15610

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Tech.(CSE)-DS-2022
Course Name – Data and Internet Security
Course Code - PEC-CSD702C
(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) Name the most common type of data security breach.
a) Phishing attack. b) Natural disaster.
c) Power outage. d) Software update.

(ii) Select the correct definition of access control.
a) Restricting unauthorized access to systems and data. b) Making systems open to all.
c) Encrypting data automatically. d) Backing up data regularly.

(iii) State the property of a one-way function that makes it difficult to reverse.
a) Collision resistance b) Pre-image resistance
c) Symmetric key usage d) Randomness

(iv) Illustrate how a hash function supports password verification.
a) By encrypting passwords for secure communication b) By mapping a password to a fixed hash value and comparing it
c) By converting hash back into passwords d) By generating keys from passwords

(v) Assess why increasing compute power weakens insecure hash functions.
a) More bandwidth usage b) Easier to brute force collisions
c) Harder to guess inputs d) More storage space needed

(vi) State the purpose of a session key in secure communications.
a) Encrypt one message only b) Reuse across sessions
c) Encrypt data in a single session d) Generate public keys

(vii) Identify the key idea behind zero knowledge proofs.
a) Reveal all data b) Prove knowledge without revealing it
c) Encrypt with zero keys d) Use random padding

(viii) Validation of an HTTPS certificate chain on a browser-
a) Verify DNS records b) Check certificate issuer and expiry
c) Use symmetric key inspection d) Run TCP traceroute

(ix) Mention a common sign of a DoS attack.

a) Increased encryption
b) High CPU usage on client
c) Slow network or server unresponsiveness
d) Decreased DNS traffic

(x) State the role of Intrusion Detection Systems (IDS) on web server.

a) Filter web content
b) Monitor and alert on suspicious activity
c) Compress network data
d) Send automated emails

(xi) Name the attack that exploits server misconfigurations.

a) Buffer overflow
b) Port scan
c) Misconfiguration attack
d) Spoofing

(xii) Interpret the function of an IDS in a corporate network.

a) Encrypts traffic
b) Detects intrusions and alerts admins
c) Improves UI
d) Caches web content

(xiii) Difference between IDS and IPS is:

a) IDS blocks threats actively
b) IPS only logs alerts
c) IDS detects and alerts; IPS detects and blocks
d) Both do the same task

(xiv) Interpret how packet filtering protects networks.

a) Checks DNS requests
b) Allows only specific packets based on rules
c) Compresses packets
d) Spoofs attacker packets

(xv) Identify the effective role of Firewall.

a) View DNS records
b) Run penetration test or packet capture
c) Enable MAC filtering
d) Check encryption method

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Describe chosen plaintext and chosen ciphertext attacks. (3)
3. Define a cryptographic hash function. (3)
4. Demonstrate the use of PRGs in key generation. (3)
5. Illustrate the use of port scanning detection to strengthen server defenses. (3)
6. Critique the effectiveness of PKI in preventing man-in-the-middle attacks. (3)

OR

Assess the effectiveness of firewalls in defending against denial of service attacks. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Judge the impact of cryptographic checksum vulnerabilities on data integrity assurance and suggest improvements. (5)
8. Recall Shamir's Secret Sharing Scheme and explain its role in secure key management. (5)
9. Use a layered defense approach to mitigate denial of service attacks. (5)
10. Propose a design for a hybrid random number generator incorporating hash functions and physical entropy sources. (5)
11. Evaluate the suitability of stream ciphers compared to block ciphers in real-time communication scenarios. (5)
12. Evaluate the role of ECC in modern cryptographic applications compared to RSA. (5)

OR

Judge the impact of weak access control on data confidentiality and organizational security. (5)

****