Printed Page:- 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 (2021 - 2022)

Subject: Introduction to Information Security and Cryptography

Time: 3 Hours Max. Marks: 100

General Instructions:

1. The question paper comprises three sections, A, B, and C. You are expected to answer them as directed.
2. Section A - Question No- 1 is 1 marker & Question No- 2 carries 2 mark each.
3. Section B - Question No-3 is based on external choice carrying 6 marks each.
4. Section C - Questions No. 4-8 are within unit choice questions carrying 10 marks each.
5. 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. A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?(CO1) 1

(a) An integer values
(b) A square matrix
(c) An array of characters
(d) All of the above

1-c. a message before decryption is known as (CO2) 1

(a) Original message
(b) Plain Text
(c) Cipher Text
(d) Encrypted Text

1-d. Which one is DES?(CO2) 1

(a) Stream Cipher
(b) Block Cipher
(c) Bit Cipher
(d) None of these

1-e. RSA _____ be used for digital signatures.(CO3) 1

(a) must not
(b) can
(c) cannot
(d) should not

1-f. A cryptographic function hash function has variable output length.(CO3) 1

(a) TRUE
(b) FALSE

(c) Sometimes True sometimes False

(d) can't be determined

1-g. When a hash function is used to provide message authentication, the hash function value is referred to as (CO4) 1

(a) Message Field

(b) Message Digest

(c) Message Score

(d) Message Leap

1-h. A digital signature is a mathematical technique which validates?(CO4) 1

(a) Authenticity

(b) integrity

(c) Non-repudiation

(d) All of the above

1 EDR stands for _____?(CO5) 1

(a) Endless Detection and response

(b) Endpoint detection and response

(c) Endless detection and recovery

(d) Endpoint detection and recovery

1 Which protocol is mostly used in Wi-fi security?(CO5) 1

(a) WPS

(b) WPA

(c) WPA2

(d) both a and b

2. Attempt all parts:-

2.a. What is Trojan virus?(C01) 2

2.b. Define threat and attack.(C02) 2

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

2.d. Define the main characteristics of SHA algorithm.(CO4) 2

2.e. Decsribe PGP?(C05) 2

SECTION B 30

3. Answer any five of the following:-

3-a. Explain various Security Counter measures in detail.(CO1) 6

3-b. "Threat + Vulnerability = Risk". Comment on the Statement.(CO1) 6

3-c. Use an affine cipher to find cipher text for the following message “hello Champ” with the key pair (7, 2). Explain the decryption process as well.(CO2) 6

3-d. Explain encryption and decryption. Draw a block diagram showing plain text, cipher text, encryption and decryption.(CO2) 6

3.e. In RSA, given N = 187 and the encryption key (E) as 17, find out the corresponding private key (D).(CO3) 6

3.f. List out the difference between a hash and a digital signature.(CO4) 6

3.g. Explain the steps involved in SSL required protocol?(CO5) 6

SECTION C 50

4. Answer any one of the following:-

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

4-b. What are three classes of intruders explain each?(CO1) 10

5. Answer any one of the following:-

5-a.	Explain Playfair cipher in detail and encrypt the following message " COME TO THE WINDOW ANNA" using the key "MONARCHY".(CO2)	10
5-b.	Explain 256-bit vs 192-bit vs 128-bit AES Encryption. Which among these is considered as the most powerfurl Encryption Scheme and hard to crack?(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.	What are the broad categories of applications of public key cryptosystems?(CO3)	10

7. Answer any one of the following:-

7-a.	Explain the Hash algorithms. Explain the properties strong hash function.(CO4)	10
7-b.	Describe the SHA-256 algorithm with example. Write down the characteristics of SHA-256.(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 User Authentication Mechanisms in detail.(CO5)	10