1. List and briefly define the fundamental security design principles.
2. What are the different security goals? Explain with examples
3. In general terms, what are four means of authenticating a user's identity?
4. List and briefly describe the principal threats to the secrecy of passwords.
5. What are two common techniques used to protect a password file?
6. List and briefly describe four common techniques for selecting or assigning passwords.
7. Explain the difference between a simple memory card and a smart card.
8. List and briefly describe the principal physical characteristics used for biometric identification.
9. In the context of biometric user authentication, explain the terms, enrollment, verification, and identification.
10. Define the terms false match rate and false nonmatch rate, and explain the use of a threshold in relationship to these two rates.
11. Describe the general concept of a challenge-response protocol.
12. Define the following cryptography terms – Plaintext, ciphertext, encryption, decryption, key
13. What are the essential ingredients of a symmetric cipher?
14. How many keys are required for two people to communicate via a symmetric cipher?
15. What are the two principal requirements for the secure use of symmetric encryption?
16. What are the different methods of symmetric encryption?
17. Name the different symmetric encryption algorithms. What are the differences between DES, 3-DES and AES?
18. What is hashing?
19. Define Avalanche effect and Collision attack in the context of hashing
20. What are the differences between hashing and encryption?
21. What properties must a hash function have to be useful for message authentication?
22. What are the principal ingredients of a public-key cryptosystem?
23. List and briefly define three uses of a public-key cryptosystem.
24. What is a digital signature? Describe how hashing is used to achieve non-repudiation?
25. How can public-key encryption be used to distribute a secret key?

26. Revise problems on public-key cryptography (calculate public key, private key, encryption and decryption), Difffie-hellman key exchange