7. (a) Explain four ethical considerations in data collection. Describe how these ethical considerations can be addressed in practice. (8)

(b) Write short notes on :

(i) Active and Passive Attacks

(ii) Cyber Crime

(iii) Cyber Espionage (3+2+2=7)

[This question paper contains 8 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 5728 **L**

Unique Paper Code : 2344000035

Name of the Paper : Data Privacy

Name of the Course : **Computer Science – Generic Elective**

Semester : VI

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 **4** questions from **Section B**.
4. All parts of a question must be answered together.

Section – A

1. (a) Justify the statement- "Privacy and Anonymity are two sides of the same coin." (3)

   (b) Explain the concept of Collision Resistance in Cryptographic Hash Function. How many bits are there in SHA-256? (3)

   (c) What do you understand by the term "Purpose Limitation" under the GDPR? (3)

   (d) What are the challenges in anonymizing graph data? (3)

   (e) State three rights available to a Data Subject under the GDPR. (3)

   (f) Explain how Public Key Infrastructure (PKI) is used to establish trust in the identity of a communicating party. (3)

   (g) Define Personal Data Breach as per the DPDP Act. Briefly explain the timeline for reporting such a breach. (3)

   (b) Compare Symmetric and Asymmetric cryptographic techniques with the help of a suitable diagram. (6)

6. (a) Compare and contrast Privacy-by-Design (PbD) and Security-by-Design (SbD). Highlight at least four key differences in their scope, objectives, and implementation approaches within an organization.

   Give an example of a practice that satisfies both PbD and SbD simultaneously. (8)

   (b) For any robust hash function, define the following terms :

      (i) Pre-image Resistance

      (ii) Second Pre-image Resistance

      (iii) Collision Resistance

   Explain why a weakness in Collision Resistance is particularly devastating for the integrity of a system that uses digital signatures. (7)

(b) What do you understand by the term CIA Triad? Explain briefly. (7)

4. (a) Encrypt the plaintext: "DEFENDTHEWALL" using the following encryption techniques :

(i) Caesar-cipher with key 7

(ii) Rail-Fence cipher with 3 rails (6)

(b) Describe the Model Surveillance System with the help of a diagram. (9)

5. (a) How does anonymization help in ensuring data privacy? Explain the following anonymization techniques : (9)

(i) Generalization

(ii) Suppression

(iii) k-anonymity

(iv) 1-diversity

(h) Why is it important to have a balance between privacy and utility? (3)

(i) Explain Denial of Service (DoS) attack with the help of a suitable example. (3)

(j) Why is Personally Identifiable Information (PII) considered the most sensitive type of data? An online learning platform collects the following data from students : (3)

- Student Name
- Age
- Courses Enrolled

Identify which data is PII. Justify your answer.

Section – B

2. (a) Under the DPDP Act 2023, define the term Data Processor and briefly explain their responsibilities. (5)

(b) Based on the case studies below, identify the relevant section(s) or key provision(s) of the DPDP Act that are violated or applicable.

For each case, briefly describe the section(s) and explain why they apply. (6)

(i) A health insurance company discovers that a third-party vendor hired to process claims has experienced a significant security incident exposing the health records of thousands of policyholders. The insurance company refuses to take responsibility, claiming the vendor is solely liable for the breach.

(ii) A local e-governance portal automatically sets the language preference of a new user based on their IP address and stores this preference without informing the user or providing an easy way to opt-out of this tracking.

(iii) A social media platform continues to store and process the chat history and personal details of users after the users explicitly withdrew their consent for data processing and requested their data be erased.

(c) Explain the following terms with suitable examples :

(i) Explicit Identifier

(ii) Quasi Identifier (4)

3. (a) Briefly explain the roles of the following components in Public-Key Infrastructure (PKI) architecture :

(i) Certification Authority (CA)

(ii) Registration Authority (RA)

(iii) Repository

(iv) Relying Party (8)