

END TERM EXAMINATION

SIXTH SEMESTER [BCA] MAY-JUNE 2016

Paper Code: BCA 314 **Subject: Computer Network and Information Security**
Time : 3 Hours **Maximum Marks :75**

**Note: Attempt any five questions including Q.NO. 1 which is compulsory.
Select one question from each unit.**

- Q1. Answer **any five** of the following briefly: (5x5=25)
- a) What are the basic principles of Information Security?
 - b) Explain the role of key generator in DES.
 - c) Explain Digital Signature and Digital Certificates.
 - d) What are the different debugging tools in ICMP?
 - e) What are the different types of connection devices?
 - f) What are the different types of addresses in the network?
 - g) What are the differences between encoding, encryption and hashing?

Unit-I

- Q2. a) What are the differences between Symmetric Cryptography and Asymmetric Cryptography? (6.5)
b) Explain traditional ciphers in detail. (6)
- Q3. a) What are the differences between stream cipher and Block cipher? (6.5)
b) Explain the working of DES and how can we generate the keys in the DES. (6)

Unit-II

- Q4. a) Explain RSA algorithm. (6.5)
b) What are the different types of messages in ICMP? (6)
- Q5. a) Explain Diffie-Hellman algorithm. (6.5)
b) Explain Hash function What is the use of MD5 algorithm? (6)

Unit-III

- Q6. a) What are the different types of attacks in the network? (6.5)
b) Explain AH and ESP to secure the layer. (6)
- Q7. a) How can we secure the VPN tunneling through IPSec protocol? (6.5)
b) Explain Security Associations and Key Management to secure the network. (6)

Unit-IV

- Q8. a) What are the differences between Application Firewall and Packet Firewall? (6.5)
b) Explain SNMP Architecture. (6)
- Q9. a) If you have to both encrypt and compress data during transmission, which would you do first, and why? (6.5)
b) Explain Gateway and proxy server. Do we use NAT in Gateway? Justify your answer. (6)

P