Code: 9F00404a

MCA IV Semester Regular & Supplementary June 2012 Examinations
INFORMATION SECURITY
(For 2009 & 2010 admitted batches only)

Time: 3 hours   **Max Marks: 60**

Answer any FIVE questions
All questions carry equal marks
*****

1. (a) Explain about security services.
   (b) With a neat diagram explain about internetwork security model.

2. (a) Explain the procedure in AES algorithm.
   (b) Explain about block cipher 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. Clearly explain in detail the Secure Multipurpose Internet Mail Extension (S/MIME).

5. (a) IP Sec Architecture document mandates support for two types of key management. What are they?
   (b) Explain about authentication header.

6. Explain in detail about secure Electronic Transactions (SET) components, Transactions?

7. (a) Explain how proxy accommodates devices that do not implement SNMP?
   (b) Discuss SNMPV1 administrative concepts.

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?

*****