O.P.Code: 23CS1207	R23	H.T.No.									

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR

(AUTONOMOUS)

B.Tech. III Year II Semester Regular Examinations April-2026

CRYPTOGRAPHY & DATA SECURITY

(CSE With Specialisation in Cloud Computing)

Time: 3 Hours **Max. Marks: 70**

PART-A

(Answer all the Questions **10 x 2 = 20** Marks)

1	a	What is meant by Disruption.	CO1	L1	2M
	b	Define cryptography.	CO1	L1	2M
	c	What does DES stand for and what is its block size.	CO2	L1	2M
	d	What is Triple DES.	CO2	L2	2M
	e	Define Blowfish cipher.	CO3	L2	2M
	f	What does IDEA stand for? Mention its key and block size.	CO3	L1	2M
	g	Define data security. What are its primary objectives.	CO4	L1	2M
	h	What is security attack.	CO4	L1	2M
	i	List the two modes of operation in IPSec	CO5	L1	2M
	j	What is the output size of SHA-1 algorithm	CO5	L1	2M

PART-B

(Answer all Five Units **5 x 10 = 50** Marks)

UNIT-I

2		A Employee shares his password with a friend. Which security principle is compromised.	CO1	L3	10M

OR

3	a	Classify possible types of attacks in cryptography.	CO1	L2	5M
	b	Illustrate different types of transposition techniques in detail.	CO1	L4	5M

UNIT-II

4	a	Illustrate Conventional encryption model.	CO2	L3	5M
	b	State the formula for the Affine cipher encryption and decryption.	CO2	L2	5M

OR

5	a	Compare conventional key with public key encryption.	CO2	L5	5M
	b	Analyze the security weaknesses of the Caesar cipher and propose improvements.	CO6	L4	5M

UNIT-III

6	a	Infer the concept of Elgamal Cryptography algorithm.	CO3	L2	5M
	b	Compare ElGamal encryption with RSA in terms of cipher text expansion	CO3	L3	5M

OR

7		Demonstrate the Structure of AES and its transformations.	CO3	L2	10M

UNIT-IV

8		Examine the types, process & tools of Vulnerability assessment.	CO4	L4	10M

OR

9	a	Infer in detail about Time-of-check to Time-of-use (TOCTTOU) Errors.	CO4	L2	5M
	b	Explain the concept of a salami attack with example.	CO4	L3	5M

UNIT-V

10	a	Justify briefly about combining Security Associations.	CO5	L5	6M
	b	Distinguish between Digital Signature and Digital Certificate.	CO4	L4	4M

OR

11	a	Explain the difference between Authentication Header (AH) and Encapsulating Security Payload (ESP).	CO6	L2	5M
	b	Describe how transport mode differs from tunnel mode in IPSec.	CO6	L2	5M

***** END *****