Printed Page:-04 **Subject Code:- ACSAI0403**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute Affiliated to AKTU, Lucknow)

B.Tech

SEM: IV - THEORY EXAMINATION (2024- 2025)

Subject: Introduction to Information Security and Cryptography

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. _____ is a weakness that can be exploited by attackers.(CO1, K1) 1

(a) System with vulnerabilities
(b) System with a strong password
(c) System without firewall
(d) System with Virus

1-b. From the options below, which of them is not a threat to information security?(CO1, K1) 1

(a) Disaster
(b) Eavesdropping
(c) Information leakage
(d) Unchanged default password

1-c. Encryption prevents hackers from obtaining information (CO1. K1) 1

(a) TRUE
(b) FALSE
(c) Sometimes true sometimes false
(d) None of these

1-d. If an encrypted message is hacked, it can easily be read without the key (CO2, K1). 1

(a) TRUE

.

(b) FALSE
(c) Sometimes true sometimes false
(d) None of these

1-e. The private key in asymmetric key cryptography is kept by (CO3, K1) 1

(a) Sender
(b) Receiver
(c) Both
(d) None of the above

1-f. In asymmetric key cryptography, _____ keys are required per communicating party. (CO3,K1) 1

(a) 1
(b) 2
(c) 3
(d) 5

1-g. Find out which of the following is /are offered by the Hash functions?(CO4, K1) 1

(a) Authentication
(b) Non repudiation
(c) Data Integrity
(d) All of the above

1-h. A cryptographic hash function is an equation used to verify the ____ of data. (CO4, K1) 1

(a) Variety
(b) Validity
(c) Veracity
(d) None of the mentioned above

1-i. Choose among the following techniques, which are used to hide information inside a picture. (CO5, K1) 1

(a) Image Rendering
(b) Steganography
(c) rootkits
(d) bitmapping

1-j. Which of the following is used for monitoring traffic and analyzing network flow? (CO5, K1) 1

(a) Managed detection and response
(b) Cloud access security broker
(c) Network traffic analysis
(d) Netwoek security firewall

2. Attempt all parts:-

.

2.b.	Explain how a block cipher differs from a stream cipher in terms of data processing.(C02, K1)	2
2.a.	What is network sniffing? (CO1, K1)	2
2.d.	Describe the definition of Hash Function.(CO4, K2).	2
2.e.	What is the purpose of a digital signature in secure communication?(CO5, K1)	2
2.c.	State Euler's Theorem used in Cryptography. (CO3, K1)	2

SECTION-B 30

3. Answer any five of the following:-

3-a.	Differentiate between a **worm** and a **Trojan horse** in the context of computer security.(CO1, K1)	6
3-b.	Explain why information security is major concern in today's world?(CO1, K1)	6
3-c.	Explain how 16 subkeys are generated in DES. (CO2. K3)	6
3-d.	Explain Full-Size Key Transposition Block Ciphers and Full-Size Key Substitution Block Ciphers. Define the size of key used in both. Explain with an example. (CO2, K2)	6
3.e.	Explain the principles of Public Key Cryptosystems. (CO3, K2)	6
3.f.	Define cryptographic hash function with proper example.(CO4, K2)	6
3.g.	Define Security Association. Specify the parameters that identifies the Security Association. (CO5, K2)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	Differentiate between information protection and information assurance. (CO1, K1)	10
4-b.	List down some factors that cause vulnerabilities.(CO1, K1)	10

5. Answer any one of the following:-

5-a.	Explain DES algorithm and how it is used in cryptography. Explain with suitable example in detail.(CO2, K4)	10
5-b.	Explain Playfair cipher in detail and encrypt the following message " COME TO THE WINDOW ANNA" using the key "MONARCHY".(CO2, K4)	10

6. Answer any one of the following:-

6-a.	Describe the counter measures to be used against Timing attack? (CO3, K2)	10
6-b.	In an RSA system, the public key of a given user is e= 31, n = 3599. What is the private key of this user? (CO3, K3)	10

7. Answer any one of the following:-

7-a.	Differenciate between message authentication code and a one way hash function. (CO4, K2)	10
7-b.	Explain the RSA algorithm in detail. Include the steps involved in key generation, encryption, and decryption. Also, mention how RSA ensures security. (CO4, K2)	10

8. Answer any <u>one</u> of the following:-

8-a.	Discuss authentication , header and Encapsulating Security Payload in detail with their packet format. (CO5, K2)	10
8-b.	Explain the term Security with respect to cryptosystem and also explain E-mail Security in detail. (CO5, K2)	10

.