Reg. No. : | | | | | | | | | | |

Question Paper Code: 22032

M.E. DEGREE EXAMINATION, MAY 2014.

Second Semester

Computer Science and Engineering

01PCS203 - INFORMATION SECURITY

(Regulation 2013)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions.

PART A - (10 x 2 = 20 Marks)

1. What is meant by Protection State?
2. Give the levels of security needed for a medium sized public organization.
3. State the need for key exchange.
4. Define Digital Signatures.
5. Give the names of places where group identity is needed rather than individual identity.
6. What is meant by Fenton's Data Mark Machine?
7. List the characteristics of Malicious Logic.
8. Write short notes on Anomaly Modeling.
9. Mention the need for security to server systems.
10. Classify the computer users based on the types of security requirements.

PART - B (5 x 14 = 70 Marks)

11. (a) Explain in detail the access control matrix and security policies. (14)

Or

(b) Discuss the confidentiality policies and hybrid policies. (14)

12. (a) Describe in detail about the key management of session and interchange keys. (14)

Or

(b) Briefly explain the cryptographic key infrastructure and cipher techniques. (14)

13. (a) Describe the implementation of access control mechanisms in detail. (14)

Or

(b) Explain the information flow and confinement problem with suitable examples. (14)

14. (a) Describe different approaches for vulnerability analysis and list out the classifications of vulnerability. (14)

Or

(b) Describe the design of an auditing system and organization of intrusion detection systems. (14)

15. (a) Describe in detail about the network organization and authentication. (14)

Or

(b) Discuss in detail the common security - related programming problems and available solutions. (14)

PART - C (1 x 10 = 10 Marks)

16. (a) Consider the following authentication protocol, which uses the classical cryptosystem. Alice generates a random message *r*, enciphers it with the key *k* she shares with Bob and sends the enciphered message {*r*} *k* to Bob. Bob deciphers it, adds 1 to r and sends {r + 1} *k* back to Alice. Alice deciphers the message and compares it with *r*. If the difference is 1, she knows that her correspondent shares the same key *k* and is therefore Bob. If not, she assumes that her correspondent does not share the key *k* and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not? (10)

Or

b) Give reasons why *root* should not be able to change the audit UID on a UNIX system and give reasons why it should. Which reasons sound more persuasive to you? (10)