

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : 50813

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2023.

Eighth Semester

Information Technology

IT 8073 – INFORMATION SECURITY

(Common to : Computer Science and Engineering/Computer and Communication Engineering)

(Regulations 2017)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Differentiate direct and indirect attacks.
2. List the characteristics of CIA triangle.
3. What is meant by the term "Information Extortion"?
4. Write any two the major differences between a Threat and an Attack.
5. Define the four communities of interest responsible for addressing all levels of risk.
6. Distinguish between asset's ability to generate revenue and its ability to generate profit.
7. Express significant points in Information Security Blueprint.
8. List any five goals of Information Security Governance.
9. Differentiate Cryptography and Steganography.
10. Differentiate signature-based IDPS and behavior-based IDPS.

PART B — (5 × 13 = 65 marks)

11. (a) Evaluate the various components of Information Security that a successful organization must have. (13)

Or

- (b) Illustrate briefly about SDLC waterfall methodology and its relation in respect to information security. (13)

12. (a) Analyze in detail about Ethics, legal and professional issues in Information Security. (13)

Or

- (b) Illustrate which management groups are responsible for implementing information security to protect the organization's ability to function. (13)

13. (a) Discuss in detail about identifying and assessing risk in Risk Management. (13)

Or

- (b) Describe and draw the components of Access Control Mechanism. (13)

14. (a) Analyze what Web resources can aid an organization in developing best practices as part of a security framework? (13)

Or

- (b) (i) Explain with a diagram about the guidelines, purposes used to achieve using ISO/IEC 17799. (6)

- (ii) Illustrate where can a security administrator find information on established security frameworks? (7)

15. (a) Examine Strengths and Limitations of IDS. (13)

Or

- (b) (i) List and explain the tools used in cryptography. (7)

- (ii) Explain Man-in-the middle attack. (6)

PART C — (1 × 15 = 15 marks)

16. (a) Formulate any methodology and explain why it is important in the implementation of information security? How does a methodology improve the process? (15)

Or

- (b) Evaluate how does a network-based IDPS differ from a host-based IDPS? (15)