which of the following is a true statement?

    A. Symmetric encryption scales easily and provides for nonrepudiation.

    B. Symmetric encryption does not scale easily and does not provide for nonrepudiation.

    C. Symmetric encryption is not suited for bulk encryption.

    D. Symmetric encryption is slower than asymmetric encryption.

23. The PKI system you are auditing has a certificate authority (CA) at the top that creates and issues certificates. Users trust each other based on the CA. Which trust model is in use here?

    A. Stand-alone CA

    B. Web of trust

    C. Single authority

    D. Hierarchical trust

24. A portion of a digital certificate is shown here:

```
Version                    V3
Serial Number              26 43 03 62 e9 6b 39 a4 9e 15 00 c7 cc 21 a2 20
Signature Algorithm        sha1RSA
Signature Hash Algorithm   sha1
Issuer                     VeriSign Class 3 Secure Server
Valid From                 Monday, October 17, 2011 8:00 PM
Valid To                   Wednesday, October 17, 2012 7:59:59 PM
.
Public Key                 RSA (2048)
.
```

Which of the following statements is true?

A. The hash created for the digital signature holds 160 bits.

B. The hash created for the digital signature holds 2,048 bits.

C. RSA is the hash algorithm used for the digital signature.

D. This certificate contains a private key.

25. Two bit strings are run through an XOR operation. Which of the following is a true statement for each bit pair regarding this function?

A. If the first value is 0 and the second value is 1, then the output is 0.

B. If the first value is 1 and the second value is 0, then the output is 0.

C. If the first value is 0 and the second value is 0, then the output is 1.

D. If the first value is 1 and the second value is 1, then the output is 0.

26. Which of the following attacks attempts to re-send a portion of a cryptographic exchange in hopes of setting up a communications channel?

A. Known plain text

B. Chosen plain text

C. Man in the middle

D. Replay

27. Within a PKI system, which of the following is an accurate statement?

A. Bill can be sure a message came from Sue by using his public key to decrypt it.

B. Bill can be sure a message came from Sue by using his private key to decrypt it.

C. Bill can be sure a message came from Sue by using her private key to decrypt the digital signature.

D. Bill can be sure a message came from Sue by using her public key to decrypt the digital signature.

28. Which of the following could be considered a drawback to using AES with a 256-bit key to share sensitive data?

    A. The key size requires a long time to encrypt and decrypt messages.

    B. It's a complex algorithm that requires intense system configuration.

    C. AES is a weak cypher.

    D. Each recipient must receive the key through a different channel than the message.

29. One use of hash algorithms is for the secure storage of passwords: The password is run through a one-way hash, and the value is stored instead of the plain-text version. If a hacker gains access to these hash values and knows the hash algorithm used to create them, which of the following could be used to speed up his effort in cracking them?

    A. Salt

    B. Rainbow tables

    C. Steganography

    D. Collision