BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Tech.(CSE)-AIML-2021
Course Name – Data and Internet Security
Course Code - PEC-CSM702C
(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) Select the primary goal of data security.
a) Confidentiality b) Speed
c) Scalability d) Accountability

(ii) Identify which of the following ensures data is only accessible by authorized individuals.
a) Integrity b) Confidentiality
c) Availability d) Redundancy

(iii) Identify the process of proving that a user is who they claim to be.
a) Encryption b) Authorization
c) Authentication d) Integrity

(iv) Select the main risk of a chosen ciphertext attack.
a) Data integrity compromised b) Encryption key revealed
c) Encrypted message altered d) Private key revealed

(v) Identify the key characteristic of symmetric key cryptography.
a) Uses different keys for encryption and decryption b) Uses the same key for encryption and decryption
c) Provides digital signatures d) Slower than asymmetric encryption

(vi) Select the hashing algorithm used in Transport Layer Security (TLS).
a) MD5 b) RSA
c) SHA-512 d) SHA-1

(vii) Identify the attack that attempts to find two different inputs that produce the same hash.
a) Brute force b) Birthday attack
c) Man-in-the-middle attack d) Phishing

(viii) Select the hashing algorithm used to verify file integrity during downloads.

a) SHA-1 b) AES
c) MD5 d) RSA

(ix) Identify the term used for transforming data into a fixed-size string using a hash function.

a) Encryption b) Compression
c) Hashing d) Key exchange

(x) Select the advantage of using hashing in digital certificates.

a) Ensures encryption b) Provides file compression
c) Verifies data integrity d) Reduces file size

(xi) Predict which block cipher uses a fixed block size of 128 bits and supports key sizes of 128, 192, and 256 bits.

a) DES b) AES
c) Blowfish d) Twofish

(xii) Choose the primary weakness of ECB mode in encryption.

a) Slow performance b) Lack of diffusion
c) Requires a unique IV d) Sensitive to key size

(xiii) Predict the mode of encryption most suitable for encrypting streaming data.

a) CBC b) ECB
c) OFB d) CFB

(xiv) Choose the block cipher mode that uses an initialization vector (IV) for each block encryption.

a) ECB b) CBC
c) OFB d) CFB

(xv) Predict which stream cipher operates on each bit of plaintext.

a) AES b) RSA
c) RC4 d) DES

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain the role of cryptography in ensuring data integrity. (3)
3. Explain the way by which symmetric ciphers ensure confidentiality during encryption and decryption processes. (3)
4. Write about the role of a private key in a Public Key Signature Scheme. (3)
5. Write about the significance of third parties in Public Key Infrastructure (PKI). (3)
6. Differentiate between a DDoS attack and a phishing attack. (3)

OR

Explain the way by which encryption helps to protect against network threats. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Justify the need for both Intrusion Detection and Intrusion Prevention Systems in a modern cybersecurity strategy. (5)
8. Illustrate the significance of the SHA-3 algorithm compared to its predecessors, SHA-1 and SHA-2. (5)
9. Discuss the role of hash functions in ensuring data integrity and security in internet communications. (5)

10. Summarize the function of digital certificates in public key infrastructure. (5)
11. Develop an explanation of how block ciphers and stream ciphers differ in their encryption processes and usage. (5)
12. Compare cryptographic checksums and HMACs for integrity protection in terms of security guarantees. (5)

OR

Illustrate the encryption process in a symmetric cipher and its relevance to secure communication. (5)

****