1) Using the keywords “good, bad, input, output” clearly distinguish between accuracy and security within the context of computer systems.
2) Clearly distinguish the following concepts in the context of computer security: Threat, Vulnerability and exploits. Give an example that outlines each of them.
3) What is a Botnet? Use a clearly labeled diagram to illustrate the life cycle of a Botnet.
4) Distinguish between malware and Ransomware. Give an example of each.
5) Data Encryption Standard (DE/S) is an example of Symmetric Key Cryptographic algorithm.
   a. What is Symmetric Key Cryptography?
   b. How many rounds are supported by DES encryption?
   c. What is the Key Size in DES encryption?
   d. What is the Block Size in DES encryption?
   e. In what ways is DES considered weak?
6) What is PKI?
7) What is the purpose of PKI?
8) Distinguish between Block and Stream Ciphers
9) CBC is one example of block ciphers.
   a. What is CBC mode of encryption?
   b. What is IV in the context of CBC?
   c. What is the problem with a fixed IV?
   d. Explain any of the general attacks against block ciphers

10) Describe a Feistel structure.
11) Distinguish between a Digital Signature and a Digital Certificate.
12) Explain how Diffie Hellman Key exchange is implemented in RSA cryptosystem.
13) In the context of Hashing:
    a. Explain what it means when it is said that a function H has a “pre-image” resistance.
    b. Describe HMAC and how it is used.

14) Distinguish between authentication and authorization.
15) Explain what is meant by Kerberos authentication scheme.
16) Explain what is meant by Kerberos realm.
17) Describe Needham-Schroeder Protocol.
18) What is a Stateful Packet Inspection Firewall?