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) Transport Layer Security (TLS) is a protocol that provides privacy and data integrity between two communicating applications. What are the benefits of using TLS ?

(b) What are the essential elements of a Symmetric Cipher ?

(c) A cryptographic attack is a method for circumventing the security of a cryptographic system by finding a weakness. Differentiate between brute force and dictionary attack.

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

(e) How does access control work at number of levels like application, middleware, operating system and hardware in system ?

(f) What is Authentication and Authorization ?

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

(7 × 4)

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 is Transport Layer Security (TLS) ? Explain how mail server, database server, or directory server can be secured with TLS.

(c) Why does key distribution process need a key distribution center ? What is certification authority ? Explain certification revocation list method.

(5 + 6 + 7)

3. (a) List the ways to combat Viruses, Worms and Trojan Horses on the computer.

(b) What is stream cipher ? Write comparisons between stream ciphers and block ciphers ?

(c) What is the importance of prime numbers in RSA ? Explain how RSA algorithm encrypt and decrypt a message giving some numerical example.

(5 + 5 + 8)

4. (a) What is MD5 ? What are the differences between MD5 and SHA ? What are a collision attack and a preimage attack ?

(b) 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 ?

(c) Define Security policy and explain its purpose with relation to IPSec.

(6 + 6 + 6)

5. (a) List the Strength of RC4. Compare RC4 and RC5 stream cipher algorithm.

(b) What is buffer overflow ? Explain the ways to prevent buffer overflow. How to spoof IP address to conceal the online user's identity ?

(c) Write steps to improve Security Incident Handling.

(5 + 8 + 5)

6. (a) Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications. Which are the protocols used by IPSec ? What are the modes of operation on which IPSec works ?

(b) List and explain Virtual Private Network (VPN) protocols.

(c) What are the five principle services provided by the PGP ?

(9 + 4 + 5)

7. (a) Encode the message "This is a test" using the following encoding system:

(i) Radix-64

(ii) Quoted-printable

(b) Modes of operation have been devised to encipher text of any size employing Data Encryption Standard (DES). Explain Cipher Block Chaining (CBC) mode. What about error propagation in it ? What is cipher text stealing ?

(9 + 9)

———————