22/4/26 FN

O.P.Code: 23CS0525	R23	H.T.No.									

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
B.Tech. III Year II Semester Regular Examinations April-2026
CRYPTOGRAPHY & NETWORK SECURITY
(Common to CSE & CSIT)

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

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

1	a	Define transposition cipher.	CO1	L1	2M
	b	What is SubBytes transformation?	CO1	L1	2M
	c	Define discrete logarithm.	CO2	L1	2M
	d	Compute a simple modular exponentiation.	CO2	L3	2M
	e	Define collision resistance.	CO3	L1	2M
	f	Explain the role of hash functions in digital signatures.	CO3	L2	2M
	g	Differentiate between PGP and S/MIME.	CO4	L2	2M
	h	List services provided by PGP.	CO4	L1	2M
	i	Differentiate between SSH and Telnet.	CO5	L2	2M
	j	List different types of firewalls.	CO5	L1	2M

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

UNIT-I

2	a	Explain in detail about passive attacks with neat sketch.	CO1	L3	5M
	b	Explain in detail about active attacks with neat sketch .	CO1	L3	5M
		OR			
3		Describe the internal structure of the Advanced Encryption Standard (AES) algorithm by explaining the key transformations	CO1	L2	10M

UNIT-II

4	a	Describe Modular Arithmetic and its fundamental rules with examples.	CO2	L2	5M
	b	Explain the application of modular arithmetic in cryptography.	CO2	L2	5M
		OR			
5	a	Describe finite fields of the form GF(2^n).	CO2	L2	5M
	b	Demonstrate multiplication in GF(2^n) using polynomial representation.	CO2	L3	5M

UNIT-III

6	a	Explain the working of the Secure Hash Algorithm with a neat diagram.	CO3	L3	5M
	b	Describe the applications of the Secure Hash Algorithm in information security.	CO3	L2	5M
		OR			
7		Differentiate between HMAC and CMAC with suitable examples.	CO4	L4	10M

UNIT-IV

8		List and explain the typical attacks remote authentication protocols must resist.	CO5	L2	10M
		OR			
9	a	Describe ESP packet format in detail and explain its security coverage.	CO5	L2	5M
	b	Evaluate the security impact of combining AH and ESP in different modes.	CO5	L3	5M

UNIT-V

10		Explain Transport Layer Security (TLS), its protocol components, and security services.	CO6	L2	10M
		OR			
11		What are the key parameters to consider when configuring a firewall?	CO6	L2	10M

***** END *****