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) How does the Secured Socket Layer transaction helps in secured data transmission?

b) Explain briefly, why IPSec is needed when TCP/IP is available.

c) Why is a network authentication protocol used?

d) Differentiate between cryptography and steganography.

e) Distinguish between TCP spoofing and DNS Spoofing?

f) What are the different types of messages define in SNMP?

g) Explain the various categories of Denial of Service Attack (DOS)?

(7x4)

2.

a) Explain how NFTS permissions are better than share permissions.

b) What are the various ways of attacking the e-mails?

c) Why is Authentication Head (AH) required? How is it different from Encapsulating Security Payload (ESP)?

(6+6+6)

3.

a) Explain briefly Active Directory and the advantages offered by it.

b) Give expressions describing the triple DES function at the sending and receiving ends. What is the purpose of the intermediate stage? Illustrate how the intended purpose of the intermediate stage is achieved.

c) Bob has just received a message. How does his Privacy Enhanced e-Mail (PEM) processor know whether the message is a PEM message or just an ordinary message?

(6+6+6)

4.

a) What are worms and when does it executes?

b) Why can IP spoofing not be prevented by using Packet Filter Firewall Technique?

c) How does RSA based digital signature help in "non-repudiation"? Explain with a suitable example scenario between a sender and a receiver.

(6+6+6)

5.

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

b) In most of the campus/corporate networks, we find firewalls preceded by a router, but not the reverse. Explain, why this has become almost a de-facto standard.

c) Explain briefly with an example, how Windows registry is secured.

(6+6+6)

6.

a) What are the advantages of using IDS?

b) What are the various classes of Digital certificates? What are the advantages of International format Standard X.509v3?

c) What is Snooping? Is Diffie-Hellman algorithm susceptible to this attack?

(5+9+4)

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

   a) Message Digest

   b) ICANN

   c) Cracking Methods

   d) Demilitarized Zone

   e) CERT

(3x6)