

## 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) What are the password vulnerabilities and attacks?
- b) How one can protect their computer from Viruses, Worms and Trojan Horses?
- c) Differentiate between brute force and dictionary attack.
- d) IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address. What are the applications of IP Spoofing? Which are the services vulnerable to IP Spoofing?
- e) What are the differences between Symmetric and Asymmetric algorithms of Security?
- f) What are the Principles of Risk Management?
- g) Define the following two terms
  - i) Screened Host Firewall System
  - ii) Screened Subnet Firewall System

**(7x4)**

**2.**

- a) What is authentication and authorization?
- b) Public-key cryptography refers to a cryptographic system requiring two separate keys. What are the weaknesses of public key cryptography?
- c) What are the threats and vulnerability? How to carry out threats and vulnerability identification?

**(4+6+8)**

**3.**

- a) Security Policy is processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. What are the issues of Security Policy Implementation?
- b) The RC4 algorithm is stream cipher. Write down pseudo code of algorithm of RC4 and explain by taking suitable example.
- c) What is a network firewall? List the critical resources in a firewall? What can't a firewall protect against that don't go through the firewall?

**(5+6+7)**

**4.**

- a) What is functionality of Biometric Authentication? What is multimodal Biometric Authentication?
- b) List and describe The steps of Risk Analysis.
- c) What are the advantages of E-mail over TLS as compared to traditional (unencrypted) e-mail?

**(6+8+4)**

**5.**

- a) What is MD5? What are the differences between MD5 and SHA? What are a collision attack and a preimage attack?
- b) By drawing suitable diagram explain Virtual Private Network (VPN). What are the types of VPN? What are the pros and cons of VPN?

**(9+9)**

6.

- a) How Cryptography System is characterized? What is Cryptanalysis?
- b) What are the security Services and Mechanism? Give relationship chart of Security Mechanism and Services?
- c) List the business requirements of Secure Electronic Transaction (SET).

**(5+8+5)**

7.

- a) Public-Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. How does the Public Key Cryptography concept work?
- b) A Port Scanner is a software application designed to probe a server or host for open ports. What are the types of scanning & How to carry out scanning?

**(9+9)**