[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 7288 **L**

Unique Paper Code : 2343010010

Name of the Paper : Data Privacy

Name of the Course : **B.Sc. (Hons.) Computer Science - DSE-NEP-UGCF**

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. Question No. 1 is compulsory in Section-A.
3. Attempt any four questions from Section-B.
4. Parts of a question should be attempted together.

SECTION A

Q1.

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

(b) Explain Explicit and Quasi identifiers with examples. (3)

(c) Differentiate between Imprecise and Insecure use of Data. (4)

(d) Define Digital signatures. How are digital signatures created and verified? (4)

(e) Differentiate between active and passive attacks with examples. (4)

(f) Explain the concept of the "Right to Privacy" and its relevance in the digital age. (4)

(g) A healthcare organization collects large amounts of patient information containing multiple attributes such as age, disease history, treatment details, and social connections among patients and doctors. Before sharing the data for research purposes, the organization wants to protect the privacy of individuals while still keeping the data useful for analysis. (4)

Based on the above situation, explain the challenges involved in preserving privacy in:

(i) Multidimensional data
(ii) Graph data.

(h) Define PII. What is the goal of privacy by design in dealing with privacy of PII? (4)

SECTION B

Q2. (a) (i) Define a Security Service. Describe important security services. (5)

(ii) Compare Symmetric and Asymmetric encryption techniques with their diagrams. (4)

(b) Give the principles of General Data Protection Regulation (GDPR). (6)

Q3 (a) Define Data Processor as per the DPDP Act. Briefly explain how its responsibilities differ from those of a Data Fiduciary. (5)

(b) (i) List and briefly describe the main objectives of GDPR. Also, explain the key responsibilities of the Data Protection Officer (DPO) in an Organization. (5)

(ii) Explain the concept of "Transparency', 'Consent' and 'Fair Processing' with respect to GDPR. (5)

Q4. (a) Read the following situations and answer the questions:

A company's website suddenly becomes unavailable because a large number of fake requests are sent to its server at the same time. In another incident, an attacker captures a user's login information during an online transaction and later reuses the same information to gain unauthorized access. The company also discovers that one employee installed a free software program that secretly damaged files and allowed unauthorized access to the system.

Based on the above situations, answer the following:

(i) Identify and define the attack in which the website becomes unavailable due to excessive fake requests. Is it an active attack or a passive attack? Give a reason. (3)

(ii) Identify and define the attack in which captured login information is reused by the attacker. Is it an active attack or a passive attack? Give a reason. (3)

(iii) Identify and define the attack in which captured login information is reused by the attacker. Is it an active attack or a passive attack? Give a reason. (3)

(b) How are authenticity, integrity, and non-repudiation preserved with the use of Digital Signatures? (6)

Q5. (a) Explain the CIA triad with respect to Data Security. Draw a diagram for it. (5)

(b) Define a cryptographic hash function. Also, discuss the purpose of using a cryptographic hash function in digital signatures and message integrity? (5)

(c) What are the essential components of Public-Key Infrastructure (PKI) Architecture? Explain each of them. (5)

Q6. (a) For each of the following, state whether it qualifies as PII and justify your answer: (5)

(i) Your Passport number
(ii) Browser cookies
(iii) Your full name
(iv) Your email address
(v) Your health records

(b) A banking application stores customer passwords using a cryptographic hash function. One day, a security analyst discovers that if two different inputs can produce the same hash value, an attacker may create a fake password or modified file that appears genuine to the system. (4)

Based on the above situation, answer the following:

Why should a cryptographic hash function be collision-resistant? How does this property help in maintaining system security?

(c) Explain the role of the following stakeholders in Data privacy organization: (6)

(i) Customer
(ii) Data Analyst
(iii) Business operation Employee
(iv) Data Anonymizer

Q7. Write short note on the following:

(a) Model Surveillance System (5)

(b) Different methods of protecting data (5)

(c) Different anonymization techniques (5)