

1. You are responsible for security at a hospital. Since many computers are accessed by multiple employees 24 hours a day, 7 days a week, controlling physical access to computers is very difficult. This is compounded by a high number of non employees moving through the building. You are concerned about unauthorized access to patient records.

What would best solve this problem?

- A. The use of CHAP
- B. Time of day restrictions
- C. The use of smart cards
- D. Video surveillance of all computers

Answer: C

2. In which of the following cryptographic attacking techniques does the attacker pick up the information to be encrypted and take a copy of it with the encrypted data?

- A. Chosen ciphertext attack
- B. Known plaintext attack
- C. Hidden text attack
- D. Ciphertext only attack

Answer: B

3. Which of the following are the goals of a public key infrastructure (PKI)? Each correct answer represents a part of the solution. Choose all that apply.

- A. Authenticity
- B. Globalization
- C. Mobility
- D. Integrity
- E. Confidentiality
- F. Nonrepudiation

Answer: A,D,E,F

4. In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

- A. Initiation
- B. Programming and training
- C. Design
- D. Evaluation and acceptance

Answer: B

5. You are the administrator for YupNo.com. You want to increase and enhance the security of your computers and simplify deployment. You are especially concerned with any portable computers that are used by remote employees. What can you use to increase security, while still allowing your users to perform critical tasks?

- C. Service Accounts
- D. AppLocker

Answer: B

6. You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? Each correct answer represents a complete solution. Choose two.

- A. MAC filtering the router
- B. Not broadcasting SSID
- C. Using WEP encryption
- D. Using WPA encryption

Answer: C,D

7. Which of the following protocols provides the highest level of VPN security with a VPN connection that uses the L2TP protocol?

- A. IPSec
- B. PPPoE
- C. PPP
- D. TFTP

Answer: A

8. Which of the following encryption methods comes under symmetric encryption algorithm? Each correct answer represents a complete solution. Choose three.

- A. DES
- B. Blowfish
- C. RC5
- D. Diffie-Hellman

Answer: A,B,C

9. An access control secures the confidentiality, integrity, and availability of the information and data of an organization. In which of the following categories can you deploy the access control? Each correct answer represents a part of the solution. Choose all that apply.

- A. Detective access control
- B. Corrective access control
- C. Administrative access control
- D. Preventive access control

Answer: A,B,D

10. You are the Network Administrator for a bank. In addition to the usual security issues, you are concerned that your customers could be the victim of phishing attacks that use fake bank Web sites. Which of the following would protect against this?

- A. MAC
- B. Mutual authentication
- C. Three factor authentication

Answer: B