Code No: R5320504 **R5**

III B.Tech II Semester(R05) Supplementary Examinations, May 2010
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Write about the Route table modification.
   (b) Explain clearly some of the prominent Format string vulnerabilities where they exist and suggest a solution for the same. [8+8]
2. (a) Compare AES cipher versus RC4 encryption algorithm.
   (b) Compare and contrast SHA-1 and HMAC functions. [8+8]
3. (a) Alice, Carol, Dave & Eric are working in an organization with Bob as their Manager. Bob wishes to share some information with his employees. But as the internal attacks are more the employees wish to authenticate sender of the message. What kind of strategy would you suggest for the above situation? Explain the strategy and also highlight the design issues related to the strategy proposed.
   (b) Define Public key cryptography? Explain with a neat illustration. Give merits and demerits of the public key cryptography. [8+8]
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) What are the selectors that determine an SPD entry?
   (b) What is the range of values a sequence number counter in AH can take? Explain its significance in defending replay attacks? [8+8]
6. (a) Give the diagram of SSL record format? Explain how it is formed?
   (b) Mention the alerts in SSLV3 that are always fatal? [10+6]
7. (a) Discuss in detail firewall characteristics?
   (b) Explain the techniques that detect intrusion by observing events in the system and applying a set of rules? [6+10]
8. (a) What is the disadvantage of a screened host firewall, single-homed bastion? Suggest a solution for it?
   (b) Explain in detail about statistical anomaly detection? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆