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 access control? Differentiate between discretionary or mandatory access control techniques.

b) Modern study of symmetric-key ciphers relates mainly to the study of block ciphers, stream ciphers and their applications. Explain block ciphers and stream ciphers.

c) 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. Briefly explain message authentication code (MAC) in message digest.

d) Briefly explain confidentiality, Integrity and Availability with respect to information security.

e) What is the meaning of configuration management or configuration control in network management and information security?

f) Which protocol is used for securing credit card transactions over insecured networks, specifically, the Internet? Which features are incorporated in the protocol to meet the business requirements?

g) A firewall's basic task is to control traffic between computer networks with different zones of trust. What are the main categories of firewall with reference to the layers where the traffic can be intercepted? Define each category with example.

(7x4)

2.

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

c) What is Intrusion Detection System (IDS)? Briefly explain network based IDS and host based IDS.

(6+6+6)

3.

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

b) What is IPsec? Explain the two modes in which IPsec works.

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

(6+6+6)

4.

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

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

c) Why is MD5 (Message-Digest algorithm 5) widely used in cryptographic hash function with a 128-bit hash value?

(6+6+6)

5.

a) What is biometrics and biometrics authentication?

b) Why does Encapsulation Security Payload (ESP) include a padding field?

c) A firewall is an Information Technology (IT) security device which is configured to permit, deny or proxy data connections set and configured by the organization's security policy. What is stateless and stateful firewall? Explain.

(4+6+8)

6.

a) How does Assymetric key encryption ensure "Non-Repudiation"? Explain with an example.

b) What is a denial-of-service attack (DoS attack)? A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Explain it by providing suitable example.

c) 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)?

(6+6+6)

7.

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

b) What is audit trail with respect to information or communication security?

c) What is network management performance? What are the factors that affect the performance of network?

d) 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.

(3+3+6+6)