

Code No: H4002/R13

M. Tech. II Semester Supplementary Examinations, May-2017

INFORMATION SECURITY

(Common to IT, CS, CS&T and CS&E)

Time: 3 Hours

Max. Marks: 60

*Answer any FIVE Questions
All Questions Carry Equal Marks*

1. a Define security service. List different categories security services and explain. 6M
b Write notes on Routing table modification and ARP attacks. 6M
2. a Given Cipher text “YMJT YMJWXNIJTKXNQJSHK”, knowing the message is encrypted by Caesar cipher and $k=5$. Try to decrypt the message. 6M
b Explain about various key distribution approaches of message authentication. 6M
3. a Explain the importance of Kerberos and give its requirements. 6M
b Explain the procedure involved in RSA public-key encryption algorithm. 6M
4. a Discuss about encapsulating security payload of IP? 6M
b Show how the S/MIME certification process is carried out. 6M
5. a What are the different types of viruses? How do they get into the systems? 6M
b Evaluate how firewall is different from intrusion detection system? 6M
6. a Explain symmetric cipher model with neat block diagram. 6M
b Explain any two cipher block modes of operations in detail. 6M
7. a Explain in detail Digital Signature Standard approach and its algorithm 6M
b What is the use of SSL protocol? Explain SSL record protocol operation with SSL record format. 6M
8. a Explain the need for trusted systems. 6M
b Write notes on SNMPv1 6M
