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 (2023 - 2024)

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 the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction. (CO1) 1

(a) Network Security

(b) Database Security

(c) Information Security

(d) Physical Security

1-b. Compromising confidential information comes under _________ (CO1) 1

(a) Bug

(b) Threat

(c) Vulnerability

(d) Attack

1-c. ___________________uses the same key to encrypt and decrypt a message. (CO2). 1

(a) Plain Text

(b) Cipher Text

.

(c) Symmetric Encryption

(d) Asymmetric Encrytion

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

(a) TRUE

(b) FALSE

(c) Sometimes true sometimes false

(d) None of these

1-e. ____________________uses two different keys to encrypt and decrypt a message.(CO3) 1

(a) Plain Text

(b) Cipher Text

(c) Symmetric Encryption

(d) Asymmetric Encrytion

1-f. Which is the cryptographic protocol that is used to protect an HTTP connection?(CO3) 1

(a) Resource reservation protocol

(b) ECN

(c) TLS

(d) None of the above

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

(a) Authentication

(b) Non repudiation

(c) Data Integrity

(d) All of the above

1-h. Hash functions are mathematical functions that transform or "map" a given set of data into a bit string of fixed size, also known as the ______(CO4) 1

(a) Hash value

(b) Map value

(c) Both A and B

(d) None of the mentioned above

1-i. Identify the oldest phone hacking technique used by hackers to make free calls.(CO5) 1

(a) Spamming

(b) Phreacking

(c) Hacking

(d) Phishing

1-j. Which software is mainly used to help users detect viruses and avoid them?(CO5) 1

(a) Antivirus

(b) Adware

(c) Malware

(d) None

2. Attempt all parts:-

2.a. Explain information security.(CO1) 2

2.b. Differentiate between P Box and S Box. (CO2) 2

2.c. Define What do you mean by Totient Function. (CO3) 2

2.d. List the attributes of hash algorithm? Explain its types with example.(CO4) 2

2.e. Mention four SSL protocols .(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. What is the difference between threat, vulnerability and risk? (CO1) 6

3-c. Explain how 16 subkeys are generated in DES. (CO2) 6

3-d. Explain One Time Pad Cipher and Hill Cipher in detail with an example of each. (CO2) 6

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

3.f. Define cryptographic hash function with proper example.(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. Explain the term two-factor authentication.(CO1) 10

4-b. List down some factors that cause vulnerabilities.(CO1) 10

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

5-a. Explain DES algorithm and how it is used in cryptography. Explain with suitable example in detail.(CO2) 10

5-b. Encrypt the message "the house is being sold tonight" using Playfair cipher with key = " HEALTH" (Ignore the spaces between words) (CO2) 10

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

6-a. A plaintext m is encrypted twice with the RSA system using two public RSA keys (n, e) and (n, f) and produce ciphertext Ce and Cf respectively, i.e.,Ce = me mod n and Cf = mf mod n.Given that gcd(e, f) = 1. Whether an attacker can recover plaintext m? If yes then how?(CO3) 10

6-b. Describe the counter measures to be used against Timing attack? (CO3) 10

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

7-a. Differenciate between message authentication code and a one way hash function. (CO4) 10

7-b. Explain the Hash algorithms. Explain the properties strong hash function.(CO4) 10

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

8-a. Explain in detail about architecture of IP Security. (CO5) 10

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

x= 2 mod 5
x= 5 mod 6
x= 3 mod 7