

FACULTY OF INFORMATICS

B.E. 4/4 (IT) I Semester (New) (Suppl.) Examination, July 2010

Subject: Information Security (Elective – III)

Time: 3 Hours

Max. Marks : 75

Note: Answer all questions from Part A. Answer any **Five** questions from Part B.

PART – A (25 Marks)

VASAVI LIBRARY

1. Distinguish between security blue print and security model. (2)
2. How does the attacker take advantage of Buffer Overflow? (3)
3. Write about Information Warfare. (3)
4. Describe risk transference. (3)
5. Why is shaping a policy difficult. (2)
6. Write about the network tool packet sniffer. (3)
7. Define the terms encryption and decryption. (2)
8. Differentiate public and private key cryptography. (2)
9. Comment on the strength of DES. (2)
10. List the services provided by SSL record protocol to SSL connections. (3)

PART – B (50 Marks)

- 11.a) Explain in detail the different phases of Security Systems Development Life cycle.
- b) How does the present day VLSI technology and speed of CPU impact the protection of Information
12. State and explain the components of asset valuation.
13. Define a firewall. Examine different firewall architectures in detail.
14. Write about the business requirements for SET and its key features along with the participants of SET.
15. Explain the process involved in generating a 160-bit message digest using SHA-1 algorithm.
16. How is AES different from DES? Briefly write the AES algorithm.
17. Write about any two of the following:
 - a) Compromises to Intellectual Property.
 - b) Intrusion Detection System.
 - c) Basic principle of RSA algorithm.