.

Printed Page:-4 **Subject Code:- AMICA0702**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
MCA (Integrated)
SEM: VII - THEORY EXAMINATION (2025 - 2026)
Subject: Cryptography and Network Security

Time: 3 Hours **Max. Marks: 100**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*

1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*

2. *Maximum marks for each question are indicated on right -hand side of each question.*

3. *Illustrate your answers with neat sketches wherever necessary.*

4. *Assume suitable data if necessary.*

5. *Preferably, write the answers in sequential order.*

6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 20

1. Attempt all parts:-

1-a. Integrity ensures that data is:(CO1,K2) 1

(a) Accurate and unaltered
(b) Always available
(c) Encrypted
(d) Accessible only to admin

1-b. Authentication is the process of:(CO1,K2) 1

(a) Verifying identity
(b) Encrypting data
(c) Hiding data
(d) Blocking access

1-c. Triple DES applies DES how many times?(CO2,K1) 1

(a) 1
(b) 2
(c) 3
(d) 4

1-d. LFSR is mainly used in:(CO2,K1) 1

(a) Hashing
(b) Stream ciphers
(c) Block ciphers
(d) Modular arithmetic

1-e. ElGamal cryptosystem is based on:(CO3,K1) 1

(a) Discrete log problem
(b) Factoring
(c) Hashing
(d) Symmetric key

1-f. Rabin cryptosystem produces:(CO3,K1) 1

(a) Four possible plaintexts
(b) One ciphertext
(c) Only hash
(d) Only signatures

1-g. MAC stands for:(CO4,K1) 1

(a) Message Authentication Code
(b) Modular Algorithm Code
(c) Multi Access Cipher
(d) Message Algorithm Check

1-h. Diffie-Hellman is a:(CO4,K1) 1

(a) Key exchange protocol
(b) Symmetric cipher
(c) Hash algorithm
(d) Compression method

1-i. Power analysis attack measures:(CO5,K1) 1

(a) Power consumption
(b) Encryption speed
(c) Hash output
(d) Key size

1-j. SSL is used to:(CO5,K1) 1

(a) Secure web communications
(b) Encrypt files only
(c) Hash emails
(d) Generate keys

2. Attempt all parts:-

2.a. Differentiate between active and passive attacks.(CO1,K4) 2

2.b. Define Diffie-Hellman key exchange.(CO2,K1) 2

2.c. One difference between deterministic and probabilistic primality tests.(CO3,K3) 2

2.d. Name the cipher against which differential cryptanalysis was effective.(CO4,K1) 2

2.e. Describe the TLS handshake process briefly.(CO5,K2) 2

SECTION-B 30

3. Attempt all parts:-

3.a. Answer any one of the following:-

3.a.(i) Differentiate between security services and security mechanisms with examples.(CO1,K2) 6

3.a.(ii)	Describe Playfair cipher with example.(CO1,K2)	6
3.b. Answer any one of the following:-		
3.b.(i)	Using a real-world example, compare how ECB and CBC modes behave when encrypting data that contains repeating patterns.(CO2,K3)	6
3.b.(ii)	Explain the working of LFSR with an example.(CO2,K3)	6
3.c. Answer any one of the following:-		
3.c.(i)	Explain Miller-Rabin primality test with an example.(CO3,K2)	6
3.c.(ii)	Describe encryption/decryption in ElGamal cryptosystem.(CO3,K2)	6
3.d. Answer any one of the following:-		
3.d.(i)	Explain message authentication techniques with examples.(CO4,K2)	6
3.d.(ii)	Analyze how MACs and digital signatures differ in terms of key usage, security guarantees, and verification processes. Which method provides non-repudiation, and why?(CO4,K4)	6
3.e. Answer any one of the following:-		
3.e.(i)	Explain the TLS handshake process and apply it to show how a client and server establish a secure session, including certificate exchange, key generation, and session key creation.(CO5,K3)	6
3.e.(ii)	Explain PGP and email security.(CO5,K2)	6

SECTION-C 50

4. Answer any one of the following:-		
4-a.	Discuss in detail different types of security attacks with examples.(CO1,K3)	10
4-b.	Explain Caesar, Monoalphabetic, and Playfair ciphers in detail.(CO1,K2)	10
5. Answer any one of the following:-		
5-a.	Discuss the design and working of Triple DES.(CO2,K2)	10
5-b.	Explain the role and importance of an Initialization Vector (IV) in block cipher modes. Why is it necessary, and how does it improve security?(CO2,K2)	10
6. Answer any one of the following:-		
6-a.	Explain the Fermat primality test. Describe how it works, its basic principle, and its limitations in checking whether a number is prime.(CO3,K2)	10
6-b.	Explain the differences and similarities between the ElGamal cryptosystem and RSA. Describe their key features, encryption/decryption methods, and security aspects.(CO3,K2)	10
7. Answer any one of the following:-		
7-a.	Apply the concept of the key management life cycle to explain how cryptographic keys are generated, distributed, stored, used, and retired in a real-world system. Illustrate each stage with an example.(CO4,K3)	10
7-b.	Explain why a hybrid key exchange uses both symmetric and asymmetric encryption instead of just one method.(CO4,K2)	10
8. Answer any one of the following:-		
8-a.	Discuss timing attacks in cryptographic systems and methods to prevent them.(CO5,K2)	10

.

8-b.	A company wants to protect its cryptographic hardware from EM attacks. Evaluate the effectiveness of shielding versus algorithmic countermeasures in this scenario.(CO5,K3)	10