[Total No. of Questions - 9] [Total No. of Printed Pages - 2]

MAY-24-1054

MCA-6206(iii) (Information Security)

MCA-2nd CBCS/NEP

Time : 3 Hours **Max. Marks : 60**

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note: Attempt five questions in all, selecting one question each from Section A, B, C and D. Section E is compulsory.

Section A

1. a. What is the difference between passive and active security threats? Explain at least five attacking techniques and show whether they are active or passive attack. (8)

   b. What is **CIA** security goal? (4)

OR

2. a. Explain the role of certification authority. (6)

   b. What is hash function? Explain the properties of hash function. (6)

Section B

3. a. What is user authentication? Consider A is a user and B is a service providing server, and RC a registration server. Explain a scenario of authentication between A and B. You can use any number of factors (password, biometric etc.). (6)

   b. Explain vulnerabilities of password-based authentication. Explain a method to remove these vulnerabilities. (6)

OR

4. a. Explain Role based access control policy for bank. (6)

   b. What is access control policy? Explain the access rights for a user of a system. (6)

Section C

5. a. Explain Service layer of cloud service. (6)

   b. Explain NIST Guidelines on Cloud Security and Privacy Issues and Recommendations. (6)

OR

6. What is the difference between DoS attack and a distributed DoS attack? Explain, in brief, how an attacker performs these attacks. Also, explain the techniques to resist these attacks. (12)

Section D

7. a. Explain environmental threats, technical threat and human caused threat. (8)

   b. What are the Personal Identity Verification credentials used in physical access control system? (4)

OR

8. Explain Integration of physical and logical security. (12)

Section E (Compulsory)

9. (i) Explain a symmetric key encryption algorithm with example. (6)

   (ii) What is the basic difference between digital signature scheme and public key encryption technique? (6)