BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – Dip.CSE-2022
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) Explain the concept of "security through obscurity.
   a) Protecting information by hiding it
   b) Encrypting information using complex algorithms
   c) Relying on complex passwords for security
   d) Securing information by making it public

(ii) Explain the role of Message Authentication Code (MAC) in data integrity.
   a) It verifies the sender
   b) It ensures data confidentiality
   c) It ensures data integrity
   d) It encrypts the message

(iii) Explain 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

(iv) Explain the role of Transport Layer Security (TLS) in internet communication.
   a) It encrypts emails
   b) It provides a secure channel over an insecure network
   c) It manages encryption keys
   d) It authenticates users

(v) Explain the purpose of Secure Electronic Transaction (SET).
   a) To secure e-commerce transactions
   b) To encrypt all internet traffic
   c) To manage authentication
   d) To hash sensitive data

(vi) Explain how Pretty Good Privacy (PGP) 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

(vii) Explain the role of intrusion detection systems (IDS) in network security.

a) They detect and alert administrators of suspicious activity.
b) They prevent suspicious activity from occurring.
c) They log all user activity for future analysis.
d) They monitor network performance for suspicious changes.

(viii) Explain 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.

(ix) Explain how password management contributes to security.

a) It ensures users create strong and secure passwords.
b) It encrypts passwords for secure storage.
c) It prevents users from using weak passwords.
d) It tracks user behavior to detect password changes.

(x) Explain the process of linear cryptanalysis and its key steps.

a) It relies on finding linear approximations.
b) It exploits biases in S-boxes.
c) It finds statistical patterns in encryption.
d) It maps plaintext patterns to key guesses.

(xi) Explain how linear cryptanalysis exploits statistical biases in block ciphers.

a) It identifies biases in ciphertexts.
b) It depends on linear combinations of bits.
c) It targets the linear propagation of data.
d) It leverages the approximation of XOR operations.

(xii) Explain the significance of a linear approximation in linear cryptanalysis.

a) A linear equation approximating inputs and outputs.
b) A method for simplifying key guesses.
c) A function that approximates cipher behavior.
d) An approximation useful for ciphertext prediction.

(xiii) Explain the targeting of non-linearity by higher-order differential cryptanalysis.

a) Higher-order approaches reveal non-linear structures.
b) Non-linearity resists simple differential attacks.
c) Non-linear relations require advanced cryptanalysis.
d) Non-linear S-boxes resist simple linear attacks.

(xiv) Explain the impact of key schedule weaknesses on linear cryptanalysis.

a) Weak schedules lead to key recovery.
b) Weak key schedules expose vulnerabilities.
c) A weak schedule simplifies linear approximations.
d) Key schedule design impacts linear cryptanalysis.

(xv) Explain the significance of avalanche effect in differential cryptanalysis.

a) It measures the sensitivity to small changes.
b) It shows how differences propagate in encryption.
c) It ensures that ciphertexts behave unpredictably.
d) Avalanche effect ensures diffusion of differences.

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain the difference between active and passive intruders. (3)
3. Explain how a virus differs from a trojan horse. (3)
4. Explain the key challenges in cryptanalysis of the Discrete Logarithm Problem (DLP). (3)
5. Explain the computational complexity involved in breaking DLP in cryptanalysis. (3)

6. Analyse the role of Message Authentication Code (MAC) in message integrity. (3)

OR

Analyse the significance of Secure Hash Algorithm (SHA) in cryptographic systems. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain the main types of intruders and how they impact network security. (5)
8. Explain different countermeasures used to protect against intrusion and virus attacks. (5)
9. Explain different types of firewalls and their roles in network security. (5)
10. Explain how Differential Cryptanalysis uses differential characteristics to uncover encryption keys. (5)
11. Explain the difference between chosen-plaintext attacks in Linear and Differential Cryptanalysis. (5)
12. Analyse the role of Transport Layer Security (TLS) in securing web communications. (5)

OR

Analyse the importance of Kerberos in securing authentication in large organizations. (5)

****