BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Sc.(ANCS)-2025
Course Name – MOOC-Cryptography and Network Security
Course Code - MNC20409C
(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) Identify a key requirement for message authentication in secure communication.
a) Confidentiality b) Data Integrity
c) Compression d) Key Exchange

(ii) Select an algorithm that is classified as a cryptographic hash function.
a) AES b) SHA-256
c) Diffie-Hellman d) RSA

(iii) Select the primary purpose of Kerberos authentication.
a) Encrypting email messages b) Managing passwords
c) Providing mutual authentication between users and services d) Generating random session keys

(iv) Select the component that is NOT a part of the CIA Model in security.
a) Confidentiality b) Integrity
c) Availability d) Encryption

(v) Predict which mathematical concept is crucial for modular arithmetic in cryptography.
a) Linear equations b) Exponential functions
c) Prime numbers d) Logarithmic functions

(vi) Select the theorem that states if p is a prime number, then a^(p-1) ≡ 1 mod p.
a) Euler's Theorem b) Fermat's Theorem
c) Chinese Remainder Theorem d) RSA Theorem

(vii) Select the primary mathematical problem that ensures the security of RSA encryption.
a) Discrete logarithm problem b) Prime factorization problem
c) Hash collision problem d) Modular addition problem

(viii) Select the primary security concern with Elliptic Curve Cryptography (ECC).
a) ECC has weak encryption strength b) ECC is vulnerable to brute-force attacks
c) ECC security depends on the difficulty of solving the Elliptic Curve Discrete Logarithm d) ECC keys are too large for practical use

Problem (ECDLP)

(ix) Choose the correct reason why Diffie-Hellman Key Exchange is vulnerable to Man-in-the-Middle (MITM) attacks.

a) The shared secret key is not directly transmitted
b) It lacks authentication during the exchange process
c) It requires a trusted third party
d) The key exchange process is based on symmetric encryption

(x) Distinguish between Elliptic Curve Digital Signature Algorithm (ECDSA) and RSA signatures.

a) ECDSA requires larger key sizes than RSA for the same security
b) RSA signatures are always more secure than ECDSA
c) ECDSA provides the same security as RSA with smaller keys
d) ECDSA does not use elliptic curves

(xi) What does fabrication mean in cybersecurity?

a) Unauthorized access
b) Creating false or forged data
c) Modifying existing data
d) Destroying critical files

(xii) Which attack involves passive listening or monitoring of network communication?

a) Making unauthorized changes to a database
b) Intercepting communication without altering it
c) Performing a DDoS attack
d) Installing ransomware

(xiii) Select an example of authentication.

a) Fingerprint recognition
b) Encrypting data
c) Spoofing a website
d) Injecting malicious code

(xiv) Match the organization responsible for defining cryptographic standards.

a) ISO
b) NIST
c) IEEE
d) All of these

(xv) Select the cryptographic algorithm that uses elliptic curves.

a) RSA
b) AES
c) ECC
d) SHA-256

Group-B

(Short Answer Type Questions) 3 x 10=30

2. Describe the main types of security threats in a computer network. (3)
3. Evaluate the GCD of 252 and 105 using the Euclidean algorithm. (3)
4. Illustrate the working of the Extended Euclidean Algorithm with an example. (3)
5. Write a short note on modular arithmetic with a real-life example. (3)
6. Explain Fermat's Little Theorem with an example. (3)
7. Describe the working of the Diffie-Hellman key exchange with an example. (3)
8. Explain how ECC is used in digital signatures. (3)
9. Differentiate between ElGamal and RSA encryption algorithms. (3)
10. Write a short note on Secure Hash Algorithm (SHA). (3)
11. Explain the working of Simplified DES (S-DES). (3)

OR

Explain double and triple DES. (3)

Group-C

(Long Answer Type Questions) 5 x 5=25

12. Analyze the four dimensions of cryptography and how they contribute to secure communication. (5)
13. Justify the continued study of the Feistel cipher structure in cryptography education. (5)

14. Describe the architecture of network security controls and how they ensure layered protection. (5)
15. Write about the principles of email security and the roles of PGP and S/MIME. (5)
16. Explain the significance of Euclidean and Extended Euclidean algorithms in cryptography. (5)

OR

Analyze how Fermat's Little Theorem supports public-key cryptographic systems. (5)

****