Code No: 9A05709/R09

Set-4

III B.Tech. II Semester Regular and Supplementary Examinations

April/May -2013

INFORMATION SECURITY

(Information Technology)

Time: 3 Hours Max. Marks: 70

*Answer any **FIVE** Questions*

***All** Questions carry **equal** marks*

- - -

1. What are the major points of weakness in a computing system? Describe the types of vulnerabilities applied to them.

2. (a) "We do not have techniques to eliminate all program security flaws". Why?

   (b) What qualities of a virus are appealing to the virus writers?

3. (a) What requirements must a public-key cryptosystems fulfill to be a secure algorithm?

   (b) Describe the public-key distribution algorithm where public-key authority is involved.

4. (a) Describe the properties of digital signature.

   (b) Explain the proposal by Needham and Schroeder for secret key distribution.

5. (a) Describe how authentication and confidentiality are handled in S/MIME.

   (b) Explain what Kerberos is and give its requirements.

6. Explain encapsulating security pay load.

7. Explain in detail about SSL record protocol operation.

8. (a) What is an access policy? On what factors does access determination depends? (b) Discuss the two techniques for developing an effective an efficient proactive password checker.