No. of Printed Pages : **2**

Sl. No.

B53 - 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.**

Total Time : 3 Hours **Total Marks : 100**

1. (a) What are the objectives of information security for an organization ?

(b) What are the difference between authentication and authorization ?

(c) What is digital signature? Where it can be applied ?

(d) List the business requirements of Secure Electronic Transaction (SET).

(e) What are the possible ways to approach the identification of threats ?

(f) An effective Unified Threat Management (UTM) solution delivers a network security platform comprised of robust and fully integrated security and networking functions. What are the advantages of it ?

(g) What does certification authority mean? What is the role of certifying authority ? **(7x4)**

2. (a) What are the implications for certificate authorities, such as those issuing SSL web server certificates containing MD5 or SHA-1 hashes ?

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

(c) The Internet Protocol (IP) is a network-layer protocol in the OSI model to enable packets being routed in network. What are the primary responsibilities of it ? Explain the packet structure of IP/IPv4 (Internet Protocol version 4) **(6+6+6)**

3. (a) What are the general techniques that firewalls use to control access and enforce the site's security policy ? Write down the limitations of firewall.

(b) What is Pseudo Random Sequences? How true randomness is generated ? Explain.

(c) Explain key generation, encryption in RSA algorithm. **(6+6+6)**

4. (a) Confidentiality, Integrity and Availability form the core principles of information security. Briefly explain each of them.

(b) With respect to cyber law, explain who are white Hat Hacker and Black Hat Hacker ?

(c) Why we cannot use a hash function to do encryption ? **(6+6+6)**

5. (a) Explain SNMP protocol with packet format.

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

(c) What is DoS (Denial of Service) attacks: List the types of DoS attacks. **(6+6+6)**

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

(b) What is "Computer virus" ? Explain it.

(c) Write a short note on "Network Security Policy: Best Practices". **(6+6+6)**

7. (a) List the requirements of successful implementation of information security policies and standards.

(b) What is Secured Electronic Transaction ? Explain.

(c) What is perfect secrecy ? Explain why it is not achievable. **(6+6+6)**

- o 0 o -