Code No.: 9A05709/R09

III B.Tech. II Semester Regular and Supplementary Examinations

Set-3

April/May - 2013

INFORMATION SECURITY

(Information Technology)

Time: 3 Hours | Max. Marks: 70

*Answer any **FIVE** Questions*

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

- - -

1. Describe in detail the controls for preserving confidentiality, integrity and availability.

2. (a) Write a detailed note on covert channels.
   (b) Explain how viruses completely replace a program.

3. (a) What is an elliptic curve? What is the zero point of an elliptic curve? What is the sum of three points on an elliptic curve that lie on a straight line?
   (b) List the requirements of MAC. Describe message authentication code based on DES.

4. (a) Why the digital signature is needed?
   (b) Explain the general approaches to deal with replay attacks. Mention where they are suitable.

5. Discuss the following in relation with S/MIME,
   (a) RFC 822
   (b) MIME header fields
   (c) MIME content types.

6. (a) What is the default length of authentication data field? On what fields is it calculated?
   (b) Explain how Diffie-Hellman protocol is vulnerable to man-in-the- middle attack. How is rectified in Oakley

7. (a) What steps are involved in the SSL record protocol transmission?
   (b) What is a dual signature and what is its purpose?

8. (a) What is a firewall? Explain the capabilities that are within the scope of a firewall.
   (b) What are the measures that may be used for intrusion detection?