

Con. 2752-09.

VR-4182

(Library)

(REVISED COURSE)

(3 Hours)

[Total Marks : 100]

- N.B. :**
- (1) Question No.1 is **compulsory**.
 - (2) Attempt any **four** questions out of remaining **six** questions.
 - (3) **Figures** to the **right** indicate **full** marks
 - (4) Answers to the questions should be **grouped** and written **together**.
 - (5) Assume any **suitable data** wherever **required** but **justify** the **same**.
1. (a) What is Brain Virus ? How it passes on its infection ? 5
 - (b) Compare signature-based and anomaly-based IDS. What the strengths and limitations of IDS ? 5
 - (c) List two disadvantages of each of the following :— 5
 - (i) Physical separation
 - (ii) Temporal separation in computing system.
 - (d) How is the encryption key generated from password in Kerberos ? 5
 2. (a) (i) Compare Secret Key and Public Key encryption in terms of number of keys, Protection of key, Best uses, Key distribution and Speed. 5
 - (ii) List and briefly define three applications of a public-key cryptosystem. 5
 - (b) In RSA system, the public key of a given user is $e = 7$, and $n = 187$. 4
 - (i) What is the private key of this user ? 4
 - (ii) You intercept the ciphertext $C = 11$ sent to a user whose public key is $e = 7$, and $n = 187$.
What is the plaintext M ? 4
 - (iii) What are two possible approaches to defeating the RSA algorithm. 2
 3. (a) List and explain the various malicious and non-malicious codes with examples. 10
 - (b) Which are the three types of controls against program threats ? Explain each with examples. 10
 4. (a) What is file protection mechanism ? List and Compare the basic forms of protection ? 10
 - (b) Describe each of the following four kinds of access control mechanisms in terms of (1) ease of determining authorized access during execution, (2) ease of adding access for a new subject, (3) ease of deleting access by a subject, and (4) ease of creating a new object to which all subjects by default have access. 10
 - (i) per-subject access control list
 - (ii) per-object access control list
 - (iii) access control matrix
 - (iv) capability.

[TURN OVER

Con. 2752-VR-4182-09.

2

5. (a) What is inference problem ? Which are the various ways to determine the sensitive data values from a database using inference problem ? **10**
- (b) What are the basic requirements for database security ? Briefly examine each of the requirement. **10**
6. (a) What is denial of service attack ? What are the way in which an attacker can mount a DOS/DDOS attack on the system ? **10**
- (b) List the threats to E-Mail and what the various requirements and solutions for secure E-Mail. **10**
7. (a) Compare copyright, patent and trade secret in terms of protects, protected object made public, requirement to distribute, ease of filling, duration and legal protection. Which are the various issues relating to information ? **10**
- (b) Explain the basic steps of risk analysis. **10**