III B.Tech II Semester Regular/Supplementary Examinations,May 2010
Information Security
Computer Science And Engineering

Time: 3 hours   Max Marks: 80
Answer any FIVE Questions
All Questions carry equal marks
⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Explain about the routing applications of IPSec?
   (b) Give the formats of ISAKMP header and Generic payload header? Explain various fields?   [8+8]

2. (a) What are the steps involved in the SSL record protocol transmission?
   (b) Explain the construction and purpose of dual signature?   [8+8]

3. Explain the AES algorithm?   [16]

4. (a) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.
   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides.   [8+8]

5. (a) Discuss the key elements included in the model of network management used for SNMP?
   (b) Explain the functional enhancements made in SNMPV2 over SNMPV1. [8+8]

6. (a) With a neat diagram explain the working principle of packet-filtering router?
   (b) What is a reference monitor? What are the rules that it has to enforce? Discuss its properties?   [8+8]

7. (a) Explain the route table modification vulnerability?
   (b) Explain the security mechanisms?   [8+8]

8. (a) Explain the procedure involved in RSA public-key encryption algorithm?
   (b) Explain what Kerberos is and give its requirements.   [8+8]

⋆ ⋆ ⋆ ⋆ ⋆