B5.3-R4: 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) Define the following terms:
   i) Virus
   ii) Worm
   iii) Trojan Horse
   iv) Logic Bomb

b) What do you understand by security service? What are the design goals for a security service?

c) What are the three primary rules defined for role based access control?

d) What is Simple Network Management Protocol? How is it useful to manage the network?

e) What is RARP? How is it different from ARP (Address Resolution Protocol)?

f) Kerberos is a computer network authentication protocol, which allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Explain how is it work?

g) An application gateway is consisting of a security component that augments a firewall or NAT employed in a computer network. Briefly explain how is it work?

(7x4)

2.

a) What is Pseudo Random Sequences? How true randomness is generated? Explain.

b) RSA involves a public and private key. The public key can be known to everyone and is used for encrypting messages. How are the keys for the RSA algorithm generated? Write steps.

(6+12)

3.

a) The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. Explain how is it work?

b) What is authentication? What is the difference between one-way authentication, two-way authentication and three-way authentication?

(9+9)

4.

a) Give main features of Indian IT Act 2000?

b) The Internet Control Message Protocol (ICMP) is a troubleshooting tool used by technicians to find errors on a network, and it communicates errors on a network as they occur. How ICMP differs from TCP and UDP? Does ICMP guarantee delivery? Justify.

(9+9)

5.

a) What are the two main branches of public key cryptography? Briefly explain each of them.

b) Explain the packet structure of IPv4.

(6+12)

6.

a) L2TP does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy. Explain L2TP.

b) A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass. How a stateful firewall works? Explain.

(9+9)

7.

a) What is the difference between configuration management and configuration control in Network Management?

b) Explain how PGP encryption works.

(6+12)