45490

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Sc.(ANCS)-2025
Course Name – Network Security and Cryptography
Course Code - MNC20409A
(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) What does Extended Euclidean Algorithm compute?

a) Only GCD b) Modular inverse
c) Hash value d) Prime factorization

(ii) Match the following security services with their primary purpose: A. Confidentiality, B. Integrity, C. Availability, D. Authentication with 1. Ensures data is not altered, 2. Ensures data is accessible when needed, 3. Verifies user identity, 4. Prevents unauthorized disclosure

a) A-4,B-1,C-2,D-3 b) A-1,B-4,C-2,D-3
c) A-4,B-2,C-1,D-3 d) A-3,B-1,C-4,D-2

(iii) Match the following attacks with their type: A. Eavesdropping, B. Masquerade, C. Replay attack, D. Traffic analysis with 1. Active attack, 2. Passive attack

a) A-1,B-2,C-2,D-1 b) A-2,B-1,C-1,D-2
c) A-2,B-2,C-1,D-1 d) A-1,B-1,C-2,D-2

(iv) Match the following cryptographic concepts with their descriptions: A. Modular arithmetic, B. Euclidean Algorithm, C. Fermat's Theorem, D. Prime number with 1. Finds GCD, 2. Arithmetic using modulus, 3. Divisible only by 1 and itself, 4. $a^{(p-1)} \equiv 1 \pmod{p}$

a) A-2,B-1,C-4,D-3 b) A-1,B-2,C-3,D-4
c) A-3,B-1,C-2,D-4 d) A-2,B-4,C-1,D-3

(v) Match the following mode with its property: A. ECB, B. CBC, C. CFB, D. CTR with 1. Independent blocks, 2. Chaining blocks, 3. Stream-like mode, 4. Counter-based encryption

a) A-1,B-2,C-3,D-4 b) A-2,B-1,C-3,D-4
c) A-1,B-4,C-2,D-3 d) A-3,B-2,C-1,D-4

(vi) Which algorithm is used for key exchange?

a) AES b) RSA

c) Diffie-Hellman
d) DES

(vii) Select an asymmetric algorithm.

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

(viii) Choose the correct use of the Euclidean Algorithm in cryptography.

a) Finding the least common multiple (LCM)
b) Computing modular exponentiation
c) Determining the greatest common divisor (GCD)
d) Generating random numbers

(ix) 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

(x) Select the correct description of Triple DES.

a) Uses one encryption key applied three times
b) Uses three different keys applied once each
c) Uses two keys in a sequence of encrypt, decrypt, and encrypt
d) Encrypts the message four times

(xi) Distinguish the difference between block and stream ciphers.

a) Stream ciphers encrypt data in large chunks
b) Block ciphers process data one bit at a time
c) Stream ciphers process data continuously, block ciphers work in fixed-size chunks
d) Both operate the same way

(xii) Classify the key exchange methods used in asymmetric cryptography.

a) Diffie-Hellman, RSA, and ElGamal
b) AES and DES
c) SHA and MD5
d) One-time pad and Playfair Cipher

(xiii) Predict the impact of Quantum Computing on RSA Cryptography.

a) RSA encryption will become stronger
b) RSA decryption will be significantly faster
c) RSA security will be weakened due to efficient prime factorization
d) RSA will replace symmetric encryption

(xiv) Distinguish how ElGamal encryption differs from RSA.

a) ElGamal uses modular exponentiation, while RSA uses factorization
b) RSA is symmetric, while ElGamal is asymmetric
c) ElGamal does not support digital signatures
d) RSA requires fewer computational steps

(xv) 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 Problem (ECDLP)
d) ECC keys are too large for practical use

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define the dimensions of cryptography. (3)
3. Distinguish between RSA and Diffie–Hellman. (3)
4. Describe the principle of the ElGamal algorithm. (3)
5. Evaluate the role of digital signatures in achieving non-repudiation. (3)
6. Evaluate the GCD of 56 and 98 using the Euclidean Algorithm. (3)

OR

Evaluate the Extended Euclidean Algorithm to find the gcd(240,46) and find s and t. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Justify the role of prime numbers in modern encryption algorithms. (5)
8. Evaluate the advantages and disadvantages of Diffie-Hellman vs. RSA for key exchange. (5)

9. Write about the application of Elliptic Curve Digital Signature Algorithm (ECDSA) in securing blockchain. (5)
10. Explain the concept of intrusion detection systems (IDS) and their role in network security. (5)
11. Explain the concept of honeypots and how they help in detecting and studying cyber attacks. (5)
12. Differentiate between simplified DES (S-DES) and full DES in terms of design and application. (5)

OR

Explain how double and triple DES improve upon the original DES algorithm. (5)

****