Code: 9A05709 **R09**

B.Tech IV Year II Semester (R09) Regular & Supplementary Examinations April 2015

INFORMATION SECURITY

(Common to ECE & ECC)

Time: 3 hours Max. Marks: 70

Answer any FIVE questions
All questions carry equal marks

*****

1 (a) Describe the types of vulnerabilities applied to the assets of hardware, software and data.
(b) Define confidentiality and integrity.

2 Write notes on the following:
(a) Code red worm.
(b) Trapdoors.
(c) Salami attacks.

3 (a) Discuss how public-keys are distributed.
(b) Explain diffie-Hellman key exchange algorithm.

4 Write in detail the arbitrated digital signature approaches and direct digital signature approaches in detail.

5 (a) List and explain the technical deficiencies of Kerberos version 4 protocols.
(b) Give the general structure of public key ring maintained by a PGP user and explain each field in detail.

6 (a) Explain authentication header protocol in detail.
(b) Mention any two ISAKMP payload types and describe them.

7 Explain SET in detail.

8 (a) Explain in detail the password selection strategies.
(b) What is a Bastion host? What are its common characteristics?

*****