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) How can be IPSec used for creating VPN?
b) What is triple DES with two keys? How is it better than double DES?
c) What do you mean by linear crypto analysis? Explain briefly.
d) List four techniques used by firewalls to control access and enforce a security policy.
e) With respect to integrity and confidentiality security services, explain types of **web security** threats, consequences and countermeasures.
f) List and briefly define four techniques used to avoid guessable passwords.
g) Risk assessment forces an organization to consider the range of potential threats and vulnerabilities it faces. Justify the statement.

(7x4)

2.

a) Explain the general idea behind challenge response entity authentication.
b) Explain IP address spoofing, source routing attack and tiny fragment attack that can be made on packet-filtering routers with appropriate countermeasures.

(6+12)

3.

a) Explain why modern block ciphers are designed as substitutions ciphers instead of transposition ciphers. Explain DES cipher.
b) What do you mean by message authentication code and message digest?
c) Explain how confidentiality and authentication can be achieved using Public-key Cryptosystem.

(8+4+6)

4.

a) Explain the working of stream cipher RC-4.
b) What is S/MIME? Explain its functions.

(10+8)

5.

a) Explain Public Key Infrastructure Architectural Model, their key elements and management function that potentially need to be supported by management protocols.
b) What are various classes of intruders? Explain each briefly.

(9+9)

6.

a) A host receives authenticated packets with the sequence number 181 and 208. The replay window spans from 200 and 263. What will the host do with these packets? What is the window span after this event?
b) What are message format in PGP? Explain each briefly.
c) Information Technology Act, 2000 deals with the cyber crime problems. Explain positive and negative aspects of IT Act, 2000.

(6+6+6)

7.

a) How the two protocols AH and ESP provide Access Control, Message authentication, Entity authentication, Confidentiality, Replay Attack protection for packets at the network layer?

b) What is Kerberos? List the requirements for designing the Kerberos environment.

(9+9)