Code No: 07A60503 **R07** **Set No. 4**

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. Explain the block cipher modes of operation? [16]
2. (a) List and explain the SET requirements?
   (b) Explain the operations of SSL Record Protocol? [8+8]
3. (a) Explain the principles and limitations of a firewall?
   (b) Statistical anomaly detection
   (c) Application-level gateway. [8+4+4]
4. (a) Explain the buffer overflow attack with an example?
   (b) Explain the format string vulnerability? [8+8]
5. (a) Explain the anti-replay mechanism in IPSec?
   (b) Explain how Diffie-Hellman protocol is vulnerable to man-in-the-middle attack? How is rectified in Oakley protocol? [8+8]
6. (a) What are three broad categories of application of public key cryptosystems?
   (b) i. What requirements must a public key cryptosystem fulfil to be a secure algorithm?
   ii. Describe the approaches of key distribution in public key cryptosystems? [8+8]
7. (a) List and explain the PGP services?
   (b) Draw and explain the transmission and reception of PGP messages? [8+8]
8. (a) Describe the main characteristics of computer virus.
   (b) Write short note on intruder? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆