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   Give examples of replay attacks. List three general approaches for dealing with replay attack.

   b   Explain key rings in PGP.

   c   What are the different protocols in SSL? How do client and server establish SSL connection?

   d   Explain TCP/IP vulnerabilities layer wise.

   e   What is the purpose of S-boxes in DES? Explain the avalanche effect.

2 a   What is need for message authentication? List various techniques used for message authentication. Explain any one.   [10]

   b   What characteristics are needed in secure hash function? Explain secure hash algorithm on 512 bit.   [10]

3 a   Use Hill cipher to encrypt the text "short". The key to be used is hill.   [10]

   b   Explain man in middle attack on Diffie Hellman. Explain how to overcome the same.   [10]

4 a   Explain IPSec protocol in detail. Also write applications and advantages of IPSec.   [10]

   b   What are different types of firewall? How firewall is different from IDS.   [10]

5 a   Explain Kerberos in detail.   [10]

   b   Provide a comparison between HMAC, CBC-MAC and CMAC.   [10]

6 a   What is PKI? List its components.   [10]

   b   What is digital certificate? How does it help to validate authenticity of a user. Explain X.509 certificate format.

****

696BD7FFAEACFB8579E69A4698B09B81