Code No.: 3157

FACULTY OF ENGINEERING

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

INFORMATION SECURITY

(Elective – I)

Time : 3 Hours] [Max. Marks : 75

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

Part A — (Marks : 25)

1. What are the three main goals of information security?
2. What are different order of data ownership?
3. What is Kennedy – Kassebaun Act?
4. How does network – based IDS differ from host – based IDS?
5. What type of policy would be needed to guide use of the web? E- mail? Office equipment for personnel use.
6. What are non –discretionary controls?
7. Is AES is more secure to attack than DES? Justify your answer.
8. What is timing attack in R.S.A?
9. What are the weaknesses of SSL?
10. In what was does message digest provide belts integrity check than a check sum such as internet checksum?

Part B — (Marks : 5 × 10 =50)

11. (a) Describe critical characteristics of information. How are they used in the study of computer security?

    (b) What are the types of password attacks? What can a system administrator do to protect against them?

12. (a) What are three general categories of unethical and illegal behaviour?

    (b) What are vulnerabilities? How do you identify them?

[P.T.O.

13. (a) List four ways to categorize risk controls.

    (b) What are the three types of security policies where would each be used?

14. (a) What is RADIUS? What advantage does it have over TACACS?

    (b) What is meant by the term "perimeter" ? Explain the need for perimeter security?

15. (a) With suitable diagrams, explain the working of symmetric and asymmetric encryption methods.

    (b) What is the difference between authentication and authorization?

16. (a) Explain keys transformation in DES.

    (b) What basic arithmetic and logical functions are used in MD5 and SHA – 1?

17. Write short notes on:

    (a) Risk appetite

    (b) SSL Record protocol

    (c) Replay attack.
