Code: 9A05709

R09

B.Tech IV Year II Semester (R09) Advanced Supplementary Examinations, July 2013

INFORMATION SECURITY

(Common to ECE and ECC)

Time: 3 hours Max. Marks: 70

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) Explain the relationship between a threat, vulnerability and a control.
(b) Compare the following:
(i) Stream and block ciphers.
(ii) Substitution and transposition ciphers.

2 (a) What are the truths and misconception about viruses? Explain.
(b) Explain how viruses attach itself to a program.

3 (a) Describe the public key cryptographic algorithm which is used only for key exchange.
(b) What are the requirements for the use of public-key certificate scheme?

4 (a) Explain the asymmetric encryption approaches for one-way authentication.
(b) List the general approaches to dealing with replay attacks.

5 (a) What are the functions included in MIME in order to enhance security how are they done?
(b) Why does PGP maintain key rings with every user? Explain how the messages are generated and received by PGP.

6 Explain in detail about IP security architecture.

7 (a) With a neat diagram explain SSL record protocol operation.
(b) Discuss about the passive attacks and active attacks in WWW.

8 (a) Define intrusion detection and the different types of detection mechanisms, in detail.
(b) Comment on password selection strategies and their significance.

*****