**EXAMPLE QUESTİONS**

1. Define computer security.
2. What is CIA
3. What is the difference between passive and active security threats?
4. List and briefly define categories of passive and active network security attacks.
5. List and briefly define the fundamental security design principles.
6. Explain the difference between an attack surface and an attack tree
7. What are the essential ingredients of a symmetric cipher?
8. How many keys are required for two people to communicate via a symmetric cipher?
9. What are the two principal requirements for the secure use of symmetric encryption?
10. List three approaches to message authentication.
11. What is a message authentication code?
12. Briefly describe the three schemes illustrated in Figure 2.3.
13. What properties must a hash function have to be useful for message authentication?
14. What are the principal ingredients of a public-key cryptosystem?
15. List and briefly define three uses of a public-key cryptosystem.
16. What is the difference between a private key and a secret key?
17. What is a digital signature?
18. What is a public-key certificate?
19. How can public-key encryption be used to distribute a secret key?
20. In general terms, what are four means of authenticating a user's identity?
21. List and briefly describe the principal threats to the secrecy of passwords.
22. What are two common techniques used to protect a password file?
23. List and briefly describe four common techniques for selecting or assigning passwords.
24. Explain the difference between a simple memory card and a smart card.
25. List and briefly describe the principal physical characteristics used for biometric identification.
26. In the context of biometric user authentication, explain the terms, enrollment, verification, and identification.
27. Define the terms false match rate and false nonmatch rate, and explain the use of a threshold in relationship to these two rates.
28. Describe the general concept of a challenge-response protocol
29. Briefly define the difference between DAC and MAC.
30. How does RBAC relate to DAC and MAC?
31. List and define the three classes of subject in an access control system.
32. In the context of access control, what is the difference between a subject and an object?
33. What is an access right?
34. What is the difference between an access control list and a capability ticket?
35. What is a protection domain?
36. Briefly define the four RBAC models of Figure 4.8a.
37. List and define the four types of entities in a base model RBAC system.
38. Describe three types of role hierarchy constraints.
39. In the NIST RBAC model, what is the difference between SSD and DSD?