

X-CE0634-001

Semester:	VI	Branch:	CE/CSE/IT
END SEMESTER EXAMINATION – May 2023			
Subject Code:	CE0634	Subject Name:	Cryptography & Network Security
Date:	19/08/2023	Time:	2:00 PM To 5:00 PM
Day:	FRIDAY	Total Marks:	100

Instructions:

1. Attempt all questions
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.

Q.1	A	Define Single Round of DES with Diagram.	10
	B	Encrypt using HILL CIPHER the plaintext="SAFEMESSAGES" using the key 2 8 15 7 4 17 8 13 6	10
Q.2	A	List out general categories of schemes for the distribution of public keys.	10
	B	Explain knapsack Algorithm with example.	10
Q.3	A	What is Digital Signature? Give it properties and requirements with details.	10
	B	Explain HMAC in detail.	10
Q.4	A	Explain IPsec Architecture.	10
	B	Explain Secure Socket Layer with its Objectives and Benefits.	10
Q.5		Any Four (05*4=20)	20
	A	What is Kerberos.explain it with all proper steps.	05

	B	Differentiate MAC and Hash function.	05
	C	Explain Elgamal digital signature Algorithm.	05
	D	List out and explain Viruses and related threats.	05
	E	Explain Types of Intrusion Detection.	05
	F	List out and explain Firewall Design Principles.	05