B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2011.

Seventh Semester

Information Technology

IT 2042 — INFORMATION SECURITY

(Regulation 2008)

Time : Three hours   Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is information security?

2. Why is a methodology important in implementing the information security?

3. Why is information security a management problem?

4. Distinguish between DoS and DDoS.

5. What is risk management?

6. What is the difference between benchmark and baseline?

7. What is information security policy?

8. What are the inherent problems with ISO 17799?

9. Distinguish between symmetric and asymmetric encryption.

10. What are the credentials of information security professionals?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Describe the critical characteristics of information. How are they used in the study of computer security?   (8)

    (ii) Explain the security system development life cycle in detail.   (8)

Or

(b) (i) Explain the NSTISSC security model and the top-down approach to security implementation. (8)

(ii) Briefly explain the components of an information system and their security. (8)

12. (a) (i) Explain the various groups of threats faced by an organization. (8)

(ii) Discuss the ethical concepts in information security and the prevention to illegal and unethical behavior. (8)

Or

(b) (i) Explain the four important functions of information security in an organization. (8)

(ii) Describe the attack replication vectors and the major types of attacks. (8)

13. (a) (i) Describe the process of risk identification in detail. (8)

(ii) Discuss the risk control strategies that guide an organization. (8)

Or

(b) (i) Discuss the risk assessment and the documentation of its results. (8)

(ii) Explain the various feasibility studies considered for a project of information security controls and safeguards. (8)

14. (a) (i) Explain the different types of information security policies. (8)

(ii) Discuss the features of VISA international security model. (8)

Or

(b) (i) Explain the NIST Security model in detail. (8)

(ii) Explain the various components used in designing the security architecture. (8)

15. (a) (i) Discuss the different types of intrusion detection systems. (8)

(ii) Describe the access controls used for providing physical security. (8)

Or

(b) (i) Write notes on scanning and analysis tools used during design. (8)

(ii) Discuss the cryptographic tools used for providing the security. (8)