Code :R5320504 **R5**

III B.Tech II Semester(R05) Supplementary Examinations, April/May 2011
INFORMATION SECURITY
(Computer Science & Engineering)

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

Answer any FIVE questions
All questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Explain about the Security Mechanisms.
   (b) Explain TCP session hijacking with Packet Blocking.
2. (a) Explain the use of S-Boxes in AES algorithm.
   (b) Differentiate between DES and AES algorithms.
   (c) Enumerate the various cipher block modes of operation.
3. (a) Explain the procedure involved in RSA public-key encryption algorithm.
   (b) Explain what Kerberos is and give its requirements.
4. (a) Explain clearly with relevant illustration how authentication is addressed in PGP.
   (b) Explain how the exchange of secret key takes place between 'X' and 'Y' users of S/MIME.
5. (a) The IPSec architecture document states that when two transport mode SAs are bounded to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate. Performing the ESP protocol before performing the AH protocol. Why this approach is recommended rather authentication before encryption?
   (b) Discuss the advantages and disadvantages of Diffie-Helman key exchange protocol? What is the specific key exchange algorithm mandated for use in the initial version of ISAKMP
6. (a) Explain how web security threats are classified in terms of the location of the threat?
   (b) What are SSL session and SSL connection? What parameters define SSL session and SSL connection?
7. (a) With a neat figure explain how the various tables in the VACM MIB come into play in making the access control decision.
   (b) Explain in detail the password selection strategies.
8. Discuss firewall design principles in detail.

⋆ ⋆ ⋆ ⋆ ⋆