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

C 3183

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2008.

Seventh Semester/Eighth Semester

Computer Science and Engineering

CS 1014 — INFORMATION SECURITY

(Common to Information Technology)

(Regulation 2004)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — ($10 \times 2 = 20$ marks)

1. Production vs Availability – Justify.

2. Draw NSTISSC security model.

3. Differentiate ethical and professional issues in security investigation.

4. Distinguish among vulnerability, threat and attacks.

5. Write the important risk factors of information security.

6. What do you mean by risk identification?

7. List any four Information Security Policies.

8. What is meant by International security Model?

9. What do you mean by false positive and false negative in IDS?

10. What is Hash functions? Where it is used in security?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Briefly discuss about security system development lifecycle model. (10)

(ii) What is information security? Discuss critical characteristics of information elaborately. (6)

Or

(b) (i) Describe Balancing information security and access. With real time example.

(ii) What are the roles involved in a project team? Where it provides security solutions for an application. Discuss.

12. (a) (i) Discuss briefly about acts of human error or failure, which includes acts performed without malicious intent.

(ii) Consider a program, to display on your website, city's current time and temperature. Who might want to attack your program? What type of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?

Or

(b) (i) Define policy vs Law. Describe 10 commandments of computer ethics.

(ii) Consider a program to accept and tabulate votes in election. Who might want to attack the program? What type of harm might they want to cause? What kinds of vulnerabilities might they exploit to cause harm?

13. (a) (i) How do you categories the components of an information system? Explain.

(ii) What do you mean by access control? Describe the different types of access control and risk control strategies.

Or

(b) (i) Describe the different categories of controls, with an example.

(ii) What is cost benefit analysis? Describe risk residual of information asset.

14. (a) (i) Compare the Issues – Specific Security Policy (ISSP) and System Specific Policies (SysSP). (8)

(ii) Describe NIST security models. (8)

Or

(b) (i) Explain clearly about spheres of security for a blue print of an Information security system. (8)

(ii) Explain contingency planning Timeline of IRP, DRP and BCP. (8)

15. (a) (i) Why the product of 2 relatively simple ciphers, such as a substitution and a transposition can achieve a high degree of security? Discuss. (8)

(ii) Describe briefly about different types of IDS and detection methods. (8)

Or

(b) (i) What do you mean by physical access controls and discuss the controls for protecting the secure facility with examples.

(ii) Describe public key and private key with an example.
