B5.3-R3: NETWORK MANAGEMENT & INFORMATION SECURITY

NOTE:

1. **Answer question 1 and any FOUR questions from 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 is denial-of-service attack (DoS)? Briefly explain the common method of it and how is it implemented?

b) Cryptanalytic attacks vary in potency and amount of threat they pose to real-world cryptosystems. What are the factors on which the practical importance of an attack depends?

c) Define Simple Network Management Protocol (SNMP). What are the major components of SNMP-managed network?

d) An application gateway is an application program that runs on a firewall system between two networks. Briefly explain how it works?

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

f) What are the three key properties of hash functions?

g) Internet Protocol Security (IPSec) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. Map the various protocols of IPSec with the functions they perform.

(7x4)

2.

a) In cryptography, MD5 (Message-Digest algorithm 5) is widely used cryptographic hash function with a 128-bit hash value. Explain the algorithm.

b) Describe the IPSec services with respect to AH and ESP. Describe the IPSec AH and IPSec ESP format with diagrams.

c) Present and discuss the *screened subnet* architecture of firewalls.

(6+6+6)

3.

a) The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet protocol suite. How does ICMP differ from TCP and UDP? Does ICMP guarantee delivery? Justify.

b) Explain Brute Force attack.

c) Name the six participants in the SET system and show their interconnections in a secure electronic commerce component diagram.

(6+6+6)

4.

a) What do you understand by Access Control List? Briefly explain discretionary and mandatory access control.

b) What is the difference between “reactive” and “proactive” fault management? State the four steps usually followed in reactive fault management.

c) 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 works?

(6+6+6)

5.

a) What is a management information base? Which are the two types of managed objects that exists?

b) Explain how PGP encryption works.

(9+9)

6.

a) The RSA algorithm involves three steps, key generation, encryption and decryption. Explain each step.

b) What do you understand by Intrusion Detection System? Briefly explain its various types.

(9+9)

7.

a) In computer networking, the Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). Explain L2TP.

b) Describe briefly the Bell-La Padula Model and its limitations. What is tranquility principle in this model?

(9+9)