B5.3-R3: NETWORK MANAGEMENT & INFORMATION SECURITY

NOTE:

1. **Answer question 1 and any FOUR from questions 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time: 3 Hours **Total Marks: 100**

1.

a) What are the key principles of information security?

b) What is plain text? What is cipher text? Give an example of transformation of plain text into cipher text.

c) Why is the SSL layer positioned between the application layer and the transport layer?

d) Why is there a need to take multiple samples during the user registration process of biometrics?

e) Describe IP Spoofing as a network attack.

f) Compare the digital signature and conventional signature with respect to the following four parameters: Inclusion, Verification, Relation, and Duplicity.

g) Define the session key and show how a Key Distribution Centre (KDC) can create a session key between two users.

(7x4)

2.

a) How does Virtual Private Network (VPN) work? Explain briefly.

b) What is a packet filter firewall? Explain the three main functions performed by packet filter firewall. Which techniques are used to break the security of packet filter firewall?

c) What are the three broad categories of applications of public key cryptosystems?

(6+9+3)

3.

a) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography.

b) List and give the purpose of following protocols defined in SSL:

Handshake protocol, ChangeCipherSpec Protocol, Alert Protocol, Record Protocol

c) The most powerful and most common approach to secure the points of vulnerability in typical business environment is encryption. If encryption is to be used to counter the attacks, then there are two alternatives to locate the encryption function – end to end encryption and link to link encryption. What are the advantages and disadvantages of both the approaches?

(9+4+5)

4.

a) Name seven types of packets used in Pretty Good Privacy (PGP) and explain their purposes.

b) What is Denial of Service (DoS) attack? Explain types of DoS attack? Differentiate between DoS attack and Distributed DoS attack.

c) How is double DES equivalent to single DES (Digital Encryption Standard)?

(7+7+4)

5.

a) What are the three benefits that can be provided by an intrusion detection system?

b) Write the formal definition of Role based access control. What are the advantages of using Role based access control over Mandatory access control (MAC) and Discretionary Access control (DAC)?

c) What is the purpose of Simple Network Management Protocol (SNMP)? A SNMP operation is performed using Protocol Data Unit (PDU), basically a word for packet. List all PDU used and explain each of them.

(3+8+7)

6.

a) Which are the services provided by IPSec? Explain each in brief.

b) What is Annualized Loss Expectancy (ALE)? How can it be directly useful in cost benefit analysis?

c) List three approaches to secure user authentication in a distributed environment.

(6+9+3)

7.

a) What is ASN.1 with respect to network management function? What is the purpose of ASN.1? Explain with the help of an example.

b) Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.
   i) Brute-Force Cryptanalytic Attack.
   ii) Replay Attack.
   iii) IP Spoofing
   iv) Password Sniffing.

c) Cyber crime may be broadly classified in three groups. Explain each of them. What precautions one has to take to prevent cyber crime in the society?

(6+4+8)