BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – M.Sc.(ANCS)-2024
Course Name – Network Security and Cryptography
Course Code - MNC20301A
(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) Select an example of authentication.
a) Fingerprint recognition
b) Encrypting data
c) Spoofing a website
d) Injecting malicious code

(ii) What type of attack is a Man-in-the-Middle (MITM) attack?
a) Passive attack
b) Active attack
c) Interruption attack
d) Authentication attack

(iii) What does a Replay Attack involve?
a) Intercepting and modifying data in real-time
b) Repeating captured communication to gain access
c) Flooding a network with traffic
d) Encrypting messages

(iv) Which attack technique is used in SQL Injection?
a) Passive attack
b) Active attack
c) Interception attack
d) Interruption attack

(v) Select the component found in the Feistel Cipher Structure.
a) Permutation only
b) Substitution and Permutation
c) Hashing and Encoding
d) Digital Signatures

(vi) Select the encryption mode that converts a block cipher into a stream cipher.
a) ECB
b) CBC
c) CFB
d) OFB

(vii) Choose the encryption mode that prevents replay attacks.
a) ECB
b) CBC

c) OFB
d) CTR

(viii) Select the key length typically used in ECC for security equivalent to 2048-bit RSA.

a) 160-bit
b) 256-bit
c) 512-bit
d) 1024-bit

(ix) Identify the mathematical problem on which ElGamal encryption is based.

a) Factoring large primes
b) Discrete logarithm problem
c) Hash collisions
d) Symmetric encryption

(x) Choose the correct property of a secure hash function.

a) It should be reversible
b) It must generate fixed-length output
c) It should use symmetric encryption
d) It should generate the same hash for different inputs

(xi) Show the length of the hash value generated by SHA-256.

a) 128 bits
b) 160 bits
c) 256 bits
d) 512 bits

(xii) Select an advantage of using digital signatures in authentication.

a) Requires a secure channel for key distribution
b) Ensures message authenticity and prevents tampering
c) Encrypts messages for confidentiality
d) Provides only user identity verification

(xiii) Choose the correct security control that ensures only authorized users can access a system.

a) Encryption
b) Authentication
c) Traffic Filtering
d) Honeypots

(xiv) Select the primary goal of cryptography.

a) Ensuring data confidentiality and integrity
b) Increasing network bandwidth
c) Improving processor speed
d) Reducing latency

(xv) 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

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain the CIA model in information security. (3)
3. Describe the main types of security threats in a computer network. (3)
4. Illustrate the ElGamal key generation process. (3)
5. Explain how digital signatures ensure authenticity and integrity. (3)
6. Justify the need for Message Authentication Codes (MACs) in secure communication. (3)

OR

Evaluate the role of hash functions in data integrity and authentication. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Differentiate between the Substitution-Permutation and Feistel cipher structures. (5)
8. Analyze the core principles of public-key cryptography and how they differ from symmetric encryption. (5)
9. Define network threats and explain the different types with examples. (5)

10. Explain the concept of intrusion detection systems (IDS) and their role in network security. (5)
11. Evaluate the strengths and weaknesses of classical cryptographic techniques in modern contexts. (5)
12. Justify the growing popularity of Elliptic Curve Cryptography (ECC) in mobile and IoT devices. (5)

OR

Evaluate the advantages and disadvantages of Diffie-Hellman vs. RSA for key exchange. (5)

****