B5.3-R4: NETWORK MANAGEMENT AND INFORMATION SECURITY

«QP_SRLNO»

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) Differentiate between trusted, secure and hybrid Virtual Private Networks (VPNs).

b) Write steps used in calculating random number in Pseudorandom Number Generation Algorithm of RC4 cryptosystem.

c) Discuss the operational services of Pretty Good Privacy (PGP).

d) Differentiate between Viruses, Worms and Trojans.

e) What do you understand by TCP/UDP Port Sweeps?

f) Differentiate between Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP).

g) What is Message Transmission Unit (MTU)? How communication occurs if MTU size is too large?

(7x4)

2.

a) What do you understand by incident handling? What common steps are required to be followed for all types of attacks?

b) Discuss Diffie-Hellman Algorithm. Let primitive element/generator (g) = 5 in a field with prime number (p) =23. The secret number selected by Alice and Bob are 6 and 15 respectively. Compute the session key generated between Alice and Bob.

(9+9)

3.

a) List various cryptography modes of operations. Compare and contrast feature of every mode of operation.

b) What do you understand by IPSec Anti-Replay Protection? Differentiate between two basic IPSec security protocols: Authentication Header (AH) and Encapsulating Security Protocol (ESP).

(12+6)

4.

a) Compare and contrast the following:

i) Symmetric vs Asymmetric Cryptosystem

ii) Transport vs Tunnel Mode in Encapsulating Security Payload or Authentication Header

iii) Stream vs Block Ciphers

b) Give few examples of offenses and the corresponding penalties in ITA 2000.

(12+6)

5.

a) Define Risk? Draw the Risk Management life cycle and identify threats to assets in Risk Assessment.

b) What are the objectives of information security policies and standards? List the requirements of successful implementation of information security policies and standards.

(9+9)

6.

a) What is the purpose of Secure/Multipurpose Internet Mail Extension (S/MIME)? What roles are performed by MIME type, subtype and the body in internet e-mail messages? Give brief explanation to security services added to S/MIME.

b) What is a firewall? Differentiate between a network gateway and a firewall. List the services provided by firewall to various TCP/IP layers.

(9+9)

7.

a) What is a hash function? List features and properties of hash functions. Also, discuss the applications of hash functions.

b) What is Triple -DES? What are the two variants of Triple-DES? Draw the encryption-decryption block diagram of Triple-DES.

(9+9)