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

08SCN22

Second Semester M.Tech. Degree Examination, May/June 2010
Information and Network Security

Time: 3 hrs. Max. Marks:100

Note: *Answer any FIVE full questions.*

1 a. What is the significance of information security and network security, to information processing and communication? (10 Marks)

b. Briefly explain the various characteristics of information. (10 Marks)

2 a. Describe briefly security attacks, security mechanisms and security services. (05 Marks)

b. Describe the various security services defined under X.800 (Security architecture for OSI). (15 Marks)

3 a. Enlist and describe briefly the five ingredients (parameters) of a symmetric encryption scheme. (05 Marks)

b. What is cryptanalysis? What are various types of possible attacks on encrypted messages? (10 Marks)

c. When is an encryption scheme considered to be computationally secure? (05 Marks)

4 a. With a neat diagram, describe the Feistel Cipher structure. (08 Marks)

b. What are the parameters which govern the design of a block symmetric cipher? (05 Marks)

c. Show how the Feistel Cipher structure is incorporated in the design of the DES (data encryption standard). (07 Marks)

5 a. What are the cipher block modes of operation? (05 Marks)

b. Describe the cipher block chaining mode, with the help of a neat diagram. (10 Marks)

c. How are encryption devices deployed in a packet-switching network? (05 Marks)

6 a. Distinguish between symmetric and asymmetric ciphers. (06 Marks)

b. Describe the RSA algorithm and show how it meets the various requirements of a public key crypto system. (14 Marks)

7 a. What are the requirements for a hash function? (08 Marks)

b. Give an example of a simple hash function. (04 Marks)

c. Describe the Diffie-Hellman key exchange algorithm. (08 Marks)

8 Write short notes on:

a. X.509 directory authentication service

b. Important features of pretty good privacy (PGP)

c. Application and benefits of I P Sec.

d. Web security threats (20 Marks)

* * * * *