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 digital signature? Which algorithms are used for digital signatures?
b) Differentiate between steganography and cryptography.
c) How does message digest help in checking the integrity of a transmitted text?
d) State four primary functions of CERT.
e) Differentiate between active and passive attacks on a computer.
f) What is an application level firewall and why is it necessary?
g) State any four acts amounting to "cybercrime" as per IT Act 2000.

(7x4)

2.

a) Suppose you are doing RSA encryption with the prime numbers p=13 and q=7. Also, assume that encryption exponent e=5. Find the least positive decryption exponent d. Next, encrypt the message m=7. Now decrypt the cipher c=2.
b) Explain the distributed DoS (Denial of Service) attack with a suitable diagram? Why is this kind of attack very common during the final hours of the Internet auction?
c) What is the importance of "no read up" plus "no write down" rule for a multilevel security system?

(9+6+3)

3.

a) What is meant by IP spooling? How can a router be used to prevent IP spooling?
b) How does RSA based digital signature help in "non-repudiation"? Explain with a concrete example scenario between a sender and a receiver.
c) Describe the Digital Signature (DS) Algorithm based on DS standard of NIST. How are signing and verifying done in DS standard?

(3+6+9)

4.

a) Consider the following threats to Web security and describe how each is countered by a particular feature of SSL (Secure Sockets Layer):
   i) Brute-Force Cryptanalytic Attack
   ii) Replay Attack
   iii) Packet Sniffing
   iv) Password Cracker
   v) SYN Flooding
   vi) Man-In-The-Middle Attack
b) Name the six participants in the SET system and show their interconnections in a secure electronic commerce component diagram.

([6x2]+6)

5.

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

b) What is the difference between “reactive” and “proactive” fault management? State the four steps usually followed in reactive fault management.

c) What does SNMP define as manager, agent and client? Why does SNMP need SMI and MIB to manage a network? How are they related to UDP?

(3+6+9)

6.

a) Describe briefly the Bell-La Padula Model and its limitations. What is tranquility principle in this model?

b) What are the three classes of intruders? Discuss any three metrics used in profile-based anomaly detection. Explain the architecture of a distributed intrusion detection system (with a suitable diagram) and name the various components.

(8+10)

7. Write short notes on any **three**:

i) Pretty Good Privacy (PGP)
ii) IPsec VPN
iii) Risk Assessment (RA)
iv) Biometrics

(3x6)