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) What are the most commonly used cryptographic protocols for managing secure communication between a client and server over the Web?

b) List and briefly explain the system security threats.

c) Compare and contrast the problems and benefits of KDC and PKI.

d) Briefly explain, why IPsec has not the same problem as TLS? Also indicate what is additionally needed in a IPsec based Virtual Private Network (VPN).

e) Briefly explain the key elements of any security policy?

f) Differentiate between Brute Force and Dictionary Attacks.

g) What is Reverse Address Resolution Protocol?

(7x4)

2.

a) Briefly explain the services provided by IPSec at the network layer.

b) What are sweeps? Compare and contrast TCP/UDP sweeps and ping sweeps.

c) Briefly explain the Distributed Denial-of-Service (DDoS) Attack.

(6+6+6)

3.

a) Why there is need of security at every layer of Open System Interconnection (OSI) model. Discuss the security methods used at each layer of OSI model.

b) Differentiate between symmetry and asymmetric key based cryptography. Given a symmetric and asymmetry system of n-users, how many keys are needed for pairwise secure communication?

(9+9)

4.

a) How Pretty Good Privacy (PGP) ensures that an e-mail message or file just downloaded from the Internet is both secure and untampered? Discuss the authentication, confidentiality, compression, e-mail compatibility and segmentation services of PGP operations.

b) How ITA 2000 provides legal framework for electronic governance by giving recognition to electronic records and digital signatures? Give few examples of offenses and the corresponding penalties.

(9+9)

5.

a) Alice selects two prime numbers, p=5 and q=11, and public exponent e=3. Bob wants to send message (M)=4 to Alice. Compute the ciphertext generated by Bob and plaintext obtained by Alice.

b) Let the elliptic curve is E: $y^2 = x^3+2x+2 \bmod 17$ and point on elliptic curve P = (5,1). Compute (i) 2P and (ii) 3P.

(6+12)

6.

a) What is use of Simple Network Management Protocol (SNMP)? What capabilities are added by SNMP Version 3 to the previous versions? Discuss the Message format of SNMP version 3.

b) What is Virtual Private Network (VPN)? List various activities performed by VPN. Discuss its components and types.

(9+9)

7.

a) Is RC4 a block or stream cipher? Discuss the Key Scheduling Algorithm (KSA), Pseudo Random Number Generation Algorithm (PRNGA), Encryption and Decryption algorithms used in RC4 cryptosystem.

b) What do you understand by System vulnerabilities? Do human factors cause vulnerabilities? If yes, explain some human factors that causes system vulnerabilities.

(10+8)