Course Code: 23CS6T03

BONAM VENKATA CHALAMAYYA INSTITUTE OF TECHNOLOGY & SCIENCE

(AUTONOMOUS)

III - B.Tech II-Semester Regular Examinations (BR23), MAY - 2026

CRYPTOGRAPHY AND NETWORK SECURITY (CSE)

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

Question Paper consists of Part-A and Part-B
*Answer **ALL** the question in **Part-A and Part-B***

PART–A (10X2 = 20M)

		Marks	CO	BL
1. a)	Define cryptography.	(2M)	CO1	BTL1
b)	Recall security mechanism.	(2M)	CO1	BTL1
c)	What is a stream cipher?	(2M)	CO2	BTL2
d)	State key expansion in AES.	(2M)	CO2	BTL1
e)	List the advantages of asymmetric key cryptography.	(2M)	CO3	BTL1
f)	Outline ECC.	(2M)	CO3	BTL1
g)	Tell about random oracle model.	(2M)	CO4	BTL2
h)	Give the use of SHA-512.	(2M)	CO4	BTL2
i)	Annotate S/MIME.	(2M)	CO5	BTL1
j)	Write about buffer overflow.	(2M)	CO5	BTL2

PART–B (5X10 = 50M)

2	Describe the different types of cryptographic attacks with suitable examples.	10(M)	CO1	BTL2
	(OR)			
3	Narrate about linear congruence and describe the method for solving linear congruence equations with a suitable example.	10(M)	CO1	BTL2
4	Explain the principles of modern stream ciphers and differentiate them from block ciphers with respect to operation and applications.	10(M)	CO2	BTL2
	(OR)			
5	Elaborate the overall structure of Advanced Encryption Standard (AES) with a neat diagram.	10(M)	CO2	BTL2
6	Solve the following system of congruences using the Chinese Remainder Theorem: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ and $x \equiv 2 \pmod 7$.	10(M)	CO3	BTL3
	(OR)			
7	In an ElGamal cryptosystem given p=23, g=5, private key x=6 and message M=10. (I) Generate the public key (II) Encrypt the message using a random integer k=3 (III) Decrypt the ciphertext	10(M)	CO3	BTL3

8	Examine the operation of cryptographic hash functions and illustrate with a suitable example.	10(M)	CO4	BTL4
	(OR)			
9	Analyze the challenges involved in symmetric key distribution and evaluate the methods used for secure key distribution.	10(M)	CO4	BTL4
10	Evaluate the two modes of IPSec and analyze their suitability for different network scenarios.	10(M)	CO5	BTL5
	(OR)			
11	Assess the performance of IDS and firewalls in network security and compare their ability to detect and prevent cyber attacks.	10(M)	CO5	BTL5

****