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) Describe the Security Mechanisms used to provide information security.
b) What is dictionary attack? Explain the importance of rainbow table.
c) Write the guidelines for 3DES given by FIPS 46-3.
d) Explain the Four different stages used in AES.
e) Write the design objectives for Hierarchical Message Authentication Code (HMAC).
f) Explain authentication exchange using EAPOL and RADIUS.
g) Define Secure Shell (SSH).

(7x4)

2.

a) A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. Explain the various threats related to information security.
b) What is Information Security Risk Management? List and explain the four stages related to Information Security Risk Management.
c) What is digital signature? How does it work?

(3+8+7)

3.

a) What is Information Security Level? Explain all the information security levels.
b) Security policy is a definition of what it means to be secure for a system, organization or other entity. Explain the five best practices for building a security policy.
c) SSL (Secure Sockets Layer) is a standard security protocol for establishing encrypted links between a web server and a browser in an online communication. Describe the parameters, which define the connection state in SSL.

(6+5+7)

4.

a) What is stream cipher? List and explain important design considerations for a stream cipher.
b) The block cipher modes ECB, CBC, OFB, CFB, CTR, and XTS provide confidentiality. Write the advantages of CTR mode.
c) HTTP Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network. Explain the connection initiation and connection closures process in HTTPS.

(5+5+8)

5.

a) Explain the firewall. What are the common capabilities and limitations of firewall?
b) What can be the objective of intruder? What are the possible ways to protect the password file? Explain the approaches to intrusion detection.
c) What is virus? During its lifetime, a typical virus goes through the four phases. Explain those phases in brief.

(6+6+6)

6.

a) Suppose a plaintext file of 5 MB is encrypted with a secret-key algorithm (e.g., DES, AES), and the resulting file is compressed with a lossless compression algorithm (e.g., zip), and the resulting file is 3 MB. What does this imply about the plaintext, about the encryption algorithm, and about the compression algorithm?

b) Draw the general format of PGP messages. Explain the various fields, which are included as a signature field.

c) List and explain benefits of IP Security (IPSec).

(5+8+5)

7.

a) List of explain criteria are used to validate that a sequence of numbers is random. Mention and explain number of network security algorithms based on cryptography, which make use of random numbers.

b) Let us choose two primes p = 11, q = 13 and public key e = 7. Demonstrate the working of RSA using the given values.

c) Differentiate Message Authentication and Message Encryption. Explain three situations in which message authentication without confidentiality is preferable.

(6+6+6)