Code No: F3403

R09

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, August - 2017
INFORMATION SECURITY

Time: 3hrs   Max.Marks:60

Answer any five questions
All questions carry equal marks
- - -

1.a) List various secuirty attacks and consequences of each attacks.
   b) Explain Block Cipher modes of operation.   [6+6]

2.a) Define principle of public key cryptography.
   b) Explain Kerberos authentication in detail.   [6+6]

3.a) Discuss the principles of PGP security.
   b) What is meant by Authenticaion Header and Encapsulated Security Payload?   [6+6]

4.   Demonstrate the procedure followed in SET(Secure Electronic Transaction) with a neat
     sketch.   [12]

5.   What is a Firewall? Discuss various types of Firewalls.   [12]

6.a) Explain Man in Middle Attack.
   b) What is Flooding? Discuss types of Flooding attacks.   [6+6]

7.a) Discuss the following:
     i) Relatively Prime numbers
     ii) Message Digest
   b) Explain the Euclid's algorithm to compute multiplicate inverse of a given Number.[6+6]

8.a) What is a security association and how security associations are combined with key
     management to ensure better email security?
   b) Explain about trusted systems.   [6+6]

--ooOoo--