Duration: 3hrs   [Max Marks:80]

N.B. : (1) Question No 1 is Compulsory.
       (2) Attempt any three questions out of the remaining five.
       (3) All questions carry equal marks.
       (4) Assume suitable data, if required and state it clearly.

1   Attempt any FOUR   [20]

  a   Describe steganography with example.

  b   Write properties of hash functions.

  c   What is Digital Signature? Why digital signatures are required?

  d   List and explain various vulnerabilities in operating system.

  e   Explain penetration testing.

2 a   Explain DES algorithm. What do you mean by double DES and triple DES   [10]

  b   Explain RSA with example.   [10]

3 a   Write a note on user authentication and session management.   [10]

  b   Explain AES algorithm in detail.   [10]

4 a   Explain Needham Schroeder Authentication protocol.   [10]

  b   Explain Hill cipher with suitable example.   [10]

5 a   What are database security requirements? What do you understand by   [10]
      Inference attacks? Explain about multilevel database security.

  b   Differentiate between MD5 and SHA256.   [10]

6 a   Write a note on Digital Certificate: X.509 and Public Key Infrastructure.   [10]

  b   Explain web security in detail.   [10]

_____