15599

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Tech.(CSE)-DS-2021/B.Tech.(CSE)-DS-2022
Course Name – Information Security and Privacy
Course Code - OEC-CSD701C
(Semester VII)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Identify the perturbative microdata masking technique that involves altering original data values.
a) Data suppression b) Data swapping
c) Generalization d) Noise addition

(ii) Identify the primary goal of using data swapping in microdata masking.
a) To remove all identifiers from the dataset b) To preserve exact data values while maintaining privacy
c) To aggregate data into broader categories d) To exchange data values between records to protect confidentiality

(iii) Select the security device which is commonly used to monitor and control incoming and outgoing network traffic based on predetermined security rules
a) Intrusion Detection System (IDS) b) Firewall
c) Antivirus software d) Encryption algorithm

(iv) Identify type of attack that is mitigated by using HTTPS instead of HTTP:
a) Cross-site scripting (XSS) b) SQL injection
c) Man-in-the-middle attack d) Denial of Service (DoS)

(v) Select the challenge that involves ensuring systems remain operational despite disruptions:
a) Availability b) Authentication
c) Integrity d) Confidentiality

(vi) Identify the service that ensures data is not altered during transmission:
a) Authorization b) Authentication
c) Encryption d) Backup

(vii) Identify the correct approach to classify data in a multidimensional dataset for anonymization purposes.
a) By randomly assigning labels b) By grouping similar records into categories

28- 348

c) By sorting data in alphabetical order
d) By aggregating all numerical data

(viii) Identify the main purpose of l-diversity in data anonymization.

a) To ensure that sensitive attributes in a dataset have at least l different values within each group.
b) To limit the number of attributes in a dataset to l.
c) To classify data into l distinct categories.
d) To reduce the dimensionality of the dataset.

(ix) Select the primary function of a monitoring system in network security:

a) Encrypt sensitive data
b) Detect and alert on anomalies and security breaches
c) Create user accounts
d) Install security patches

(x) Identify the best practice for backing up configurations of security devices:

a) Backup the configurations manually once a year
b) Use automated backup tools and schedule regular backups
c) Store backups on the security device itself
d) Backup configurations only after a system failure

(xi) Identify the type of control used to prevent unauthorized access to a server:

a) Detective Control
b) Preventive Control
c) Corrective Control
d) Compensating Control

(xii) Identify one of the main limitations of k-anonymity as a data anonymization technique.

a) It does not protect against attribute disclosure.
b) It requires the dataset to be encrypted.
c) It increases the risk of re-identification.
d) It is difficult to implement on small datasets.

(xiii) Choose the correct statement related to k-anonymity, l-diversity, and t-closeness.

a) t-Closeness provides the strongest privacy protection but may reduce data utility more than k-anonymity and l-diversity.
b) k-Anonymity always provides better data utility than l-diversity.
c) l-Diversity and t-closeness are only applicable to numeric datasets.
d) k-Anonymity protects against all types of re-identification risks.

(xiv) Select the correct example of a social engineering attack.

a) Phishing
b) SQL Injection
c) Denial of Service
d) Man-in-the-Middle

(xv) Identify a key benefit of multi-factor authentication (MFA).

a) Speed
b) User convenience
c) Increased security
d) Low cost

Group-B

(Short Answer Type Questions)

3 x 5=15

2. Explain the importance of balancing data privacy and utility. (3)
3. Explain the need for estimating re-identification risk in microdata. (3)
4. List two methods used in perturbative microdata masking. (3)
5. Discuss the importance of 'incident response' in information security management. (3)
6. Discuss different types of Hacking in brief. (3)

OR

Estimate the strategies of effective Network Security. (3)

Group-C

(Long Answer Type Questions)

5 x 6=30

7. Define Computer Security and list the objectives of information security (5)
8. List and explain the major causes of Information Loss in Microdata. (5)

9. Evaluate the effectiveness of Intrusion Detection Systems (IDS) in identifying security breaches and suggest improvements for modern systems. (5)
10. Evaluate the use of automated tools for security assessment and explain how they improve system security. (5)
11. Differentiate between an attack surface and an attack tree. (5)
12. Analyze the role of firewalls in protecting organizational networks. (5)

OR

Analyze common system vulnerabilities and describe the potential impact they have on organizational security. (5)

****