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) Confidentiality, Integrity and Availability form the core principles of information security. Briefly explain each of them.

b) A firewall's responsibility is to control traffic between computer networks with different zones of trust. Explain the main categories of firewall with reference to the layers where the traffic can be intercepted. Briefly explain each of them

c) Mandatory access control (MAC) is an access policy determined by the system, not the owner. Is it true or false? Justify.

d) What do you understand by biometrics and biometrics authentication?

e) A hash function takes a long string (or 'message') of any length as input and produces a fixed length string as output, termed a message digest or a digital fingerprint. Explain message authentication code (MAC) in message digest in brief.

f) What do you understand by audit trail with respect to information security?

g) Is there any difference between configuration management and configuration control in network management? Explain the term in brief.

(7x4)

2.

a) What is a Denial-Of-Service attack (DOS attack)? Explain it by providing suitable example.

b) RSA involves a public and private key. How are these keys, for the RSA algorithm, generated? Write steps.

c) Explain attack in Diffie-Hellman Key Exchange algorithm.

(6+6+6)

3.

a) The Internet Protocol (IP) is a network-layer protocol in the OSI model to enable packets being routed in network. What are the primary responsibilities of it? Explain the protocol structure of IP / IPv4 (Internet Protocol version 4).

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

c) What is steganography and how it works? What are the advantages and application of it?

(6+6+6)

4.

a) What is access control method? Explain the following access control model:

i) Bell-La Padula Model

ii) Biba Integrity Model

b) What is secure mail? What is the reason for the lack of deployment of Privacy-enhanced Electronic mail (PEM) as compared to Pretty Good Privacy (PGP)? Explain PEM and PGP.

c) Define the terms: Logic Bomb, Trojan Horse

(8+8+2)

5.

a) When management chooses to mitigate a risk in the design and implementation of security policy, what are the different security controls used?

b) What are the procedures involved in Quantitative Risk Management? How is the Annualized Loss Expectancy (ALE) calculated?

c) How does Assymetric key encryption ensure “Non-Repudiation”? Explain with an example.

(6+6+6)

6.

a) What is Abstract Syntax Notation One (ASN.1) with respect to network management functions? Explain the key components of an SNMP-managed network.

b) What is intrusion detection system (IDS)? Briefly explain the following types of IDS.

i) Network based IDS
ii) Protocol based IDS
iii) Application based IDS
iv) Host based IDS

c) How does User Based Security Model provide integrity protection with or without delay detection and privacy protection?

(6+6+6)

7.

a) How ICMP differs from TCP and UDP? Does ICMP guarantee delivery of packets? Justify.

b) What are the purposes and functions of a Public Key Infrastructure (PKI) in cryptography? Explain.

c) What is cyber crime and cyber forensic?

(8+6+4)