15905

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – Dip.CSE-2022/Dip.CSE-2023
Course Name – Information Security
Course Code - DCSE-PE502A
(Semester V)

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) Select how hash functions contribute to security.

a) They create digital signatures
b) They encrypt data
c) They provide a unique output for any input
d) They compress files

(ii) Select the purpose of HMAC in cryptographic systems.

a) To create a hash
b) To authenticate a message using a secret key
c) To encrypt messages
d) To generate digital signatures

(iii) Select about Pretty Good Privacy (PGP) that enhances email security.

a) It encrypts only the body of the email
b) It provides end-to-end encryption
c) It compresses the email for security
d) It uses SSL for encryption

(iv) Select the role of TLS in securing online transactions.

a) It encrypts data
b) It authenticates users
c) It manages session keys
d) It provides end-to-end security

(v) Select the purpose of Secure Electronic Transaction (SET) in e-commerce.

a) It secures the entire transaction
b) It encrypts payment information
c) It verifies user identity
d) It manages credit card information securely

(vi) Choose the difference between active and passive intrusion detection.

a) Active IDS takes preventive actions, passive IDS does not.
b) Passive IDS takes preventive actions, active IDS does not.
c) Active IDS only detects, passive IDS takes action.
d) Passive IDS monitors, active IDS alerts on threats.

(vii) Identify viruses that differ from worms in cybersecurity threats.

a) Viruses require a host, worms can replicate independently.
b) Worms require a host, viruses can replicate independently.
c) Viruses can replicate on their own, worms require a host.
d) Worms spread faster than viruses.

(viii) Identify the role of antivirus software in cybersecurity.

a) It detects and removes malicious software.
b) It prevents users from accessing malicious websites.
c) It blocks access to infected devices.
d) It monitors network traffic for suspicious behavior.

(ix) Identify the difference between a packet-filtering firewall and a stateful firewall.

a) Packet-filtering inspects individual packets, stateful tracks state of connections.
b) Stateful firewall inspects individual packets, packet-filtering tracks state of connections.
c) Packet-filtering firewall tracks state of connections, stateful inspects individual packets.
d) Stateful firewall blocks all traffic, packet-filtering allows traffic.

(x) Select the process of building a differential characteristic from the DDT.

a) By chaining differences through S-box layers.
b) It relies on high-probability differences.
c) It builds probable key guesses from differences.
d) It tests key guesses based on observed outputs.

(xi) Select the purpose of using multiple linear approximations in linear cryptanalysis.

a) Multiple approximations increase accuracy.
b) It increases the likelihood of key recovery.
c) It helps eliminate false positives in attacks.
d) Using multiple approximations reduces noise.

(xii) Identify which of the following is not an approach to information security implementation.

a) Bottom-up approach
b) Top-down approach
c) Lateral approach
d) Combined approach

(xiii) Identify the function of a firewall.

a) Virus detection
b) Intrusion
c) Packet filtering and access control
d) Key generation

(xiv) Select the type of attack that uses statistical methods to guess keys.

a) Brute-force
b) Differential cryptanalysis
c) Steganography
d) DOS attack

(xv) Choose the firewall type that monitors the state of active connections.

a) Packet-filtering firewall
b) Stateful inspection firewall
c) Application proxy firewall
d) Static firewall

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Describe the key components of an information system and explain their roles. (3)
3. Explain the term 'Intruders' in cybersecurity. (3)
4. Explain the procedure of spreading of virus through a network. (3)
5. Evaluate the security limitations of DES. (3)
6. Analyse the role of IPSec in securing network traffic. (3)

OR

Analyse the importance of SSL to enhance security in transport layer. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Analyse the role of Secure Electronic Transaction (SET) in e-commerce security. (5)
8. Explain the main types of intruders and how they impact network security. (5)
9. Explain different types of firewalls and their roles in network security. (5)
10. Analyze the role of people and processes in an information system. (5)

11. Explain the difference between chosen-plaintext attacks in Linear and Differential Cryptanalysis. (5)
12. Explain how Differential Cryptanalysis uses differential characteristics to uncover encryption keys. (5)

OR

Explain how Linear Cryptanalysis can be adapted to attack modern symmetric encryption algorithms. (5)

****