

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 is Simple Network Management Protocol? How is it useful to manage the network?
- b) Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. Briefly explain IPsec services.
- c) Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. Briefly explain how PGP encryption works.
- d) Mandatory access control (MAC) is an access policy determined by the system, not the owner. Is it true or false? Justify.
- e) What is Substitution cipher?
- f) What is denial-of-service attack (DoS)? Briefly explain the common method of it and how is it implemented?
- g) An application gateway is consisting of a security component that augments a firewall or NAT employed in a computer network. Briefly explain how is it work?

(7x4)

2.

- a) What is the difference between configuration management and configuration control in Network Management?
- b) The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. Explain the algorithm.
- c) Explain Brute Force attack.

(4+10+4)

3.

- a) Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. Explain L2TP.
- b) Explain key generation, encryption and decryption in RSA algorithm.

(8+10)

4.

- a) Kerberos is a computer network authentication protocol which works on the basis of "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Explain how it works?
- b) What are the design goals for a security service in network management?
- c) What is RARP? How is it different from ARP (Address Resolution Protocol)?

(10+4+4)

5.

- a) A firewall is a device which is used to permit, deny or proxy data connections set and configured. How a stateful firewall works? Explain.
- b) Define Simple Network Management Protocol (SNMP). What are the major components of SNMP-managed network?
- c) What is Multipurpose Internet Mail Extensions (MIME)?

(10+4+4)

6.

- a) What are the types of Network Security Attacks? Explain each briefly.
- b) Briefly Explain Stegnography and also explain how it works? What are its advantages and applications?

(12+6)

7.

- a) Explain the working of Stream Cipher RC-4.
- b) What is access control method? Explain the following access control model.
 - i) Bell-La Padula Model
 - ii) Biba Integrity Model

(10+8)