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 (222-2023 **)**

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. Security Goals of Cryptography are (CO1) 1

(a) Confidentiality

(b) Authenticity

(c) Data integrity

(d) all above

1-b. CIA triad is also known as _____. (CO1) 1

(a) NIC (Non-repudiation, Integrity, Confidentiality)

(b) AIC (Availability, Integrity, Confidentiality)

(c) AIN (Availability, Integrity, Non-repudiation)

(d) AIC (Authenticity, Integrity, Confidentiality)

1-c. In a(n) _____, the key is called Secret Key. (CO2) 1

(a) Symmetric Encryption

(b) Asymmetric Encrytion

(c) either (a) or (b)

(d) neither (a) nor (b)

1-d. The process of decryption of an AES ciphertext is similar to the encryption process in the _____.. (CO2) 1

(a) Reverse order

(b) Next Order

(c) Both a and b

(d) All of these

1-e. Symmetric-key cryptography is _____ than asymmetric key cryptography. (CO3) 1

(a) always slower

(b) of the same speed

(c) faster

(d) usually slower

1-f. ECDSA stands for _____.. (CO3) 1

(a) Elliptic Curve Digital Signature Algorithm

(b) Elliptic Curve Data Signature Algorithm

(c) Elliptic Curve Digital Single Algorithm

(d) Encryption Curve Digital Signature Algorithm

1-g. Which of the following options is not correct according to the definition of the Hash Function? (CO4) 1

(a) Hash Functions are mathematical functions

(b) They compress the input values

(c) The hash functions work on arbitrary length input but produces fixed length output.

(d) None of the above

1-h. Following are the example of massege authentication code. (CO4) 1

(a) MHAC

(b) CMAC

(c) SHA

(d) Both A and B

1-i. State whether True or False: Data encryption is primarily used to ensure confidentiality. (CO5) 1

(a) TRUE

(b) FALSE

(c) cannot be interpreted

(d) None

1-j. Which of the following platforms is used for the safety and protection of information in the cloud? (CO5) 1

(a) AWS

(b) cloud workload protection platform

(c) cloud security protocols

(d) one drive

2. Attempt all parts:-

2.a. Explain the difference between interception and interruption. (CO1) 2

2.b. What are two problems associated with mono-alphabetic substitution cipher? (CO2) 2

2.c. Find x such that $3x \equiv 6 \pmod{12}$. (CO3) 2

2.d. Describe the digital signature. (CO4) 2

2.e. For what purpose kerberos is used? (CO5) 2

SECTION B **30**

3. Answer any <u>five</u> of the following:-

3-a. Differentiate between malware and viruses. (CO1) 6

3-b. Explain vulnerability and its types. (CO1) 6

3-c. Explain Triple DES in detail. (CO2) 6

3-d. How confusion and diffusion can be achieved as per Shannon's Theory of Confusion and Diffusion? (CO2) 6

3.e. Explain the principles of Public Key Cryptosystems. (CO3) 6

3.f. What are the message authentication requirements? (CO4) 6

3.g. Explain PGP and MIME in detail. (CO5) 6

SECTION C **50**

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

4-a. Modification causes loss of message integrity. Justify the statement. (CO1) 10

4-b. Explain Network Security Services in detail. (CO1) 10

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

5-a. Encrypt " Hello there mate" using playfair cipher with "window" as key. (CO2) 10

5-b. Fabrication attacks involve generating data, processes, communications, or other similar activities with a system. Comment on the statement. (CO2) 10

.

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

6-a. Explain the approaches of attacking RSA mathematically. (CO3) 10

6-b. In what order should the signature function and the confidentiality function applied to a message, and why? (CO3) 10

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

7-a. Describe the main Problems assiciate With Hashing Functions. (CO4) 10

7-b. How does a birthday attack on a hashing algorithm work? (CO4) 10

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

8-a. Find the solution of the simultaneous equations using Chinese Reminder Theorem. (CO5) 10

$x = 2 \bmod 5$

$x = 5 \bmod 6$

$x = 3 \bmod 7$

8-b. Explain the protocols which helps in achieving security at IP Layer. (CO5) 10