TE SEM-VI CMPN C-scheme May 2026

Date : 13/05/2026

Duration: 3hrs **[Max Marks:80]**

N.B. : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

1		Attempt any FOUR	[20]
	a	Explain challenge response-based authentication tokens.	[5]
	b	Find Multiplicative Inverse of 1234 and 4321.	[5]
	c	Explain TCP/IP vulnerabilities layer wise.	[5]
	d	Compare AES and DES. Which one is bit oriented? Which one is byte oriented?	[5]
	e	Discuss any two block cipher modes of operation.	[5]
2	a	Perform encryption and decryption using the RSA algorithm for the following: p=3; q=11; e=7; M=5	[10]
	b	What is DOS attack? Explain different types of denial-of-service attacks.	[10]
3	a	What are the requirements of cryptographic hash functions? Compare MD5 and SHA hash functions. State real world applications of hash functions.	[10]
	b	How is security achieved in Transport and Tunnel modes of IPSEC? Explain the role of AH and ESP.	[10]
4	a	Why are digital certificates and signatures required? What is the role of digital signature in digital certificates? Explain various attacks on digital signatures.	[10]
	b	How does PGP achieve confidentiality and authentication in emails?	[10]
5	a	Explain RC4 encryption algorithm.	[10]
	b	Explain Kerberos. Why is it called as SSO?	[10]
6	a	Enlist the various functions of the different protocols of SSL. Explain the phases of handshake protocol.	[10]
	b	What are different types of firewalls? How firewall is different from IDS.	[10]

****