# BRAINWARE UNIVERSITY

## Term End Examination 2025-2026
## Programme – MCA-2025
## Course Name – MOOC-Cryptography and Network Security
## Course Code - MCA20408C
## ( Semester II )

**Full Marks : 70** **Time : 3:0 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) Cryptography primarily deals with
  a) Data compression b) Data encryption and decryption
  c) Data storage d) Data mining

(ii) The main goal of cryptography is to ensure
  a) Efficiency b) Confidentiality
  c) Availability d) Scalability

(iii) Which of the following is NOT a security service?
  a) Confidentiality b) Integrity
  c) Authentication d) Compilation

(iv) Classical cryptography mainly uses
  a) Symmetric keys b) Public keys
  c) Quantum keys d) Digital certificates

(v) Caesar cipher is an example of
  a) Transposition cipher b) Substitution cipher
  c) Stream cipher d) Block cipher

(vi) In a substitution cipher,
  a) Letters are rearranged b) Letters are replaced
  c) Blocks are permuted d) Bits are XORed

(vii) A block cipher encrypts data in units called
  a) Streams b) Blocks
  c) Packets d) Frames

(viii) Stream ciphers encrypt data
  a) Block by block b) Byte by byte
  c) Bit by bit d) File by file

(ix) Which cipher is faster for real-time applications?
  a) Block cipher b) Stream cipher

c) Hash function d) Asymmetric cipher

(x) ECB mode stands for

a) Electronic Cipher Block b) Encrypted Cipher Block
c) Electronic Code Book d) Encrypted Code Block

(xi) An organization uses ECB mode for encrypting confidential records and observes identical ciphertext blocks for repeated plaintext patterns. Which mode change would best mitigate this issue while maintaining block cipher usage?

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

(xii) A stream cipher reuses the same keystream for two different plaintexts. What is the most likely cryptographic weakness introduced?

a) Ciphertext expansion b) Known plaintext attack
c) Key collision d) XOR-based plaintext recovery

(xiii) A block cipher with 64-bit blocks is used to encrypt a very large dataset. Which cryptographic risk becomes significant due to the block size limitation?

a) Key exhaustion b) Birthday paradox collision
c) Differential attack d) Side-channel leakage

(xiv) When switching from DES to AES in a secure system, which design change primarily improves resistance against brute-force attacks?

a) Increased block size b) Increased key size
c) Improved S-box design d) Use of Feistel structure

(xv) Which operational scenario best justifies the use of a stream cipher over a block cipher?

a) Disk encryption b) Secure email
c) Real-time voice communication d) File archival

## Group-B

(Short Answer Type Questions) 3 x 10=30

2. What is cryptography? (3)
3. Define plaintext and ciphertext. (3)
4. Distinguish between block cipher and stream cipher. (3)
5. What is symmetric key cryptography? (3)
6. Why is AES preferred over DES? (3)
7. Analyze why classical cryptosystems fail to provide confidentiality in modern communication. (3)
8. Analyze how the Extended Euclidean Algorithm supports secure key generation. (3)
9. Evaluate the importance of Euler's Phi function in public key cryptography. (3)
10. Analyze the security principles behind the Diffie–Hellman key exchange. (3)
11. Analyze the security impact of choosing an improper mode of operation for block ciphers. (3)

**OR**

Compare block ciphers and stream ciphers in terms of resistance to cryptanalysis. (3)

## Group-C

(Long Answer Type Questions) 5 x 5=25

12. Explain the fundamental objectives of cryptography and their significance in secure communication. (5)
13. Describe classical cryptosystems with suitable examples. (5)
14. Analyze the security assumptions underlying public key cryptosystems. (5)
15. Analyze the Diffie–Hellman key exchange and identify potential vulnerabilities. (5)
16. Evaluate Diffie–Hellman key exchange for use in modern internet protocols. (5)

**OR**

Evaluate RSA in terms of security strength and computational efficiency. (5)