8/12/14 FN
IT D

Reg. No. :

**Question Paper Code : 91556**

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2014.

Eighth Semester

Computer Science and Engineering

IT 2042/IT 706/10144 CSE 58/10177 ITE 33 — INFORMATION SECURITY

(Common to Seventh Semester Information Technology)

(Regulation 2008/2010)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What type of security was dominant in the early years of computing?

2. Who should lead a security team? Should the approach to security be more managerial or technical?

3. What are the types of password attack? What can a systems administrator do to protect against them?

4. What are the three general categories of unethical and illegal behavior?

5. What are vulnerabilities? How do you identify them?

6. What is cost benefit analysis?

7. What are the inherent problems with ISO 17799, why hasn't the U.S adopted it? What are the recommended alternatives?

8. What is firewall? How does it differ from gateway?

9. What is the difference between digital signatures and digital certificates?

10. What are some of the factors that influence an organization's information security hiring decisions?

PART B — (5 × 16 = 80 marks)

11. (a) Identify the five components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?

Or

(b) Explain and discuss the difference between Systems Development Life Cycle (SDLC) and Security Systems Development Life Cycle (SecSDLC).

12. (a) Explain Denial-of-service (DoS) and Distributed Denial-of-Service (DDoS) attacks with neat sketch.

Or

(b) Briefly explain about any five information security professional organizations with their role and motivation.

13. (a) Explain the components of risk identification with neat Illustration.

Or

(b) Write the difference between quantitative and qualitative risk control practices with respect to suitable metrics.

14. (a) Briefly describe the Enterprise Information Security Policy and Issue Specific Security Policy.

Or

(b) (i) List the contents of NIST security publication NIST SP 800-14. (8)

(ii) Describe the various processes involved in Business Impact Analysis (BIA). (8)

15. (a) Discuss about the different types of intrusion detection and prevention systems with suitable examples.

Or

(b) (i) Explain the working model of single round DES encryption algorithm with neat sketch. (8)

(ii) What is the relationship between HVAC and physical security? What four physical characteristics of the indoor environment are controlled by a properly designed by HVAC system? (8)