No. of Printed Pages : **2**

Sl. No.

B53-R4 : NETWORK MANAGEMENT & INFORMATION SECURITY

NOTE :

1. **Answer question 1 and any FOUR questions from 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) Password Authentication Protocol (PAP) is an authentication protocol used by Point to Point Protocol (PPP) to validate users. Why does organization force to have a strong password ?

(b) Information security threats come in many different forms. What are the various threats present today ? Write examples of each type of threat.

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

(d) Secure Electronic Transaction (SET) is a communication protocol for ensuring the security of financial transactions on the Internet. What are the key feature of SET protocol?

(e) What are the problems associated with implementation of security policy ?

(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 UTM ?

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

2. (a) Authentication is the act of confirming the truth of an attribute of a single piece of data claimed by an entity. What are the types of authentication ?

(b) What are the differences between dictionary attack and brute force attack ?

(c) RSA (Rivest-Shamir-Adleman) algorithm is asymmetric cryptography algorithm. Write down the steps of RSA algorithm. **5+6+7**

3. (a) Biometric authentication is the process of verifying your identity using measurements or other unique characteristics of body. How does biometric authentication work ? What are the types of it ? Write down the advantages and disadvantages of biometric authentication.

(b) What is encryption and decryption ? By taking suitable example, explain Symmetric-Key Encryption and Public-Key Encryption. What is relation between key Length and Encryption Strength ? **9+9**

4. (a) IT security is a concern for every business. Write any six best practices to establish security policy.

(b) The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. Explain overall structure of data encryption standard.

(c) What is Session Hijacking? What are different ways of session hijacking? What are counter measure to prevent session hijacking ? **6+6+6**

5. (a) Incident handling is a generalized term that refers to the response by a person or organization to an attack. Write down five steps of incident handling.

(b) Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. What is property of elliptic curve so that it is being used in cryptography ?

(c) Differentiate between Block Cipher and Stream Cipher with respect to following points. Basic, Complexity, Number of bits used, Confusion and Diffusion, Algorithm modes used, Reversibility, Implementation. **5+6+7**

6. (a) What does Cryptanalysis mean ? Write down types of Cryptanalysis.

(b) Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Write in a brief: attributes of information security.

(c) Information Security Risk Management (ISRM) is the process of managing risks associated with the use of information technology. What are the stages of risk assessment ? **6+6+6**

7. Explain in Brief (Any three).

(a) Virus

(b) Worms

(c) Trojan

(d) Spyware **6+6+6**

- o 0 o -