Printed Page:- 03 **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. From the options below, which of them is not a vulnerability to information security? (CO1) 1

(a) flood

(b) without deleting data, disposal of storage media

(c) unchanged default password

(d) latest patches and updates not done

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

(a) Bug

(b) Threat

(c) Vulnerability

(d) Attack

1-c. A message before encryption is known as (CO2). 1

(a) Original message

(b) Plain Text

(c) Cipher Text

(d) Encrypted Text

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. The private key in asymmetric key cryptography is kept by (CO 3) 1

(a) Sender

(b) Receiver

(c) Both

(d) None of the above

1-f. Which one of the following algorithms is not used in asymmetric-key cryptography? (CO3) 1

(a) DSA algorithm

(b) ECB

(c) Diffie-Hellman algorithm

(d) RSA

1-g. Which of the following security services cannot be achieved using the Hash functions? (CO4) 1

(a) Password Check

(b) Data Integrity check

(c) Digital Signature

(d) Data retrieval in its original form

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

(a) Image Rendering

(b) Steganography

(c) rootkits

(d) bitmapping

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 CIA triad. (CO1) 2

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

2.c. What is the role of Public Key?(C03) 2

2.d. Describe the definition of Hash Function.(CO4). 2

2.e. Explain the hashing function in details.(CO5) 2

SECTION-B 30

3. Answer any five of the following:-

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

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

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

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

3.f. Describe in detail, What is digital signature and hash functions.(CO4) 6

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

SECTION-C 50

4. Answer any one of the following:-

4-a. Explain the Intrusion Detection and its categories (CO1) 10

4-b. Differentiate between information protection and information assurance. (CO1) 10

5. Answer any one of the following:-

5-a. Explain AES in detail. (CO2) 10

5-b. Encrypt the message "the house is being sold tonight" using Autokey cipher with key = 7 (Ignore the spaces between words). (CO2) 10

6. Answer any one 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. 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) 10

7. Answer any one of the following:-

7-a. Where is the Diffie-Hellman key exchange used?Explain its significance.(CO4) 10

7-b. Explain how the RSA key exchange work with an example. (CO4) 10

8. Answer any one of the following:-

8-a. Explain the steps, methodology involved in SSL/TLS protocol?(CO5) 10

8-b. Explain the term Security with respect to cryptosystem and also explain E-mail Security in detail. (CO5) 10