Code No.: 3172

FACULTY OF INFORMATICS

B.E. IV/IV Year (IT) I Semester (Main) Examination, December 2010

INFORMATION SECURITY

(Elective - II)

Time : 3 Hours] [Max. Marks : 75

PASAVI LITHO

Part A — (Marks : 25)

Answer **all** *question from Part A.*
Answer any **five** *questions from Part B.*

1. What are the activities performed during the maintenance phase of the Sec SOLC? 3
2. List the components of an Information System. 2
3. Differentiate with an example between a law and ethic. 2
4. Enumerate the conditions under which a policy can be enforced. 3
5. In the context of information security, explain the significance of a DMZ. 3
6. How does the use of a proxy server enhance the level of security protection to a network? 2
7. Differentiate between a monoalphabetic & Polyalphabetic substitution ciphers. 2
8. Discuss the implementation of digital signatures. 3
9. What is a message digest? 2
10. How is SSL used to enhance the level of security of Internet communications? 3

Part B — (Marks :50)

11. (a) Discuss the various types of deliberate software attacks designed to damage, destroy, or deny service to target systems? 6

    (b) How can the threats proved by social engineering to information security be overcome. 4

12. Discuss the various risk control strategies in an organization. 10

13. (a) With the help of a diagram discuss the security architecture of an organization that incorporates defence in depth. 6

    (b) Discuss the use of intrusion detection systems to enhance the level of information security protection. 4

[P.T.O.

14. Explain in detail the RSA algorithm and its working. 10

15. (a) How does SET provide protection? 6

(b) Explain the operation of SHA-1 algorithm in the implementation of a message desert. 4

16. (a) Explain the inadequacy of DES as an encryption algorithm. 5

(b) Discuss how Public Key infrastructure enables the protection of information assets. 5

17. Write short notes on (any **two**): 10

(a) AES

(b) Firewalls

(c) Balancing of Security of Information access.