B5.3-R4 NETWORK MANAGEMENT AND 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) A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. Give your suggestion to have a strong password policy in your organization.

b) What are the differences between secret key and public key cryptography?

c) Risk assessment is the process of quantifying the probability of a harmful effect to computer network. What are the ways to asses or determine risk in network?

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

e) A virtual private network (VPN) is a network that uses primarily public telecommunication infrastructure. How can VPN be implemented in a campus?

f) Once Internet Authentication Service (IAS) has authenticated the user, it can use a few authorization methods to verify that the authenticated user is permitted to access the network resource. Briefly write down these authorization methods.

g) How does Computer Viruses spread in internet?

(7x4)

2.

a) What are the attributes of Information security?

b) Firewall prevents unauthorized access to personal network. What are different types of firewalls? Describe each briefly.

(10+8)

3.

a) What are the types of Network Security Attacks? Explain each briefly.

b) Write the steps of Message Digest 5 (MD-5) algorithm.

(12+6)

4.

a) With respect to cyber law, explain who are white Hat Hacker and Black Hat Hacker?

b) Write RC4 algorithm for stream cipher.

c) Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. How does PGP encryption work?

(6+6+6)

5.

a) Explain Diffe-Hellman Key Exchange algorithm. How can the attack in the middle be performed?

b) The Kerberos authentication protocol verifies the identity of network users. What are the steps performed by Kerberos to authenticate user?

(10+8)

6.

a) What do you mean by cryptanalysis? Give an example.

b) Explain following terms with respect to network security

i) IP spoofing

ii) Server spoofing

iii) DNS poisoning

c) Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. What kinds of messages are exchanged between client and server to ensure security of data?

(5+6+7)

7.

a) What are the areas of cyber crime?

b) Public Key Cryptography (PKC) is an arrangement that binds public keys with respective user identities by means of a certificate authority. What does it consist of? How does Public and Private Key Cryptography Work?

c) Risk management reduces risk of the system. What are the principles and processes of risk management?

(6+6+6)