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

10SCS333

Third Semester M.Tech. Degree Examination, December 2012

Information Security

Time: 3 hrs. Max. Marks:100

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

1 a. Why is a methodology important in the implementation of information security? Explain the security systems development life cycle, in detail. **(10 Marks)**

b. List and describe the continuity strategies. **(10 Marks)**

2 a. Describe how the various types of firewalls interact with the network traffic at various levels of the OSI model. **(10 Marks)**

b. List and describe the three control strategies proposed for intrusion detection/prevention system (IDPS) control. **(10 Marks)**

3 a. Explain five categories of security services s defined by X.800. **(10 Marks)**

b. With a neat block diagram, explain AES encryption and decryption algorithm, in detail. **(10 Marks)**

4 a. What are the requirements for public-key cryptography? **(06 Marks)**

b. Explain RSA algorithm. **(08 Marks)**

c. Perform encryption and decryption using RSA algorithm for P = 7, Q = 11, e = 17 and M = 8. **(06 Marks)**

5 a. With a neat labeled diagram, discuss the general format of a X.509 certificate. **(12 Marks)**

b. What are the principle differences between Ver. 4 and Ver. 5 Kerberos? **(08 Marks)**

6 a. Explain the operational description of PGP. **(10 Marks)**

b. With a neat diagram, discuss IPSec authentication header along antireply service and integrity check value. **(10 Marks)**

7 a. Explain the overall operation of secure socket layer record protocol, in detail. **(10 Marks)**

b. Discuss the business requirements, key features of secure electronic transaction along with the participants in SET transaction. **(10 Marks)**

8 Write short notes on:

a. Diffe-Hellman ket exchange

b. Limitations of SMTP

c. Software-based attacks

d. Secure Hash functions. **(20 Marks)**

* * * * *