MCA.IV/05.14.0498

D

MCA DEGREE IV SEMESTER EXAMINATION MAY 2014

CAS 2404 SECURITY IN COMPUTING

(Regular)

Time: 3 Hours Maximum Marks : 50

PART A

(Answer *ALL* questions)

(15 x 2 = 30)

I. (a) Mention about security goals.
(b) Distinguish vulnerability and threat.
(c) Consider a program that allows a surgeon in one city to assist in an operation on a patient in another city via an internet connection. Who might want to attack the programme? What types of harm might they want to cause?

II. (a) What characteristics would make an encryption absolutely unbreakable? What characteristics would make an encryption impractical to break?
(b) Describe strengths of DES.
(c) Decrypt the following encrypted quotation using Ceasar cipher
fqjcb rwjwj vnjax bnkhj whxcq nawjv
nfxdu mbvnu ujbbf nnc

III. (a) Describe the following access control mechanisms in terms of
(i) ease of determining authorized access during execution (ii) ease of deleting access by a subject:
(1) Access control matrix
(2) Capability matrix
(b) Does the standard Unix operating system use a nondiscretionary access control? Explain your answer.
(c) Explain the meaning of the term granularity with reference to access control. Discuss the tradeoff between granularity and efficiency.

IV. (a) Can a database contain two identical records without a negative effect on the integrity of the database? Why or why not?
(b) Explain the disadvantages of partitioning as a means of implementing multilevel security for databases.
(c) What is the purpose of encryption in a multilevel secure database management system?

V. (a) Cite a risk in computing for which it is impossible or infeasible to develop a classical probability of occurrence.
(b) How will citizens create, record and protect their keys?
(c) What legal protections are available to electronic transactions?

PART B

(5 x 4 = 20)

VI. Describe substitution methods and transposition methods with examples.

OR

VII. Explain software vulnerabilities.

VIII. Write a note on malicious software.

OR

IX. Explain how RSA algorithm achieve security goals.

(P.T.O.)

X. Mention security methods available in any one OS.

OR

XI. Explain how a semaphore could be used to implement a covert channel in concurrent processing.

XII. Suppose a database manager was to allow nesting of one transaction inside another. That is, after having updated part of one record, the DBMS would allow you to select another record, update it, and then perform further updates on the first record. What effect would nesting have on the integrity of a database? Suggest a mechanism by which nesting could be allowed.

OR

XIII. Explain email security protocol.

XIV. Prepare an argument for or against the proposition that the following is ethical behaviour. You and some friends decide to share music from CDs. You copy some to your computer and then burn identical copies for your friends. Does the argument change if the exchange is done with unknown people, through an anonymous file-sharing service on the order of Napster?

OR

XV. Describe ownership of products.

***