USN | | | | | | | | | | |

12SCS31

Third Semester M.Tech. Degree Examination, Dec.2014/Jan.2015
Information Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions.***

1 a. What is security? What are the critical characteristics of information? **(08 Marks)**
b. Explain in brief the different phases of security systems development life cycle. **(06 Marks)**
c. Explain the relationship between the policies, standards and practices. Give the block diagram for the same. **(06 Marks)**

2 a. Describe the issue specific security policies and system specific security policies defined by the management of the organization. **(10 Marks)**
b. Define firewall? How are the firewall categorized based on processing mode? **(10 Marks)**

3 a. Explain the different detection methods used by intrusion detection and prevention systems to monitor and evaluate network traffic. **(10 Marks)**
b. What are honey pots, honey nets and padded cells? List the advantages and disadvantages of using them. **(10 Marks)**

4 a. What are passive and active attacks? Discuss different types of passive and active attacks. **(08 Marks)**
b. Name the organizations under the internet society that are responsible for the work of standards development and publications. **(06 Marks)**
c. Summarize the various types of cryptographic attacks based on the amount of information known to the cryptanalyst. **(06 Marks)**

5 a. With a neat diagram give an overview of the AES algorithm. Explain. **(10 Marks)**
b. Explain message digest generation using SHA – 512. Draw a block diagram for the same. **(10 Marks)**

6 a. List the requirements of public key cryptography. **(06 Marks)**
b. Perform the encryption and decryption using the RSA algorithm for the following : P = 3, q = 11, e = 7, M = 5. **(08 Marks)**
c. Explain the Diffie – Hellman key exchange algorithm. **(06 Marks)**

7 a. List the differences between Kerberos version 4 and version 5. **(10 Marks)**
b. Describe with a block diagram, the PGP message generation from user A to user B. **(10 Marks)**

8 a. What are the functionalities provided by AH and ESP in transport and tunnel mode? **(06 Marks)**
b. Explain the anti – replay service provided by AH. **(06 Marks)**
c. Explain the generation of dual signature of secure electronic transaction. **(08 Marks)**

* * * * *