Course Code: 23CS6T05

BONAM VENKATA CHALAMAYYA INSTITUTE OF TECHNOLOGY & SCIENCE
(AUTONOMOUS)
III - B.Tech II-Semester Regular Examinations (BR23), APRIL - 2026
CRYPTOGRAPHY & 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 3 Security goals?	(2M)	CO1	BL1
b)	Define properties of Modular Ariththmetic?	(2M)	CO1	BL1
c)	Give example for Group?	(2M)	CO2	BL1
d)	Specify types of D boxes?	(2M)	CO2	BL1
e)	Give formula(s) to get Euler's totient function?	(2M)	CO3	BL1
f)	How Chinese Remainder Theorem used to solve set of congruent equations?	(2M)	CO3	BL2
g)	How Message integrity will be checked?	(2M)	CO4	BL2
h)	Write names of different Digital signature schemes?	(2M)	CO4	BL1
i)	Write about E-mail architecture?	(2M)	CO5	BL1
j)	Explain about viuses?	(2M)	CO5	BL2

PART–B (5X10 = 50M)

2	.Explain Cryptographic attacks in detail by giving Examples?	10(M)	CO1	BL2
	(OR)			
3	Define Security services and Security Mechanisms? Relate them?	10(M)	CO1	BL2
4	With neat diagram(s) elaborate Data Encryption Standard (DES)?	10(M)	CO2	BL2
	(OR)			
5	With neat diagram(s) elaborate Advanced Encryption Standard (AES)?	10(M)	CO2	BL2
6	Explain the Idea behind RSA cryptosystem? Give Example?	10(M)	CO3	BL3
	(OR)			
7	Explain the behind ElGamal Cryptosystem? Give Example?	10(M)	CO3	BL3
8	Analyse main features of SHA-512 cryptographic hash function? What kind of compression function is used in SHA-512?	10(M)	CO4	BL4
	(OR)			
9	Analyse Diffie-Hellman key Exchange process?	10(M)	CO4	BL4
10	Evaluate the effectiveness of the architecture SSL in providing secure communication over the Internet	10(M)	CO5	BL5
	(OR)			
11a.	Write a short note on S/MIME?	5(M)	CO5	BL5
11b.	Evaluate working Principles Firewalls?	5(M)		

****

Head of the Dept.,
Department of CSE
BVCITS, Amalapuram