BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Sc.(MATH)-2025
Course Name – Cryptography
Course Code - MSM20504C
(Semester II)

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) Identify the correct option: Big-Oh notation is used to
   a) Estimate algorithm growth b) Measure exact running time
   c) Count operations exactly d) Reduce complexity

(ii) Identify the correct option: The Euclidean algorithm computes
   a) LCM b) GCD
   c) Prime factor d) Inverse

(iii) Select the correct option: In a shift cipher, the number of possible keys is
   a) 24 b) 25
   c) 26 d) 52

(iv) Select the correct option: The size of the key space of a substitution cipher is
   a) 26 b) 26^2
   c) 26! d) 2^26

(v) Identify the correct option: A permutation cipher alone is weak because
   a) it uses small keys b) it keeps letter frequencies unchanged
   c) it uses modulo arithmetic d) it has no decryption

(vi) Choose the right option: A cryptosystem is defined as a
   a) 3-tuple b) 4-tuple
   c) 5-tuple d) 6-tuple

(vii) Choose the right option: Perfect secrecy requires
   a) Large ciphertext space b) Large plaintext space
   c) Statistical independence of plaintext and ciphertext d) Computational hardness

(viii) Choose the correct option: Information-theoretic security assumes attacker has
   a) Polynomial-time power b) Unlimited computational power
   c) Limited power d) No power

(ix) Choose the correct option: A cryptosystem is computationally secure if breaking it is

a) Impossible
b) Undetectable
c) Easy
d) Computationally infeasible

(x) Select the correct option: A differential characteristic is defined as

a) A linear equation
b) A random mapping
c) A sequence of input–output differences across rounds
d) A brute-force strategy

(xi) Select the right option. The Difference Distribution Table (DDT) of an S-box is used to

a) Measure linear bias
b) Generate keys
c) Compute entropy
d) Determine probabilities of output differences for given input differences

(xii) Choose the condition for the Euler's totient function if n=pq

a) $\phi(n)=p+q$
b) $\phi(n)=pq$
c) $\phi(n)=(p-1)(q-1)$
d) $\phi(n)=p^2-q^2$

(xiii) Choose from the following: RSA decryption works correctly because of

a) Fermat's Little Theorem only
b) Chinese Remainder Theorem
c) Euler's Theorem
d) Lagrange's Theorem

(xiv) Choose from the following: The security of RSA cryptosystem is based on the difficulty of

a) Discrete logarithm problem
b) Integer factorization problem
c) Hash inversion problem
d) Elliptic curve problem

(xv) Select the right option: Finite fields are also known as

a) Prime fields
b) Integer fields
c) Galois fields
d) Ring fields

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Identify the value of gcd(252,198) by applying Euclidean Algorithm. (3)
3. Explain the shift cipher using modular arithmetic and state its key space. (3)
4. Estimate the Index of Coincidence and state its cryptanalytic significance. (3)
5. Explain S-box and write its uses in Substitution-Permutation Network (SPN) (3)
6. Justify square-and-multiply algorithm. (3)

OR

Evaluate ELGamal signature scheme. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Illustrate the algorithm of Linear attack on SPN (5)
8. Evaluate digital signature in modern cryptography. (5)
9. Using the RSA algorithm, evaluate the encryption of message M=89 with public key (n,e)= (187,7) (5)
10. Show that Euler phi function is multiplicative. (5)
11. Illustrate the Hill cipher using matrix multiplication modulo 26 and describe its encryption and decryption processes. (5)
12. Justify Diffie-Hellman Key Agreement. (5)

OR

Justify elliptic curve digital signature algorithm. (5)

****