B5.3-R3: 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) How are block ciphers different from stream ciphers?

b) Why does an application level gateway tend to be more secure than packet filters?

c) Explain briefly any three tasks performed by a firewall.

d) In a cryptosystem, P, C and K stand for Plain Text, Cipher text and Key respectively. Answer the following:

i) Give an interpretation of the following equation:

$$C= E_{K2}(E_{K1}(P))$$

ii) Give an example of a cryptosystem with the above property.

e) How IPsec can be used to create a VPN?

f) Describe Proxy/Wingate Trojans?

g) What is the utility of detached signature in PGP?

(7x4)

2.

a) What are the various classes of Digital Certificates? List three primary functions of CERT.

b) Explain two major requirements for secure symmetric encryption.

c) How key distribution can be achieved in symmetric encryption?

(6+6+6)

3.

a) List three approaches to secure user authentication in a distributed environment.

b) What are Kerberos? List four requirements for designing the Kerberos environment?

(9+9)

4.

a) List four public key cryptography algorithms. Explain one of the algorithms where public key cryptosystems is used.

b) What is S/MIME? Explain its functions.

(9+9)

5.

a) What is Annualized Loss Expectancy (ALE)? How can it be directly useful in cost benefit analysis?

b) List three attacks that can be activated on packet filtering routers. Also suggest appropriate counter measures.

(9+9)

6.

a) Briefly classify three classes of intruders?

b) What are the benefits of an Intrusion Detection System? Explain.

c) Distinguish between Dictionary Attack and Heuristic Attack methods?

(6+5+7)

7. Write short notes on any **three** of the following:

a) SET

b) MD

c) Triple DES

d) Back Door

(3x6)