[Time: Three Hours]   **[Marks:100]**

Please check whether you have got the right question paper.

N.B: 1.   Question No. 1 is compulsory.
         2.   Attempt any four from remaining six questions.
         3.   Illustrate answers with sketches wherever required and use of pencil should be done for drawing sketches.

Q.1   a)   Explain in detail DES algorithm with reference to its overview and a DES round.   **10**
         b)   What is key distribution center? How does the key distribution work with multiple KDC domains?   **10**

Q.2   a)   Explain Diffie Hellman key exchange protocol with a suitable example. How can this Mechanism is   **10**
              foiled by an attacker?   **10**
         b)   Define network security? What are the services and mechanisms provided by network security?

Q.3   a)   Explain RSA with the help of numerical example.   **10**
         b)   Explain different modes of algorithm with diagram.   **10**

Q.4   a)   Explain Kerberos and its working.   **10**
         b)   What is a firewall? Explain different types of firewall.   **10**

Q.5   a)   Explain in detail Email Security.   **10**
         b)   Explain mutual authentication and reflection attack with the help of diagram. Suggest two methods   **10**
              to fix it.

Q.6   a)   What is hash algorithm? Discuss MD4 in detail.   **10**
         b)   What is a digital certificate? Explain stepwise certification generation process.   **10**

Q.7   Write short notes on any four   **20**
         a)   Smart cards
         b)   Digital signature
         c)   Certificate Revocation
         d)   PGP
         e)   IPSec