Câu hỏi **1**

**Which of the following is BEST used as a secure replacement for TELNET?**

a. SSH

b. GPG

c. HMAC

d. HTTPS

The correct answer is: SSH

Câu hỏi **2**

**A system administrator is setting up a file transfer server. The goal is to encrypt the user authentication and the files the user is sending using only a user ID and a key pair. Which of the following methods would achieve this goal?**

a. AES

b. PGP

c. SSH

d. IPSec

The correct answer is: SSH

-> With SSH you can use automatically generated public-private key pairs to encrypt a network connection, and then use password authentication to log on. Or you can use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password.

Câu hỏi **3**

How many keys are required to fully implement a symmetric algorithm with 10  
participants?

a. 10

b. 100

c. 20

d. 45

Câu hỏi **4**

What is the length of the cryptographic key used in the Data Encryption Standard  
(DES) cryptosystem?

a. 56 bits

b. 192 bits

c. 256 bits

d. 128 bits

Câu hỏi **5**

**A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:**

a. Integrity of downloaded software.

b. Integrity of the server logs.

c. Confidentiality of downloaded software.

d. Availability of the FTP site.

-> Digital Signatures is used to validate the integrity of the message and the sender. In this case the software firm that posted the patches and updates digitally signed the checksums of all patches and updates.

Câu hỏi **6**

**Which of the following are restricted to 64-bit block sizes? (Select TWO).**

a. RSA

b. AES

c. AES256

d. 3DES

e. PGP

f. DES

The correct answers are: DES, 3DES

Câu hỏi **7**

**Digital signatures are used for ensuring which of the following items? (Select TWO).**

a. Non-Repudiation

b. Availability

c. Integrity

d. Confidentiality

e. Algorithm strength

Câu hỏi **8**

**An SSL session is taking place. After the handshake phase has been established and the cipher has been selected, which of the following are being used to secure data in transport? (Select TWO)**

a. Diffie-Hellman

b. Symmetrical encryption

c. Ephemeral Key generation

d. Asymmetrical encryption

e. RSA

f. AES

Câu hỏi **9**

**Which of the following concepts is used by digital signatures to ensure integrity of the data?**

a. Hashing

b. Key escrow

c. Non-repudiation

d. Transport encryption

Câu hỏi **10**

**Which of the following is used to verify data integrity?**

a. RSA

b. AES

c. SHA

d. 3DES

Câu hỏi **11**

**Symmetric encryption utilizes \_\_\_\_\_\_\_\_\_\_, while asymmetric encryption utilizes \_\_\_\_\_\_\_\_\_.**

a. Private keys, session keys

b. Public keys, one time

c. Private keys, public keys

d. Shared keys, private keys

Câu hỏi **12**

**Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO).**

a. The CA’s public key

b. Ann’s private key

c. Joe’s private key

d. Ann’s public key

e. Joe’s public key

f. The CA’s private key

Câu hỏi **13**

How many encryption keys are required to fully implement an asymmetric algorithm with 10 participants?

a. 20

b. 10

c. 45

d. 100

Câu hỏi **14**

**Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?**

a. Digital Signature

b. Session Key

c. Private Key

d. Public Key

Câu hỏi **15**

**Joe must send Ann a message and provide Ann with assurance that he was the actual sender. Which of the following will Joe need to use to BEST accomplish the objective?**

a. Ann’s public key

b. A pre-shared private key

c. His public key

d. His private key

Câu hỏi **16**

**Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?**

a. Recipient’s private key

b. Sender’s public key

c. Sender’s private key

d. Recipient’s public key

Câu hỏi **17**

**A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel. Which of the following MUST be implemented?**

a. SHA-256

b. Diffie-Hellman

c. 3DES

d. AES

Câu hỏi **18**

**Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?**

a. Hashing

b. Encryption

c. Steganography

d. Digital Signatures

Câu hỏi **19**

**An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?**

a. Confidentiality

b. Availability

c. Remediation

d. Integrity

Câu hỏi **20**

**Which of the following is true about asymmetric encryption?**

a. A message encrypted with the public key can be decrypted with a shared key.

b. A message encrypted with a shared key, can be decrypted by the same key.

c. A message encrypted with the public key can be decrypted with the private key

d. A message encrypted with the private key can be decrypted by the same key

Câu hỏi **21**

**Digital certificates can be used to ensure which of the following? (Select TWO).**

a. Authorization

b. Non-repudiation

c. Verification

d. Availability

e. Confidentiality

Câu hỏi **22**

**Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?**

a. Certificate revocation list

b. Key escrow

c. Certification authority

d. Registration authority

Câu hỏi **23**

**Protecting the confidentiality of a message is accomplished by encrypting the message with which of the following?**

a. Sender’s private key

b. Recipient’s private key

c. Recipient’s public key

d. Sender’s public key

Câu hỏi **24**

**An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?**

a. Blowfish

b. DSA

c. 3DES

d. Diffie-Hellman

e. DES

Câu hỏi **25**

**Digital certificates can be used to ensure which of the following? (Select TWO)**

a. Availability

b. Verification

c. Non-repudiation

d. Authorization

e. Confidentiality

Câu hỏi **26**

**Which of the following provides additional encryption strength by repeating the encryption process with additional keys?**

a. 3DES

b. Blowfish

c. TwoFish

d. AES

Câu hỏi **27**

**A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user’s digital certificate. Which of the following will help resolve the issue? (Select TWO).**

a. Restore the certificate using a CRL

b. Issue a new digital certificate

c. Mark the key as private and import it

d. Restore the certificate using a recovery agent

e. Revoke the digital certificate

Câu hỏi **28**

**Which of the following symmetric key algorithms are examples of block ciphers? (Select Two).**

a. AES

b. MD5

c. 3DES

d. RC4

e. PGP

Câu hỏi **29**

Which one of the following cannot be achieved by a secret key cryptosystem?

a. Key distribution

b. Availability

c. Confidentiality

d. Nonrepudiation

Câu hỏi **30**

**Which of the following uses both a public and private key?**

a. RSA

b. AES

c. SHA

d. MD5

ĐÁP ÁN

              