[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 5053 **L**

Unique Paper Code : 2344000031

Name of the Paper : Information Security

Name of the Course : **B.Sc. (H) CS (General Elective)**

Semester : VIII

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **Section A** is compulsory.
3. Attempt any **four** questions from **Section B**.
4. Answer **all** parts of a question together.

Section A

Q1. (a) Distinguish between active and passive attacks. Which type of attack is more difficult to detect? Justify your answer. (3)

(b) Consider an e-commerce website. Identify any two potential vulnerabilities and explain the corresponding attacks that may be carried out by exploiting them. (3)

(c) What is a hash function? State any two properties. (3)

(d) Differentiate between cryptanalysis and brute-force attack. (3)

(e) Explain why Role-Based Access Control (RBAC) is considered suitable for database access control. (3)

(f) Distinguish between a SYN flooding attack and a SYN spoofing attack. (3)

(g) Explain the inference problem in databases with a simple example. (3)

(h) Describe any three wireless security measures employed to deal with wireless transmissions. (3)

(i) Identify and explain the key characteristics of an Advanced Persistent Threat (APT) that justify its name. (3)

(j) Differentiate between a Distributed Denial-of-Service (DDoS) attack and a classic Denial-of-Service (DoS) attack. Why are DDoS attacks considered more potent than classic DoS attacks? (3)

Section B

Q2. (a) For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers. (8)

(i) An organization managing public information on its Web server.

(ii) A law enforcement organization managing extremely sensitive investigative information.

(iii) A financial organization managing routine administrative information (not privacy related information).

(iv) An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

(b) Discuss the propagation mechanisms of viruses, worms, and Trojans. Compare their behavior and impact on systems. (7)

Q3. (a) Describe the concept of trusted systems. Explain the role and properties of a reference monitor with suitable justification. (8)

(b) List and briefly define the fundamentals security design principles. (7)

Q4 (a) Explain the following terms: backdoor, bot, keylogger, spyware, and rootkit. Distinguish between them. Can these components coexist within a single program? Justify your answer. (8)

(b) Define security intrusion and intrusion detection. Discuss the classification of Intrusion Detection Systems (IDS) and describe the key components of an IDS architecture. (7)

Q5 (a) Explain buffer overflow attacks and discuss various run-time defenses against them. (8)

(b) Compare confidentiality and integrity models in computer security. Give an example of each. (7)

Q6. (a) An organisation is migrating its customer database to a public cloud. Identify four cloud specific security specific threats it should prepare for. For any two threats, recommend counter measures and justify your choice. (8)

(b) Explain the main components of Identity, Credential, and Access, Management (ICAM). (7)

Q7. (a) Write short note on any five of the following: (3X5)

(i) Message Authentication Code (MAC)

(ii) WPA2

(iii) Shell Code

(iv) Digital Signatures

(v) SQL-Based Access Control

(vi)Honeypot