Paper / Subject Code: 56303 / Information security

Friday, May 24, 2019   02:30 pm - 05:30 pm   1T00143 - M.C.A. (Sem. III)(Choice Based) / 56303 - Information
Security.   40272

Q.P. Code: 40272

(3 Hours)   **Total Marks: 80**

Note:
- a) **Question No.1 is compulsory.**
- b) Attempt any three from the remaining five questions.
- c) Answer to sub questions should be answered together.
- d) Illustrate answers with diagrams wherever necessary.
- e) Use of Calculator is allowed.

Q1

A   Explain Diffie-hellman key exchange algorithm with example also discuss   10
     possible attack

B   What is mutual Authentication? Discuss the problem associated with Mutual   10
     Authentication

Q2   A   Analyze the various principles of Security   10
      B   Discus the security services provided in the IEEE 802.11i   10

Q3   A   Discuss Kerberos as a third party authentication System   10
      B   What are firewalls? Explain the various configurations of the firewalls   10

Q4   A   Discuss the various methods of securing the databases   10
      B   Explain the various methods of providing security to the web services   10

Q5   A   Explain SHA-1 to calculate MD and compare it with MD5   10
      B   Write short notes on any two of the following   10
           i.   HMAC
           ii.   Key Distribution Center
           iii. DDOS

Q6   A   Discuss the various mode(Block cipher Modes) in which the algorithm can   10
           operate.

      B   What is Asymmetric key Encryption technique? Explain RSA With Suitable   10
           Example

****