Code: 9F00404a

MCA IV Semester Regular & Supplementary Examinations July 2015

INFORMATION SECURITY

(For students admitted in 2009, 2010, 2011, 2012 and 2013 only)

Time: 3 hours Max Marks: 60

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) Discuss the general model that reflects a concern for protecting an information system from unwanted access.
(b) What criteria are to be met for a specification to become a standard?

2 Draw the overall structure of AES and explain.

3 (a) List key distribution using public key cryptography.
(b) List the design objectives of HMAC.

4 (a) Explain PGP trust model with an example.
(b) What is the difference between signed data and clear signed data?

5 (a) Explain about the routing applications of IPSec.
(b) Explain encapsulating security payload protocol in detail.

6 (a) What services SSL record protocol provides for SSL connections?
(b) Explain how a dual signature is constructed.

7 (a) Under what circumstances a decentralized distributed approach works best. Discuss.
(b) Who is an intruder? Discuss about the intrusion techniques.

8 (a) Explain the general model of access control as exercised by DBMS.
(b) Discuss in detail, two types of proxy based firewalls.

*****