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) What are the threats of web security? What are the Consequences and Counter measures of each threat?

b) Write down the similarities and differences between Brute force and Dictionary attack.

c) Simple Network Management Protocol is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. What are the key elements of SNMP?

d) A Virtual Private Network (VPN) is a network that uses primarily public telecommunication infrastructure. How can be implemented in an Organization?

e) Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP). What are the applications of it? Write down benefits of it.

f) With respect to Cyber law, who can be Gray Hat Hacker?

g) Explain the terms: Virus, Worms, Trojans and Spyware.

(7x4)

2.

a) Pretty Good Privacy (PGP) is a data encryption and decryption computer program. What are the five principle services provided by the PGP?

b) What types of attacks are addressed by Message Authentication? What two levels of functionality comprise a message authentication?

c) Asymmetric cryptography, is a class of cryptographic algorithms which requires two separate keys, one private and other one is public. What are the elements of Asymmetric Cryptography? Write down step-by-step procedure of working of Asymmetric Cryptography?

(5+5+8)

3.

a) India IT Act 2000 aims to provide the legal infrastructure for e-commerce in India. What are the offerings given under IT Act 2000?

b) What are the attributes of Information Security?

c) What are the general techniques that firewalls use to control access and enforce the site's security policy? Write down the limitations of firewall.

(5+6+7)

4.

a) What are Block cipher modes of operation? Compare the various block cipher modes of operations.

b) The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. Write down the steps of DES.

c) Transport Layer Security (TLS) uses state full connection by using a handshaking procedure. What kinds of messages are exchanged during handshaking between client and server to ensure security of data?

(5+6+7)

5.

a) Network Security consists of the provisions and policies adopted by a network administrator to monitor and prevent unauthorized access, misuse, modification, or denial of a computer network. What are the types of Network Security Attacks?

b) Risk management reduces risk of the system. What are the principle and process of risk management?

(9+9)

6.

a) What is firewall? What does a firewall do?

b) MD5 has been utilized in variety of cryptographic applications, and is also commonly used to verify data integrity. How does MD5 achieve data integrity?

c) Explain following terms with respect to network security

i) IP spoofing

ii) Server spoofing

iii) DNS poisoning

(6+6+6)

7.

a) Denial-of-Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. What are some known DoS Attack?

b) What is Public-Key Infrastructure (PKI)? What are the requirements for the user of a public-key certificate scheme?

c) In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. What are the possible vulnerability of password? What are the type's attacks on Password? Suggest what should be minimum password defining policy.

(6+6+6)