

11

END TERM EXAMINATION

SIXTH SEMESTER [BCA] MAY-JUNE 2014

Paper Code: BCA-314

Subject: Computer Network & Information Security (Batch 2011 Onwards)

Time: 3 Hours

Maximum Marks: 75

Note: Attempt five questions including Q.no.1 which is compulsory.

- Q1 Briefly answer the following questions:-
- (a) Give an application of Public Key Cryptography. (1)
 - (b) What are the mechanisms to achieve Integrity? (2)
 - (c) Give an example of a computer Virus and Computer Worm. (2)
 - (d) Explain the one way property of Hash function. (2)
 - (e) What is the use of agent in SNMP? (2)
 - (f) Differentiate between Symmetric Vs Asymmetric Cryptography. (3)
 - (g) Name the protocols used in:- (3)
 - (i) Application Layer (ii) Transport Layer (iii) Network Layer.
- Q2 Define the following terms briefly:- (15)
- (a) Logic Bomb
 - (b) Denial of Service attacks
 - (c) Block Cipher
 - (d) Stream Cipher
- Q3 Explain the structure of DES. Describe the Rounds used in Key Generation Process of DES. What is the use of S-boxes and P-boxes in DES? (15)
- Q4 (a) Explain RSA algorithm. (8)
- (b) Explain the message digest generation process using MD5. (7)
- Q5 (a) Explain How does Buffer Overflow attack occur? (8)
- (b) Explain IPSec achieves Authentication, Confidentiality? (7)
- Q6 (a) Explain the design principle of a firewall? What is the difference between a Packet filter router and stateful inspection Firewall? (8)
- (b) Write a short note on Virtual Private Network. (7)
- Q7 Write notes on the following:- (3x5=15)
- (a) Participants in Secured Electronic Transaction.
 - (b) ICMP Design consideration.
 - (c) Key management in IPSec.

P