QP Code : 26696

(3 Hours)   [total Marks: 80]

N. B.: (1) Question number 1 is compulsory
     (2) Attempt any 4 from question Nos. 2 to 7.
     (3) Illustrate answers with sketches wherever necessary.

1. A] Define Network Security. What are the services and mechanisms provided by Network Security?   10
   B] What are the algorithm modes uses for secret key cryptography?   10

2. A] Explain in details on DES algorithm with reference to its overview and a DES round.   08
   B] What do you mean by Hash function? Compare the terms SHA1 and MD5.   07

3. A] Explain RSA algorithm with a suitable example.   08
   B] Write an algorithm of Diffie – Hellman Key distribution and explain the concept of Man – in – the – Middle attack with proper numerical example.   07

4. A] What are the various forms of Authentication? Explain in details.   08
   B] Explain KDC. How does the key distribution work with multiple KDC domains?   07

5. A] How are Kerberos ticket lifetimes in V5 different from V4?   08
   B] Discuss Inter – realm authentication in Kerberos.   07

6. A] What is a digital certificate? Explain the stepwise process of certificate generation?   08
   B] Explain how SET ensures a secure e – commerce transaction.   07

7. Write short notes on: (any three)   15
      a) Honey Pots
      b) Intrusion Detection and its types
      c) Integrity check
      d) SSL