Course Code: 1970526 Roll No: **MLRS-R19**

MARRI LAXMAN REDDY
INSTITUTE OF TECHNOLOGY AND MANAGEMENT
(AN AUTONOMOUS INSTITUTION)
(Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad)
Accredited by NBA and NAAC with 'A' Grade & Recognized Under Section2(f) & 12(B)of the UGC act,1956

IV B.Tech I Sem Regular End Examination, Nov/Dec 2022

Cryptography & Network Security

(CSE)

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

Note: 1. Question paper consists: Part-A and Part-B.
2. In Part – A, answer all questions which carries 20 marks.
3. In Part – B, answer any one question from each unit.
Each question carries 10 marks and may have a, b as sub questions.

PART- A

(10*2 Marks = 20 Marks)

1.	a)	Differentiate passive attack from active attack with example	2M	CO1	BL1
	b)	What are the two basic functions used in encryption algorithms?	2M	CO1	BL1
	c)	What primitive operation is used in RC4	2M	CO2	BL1
	d)	What is the purpose of the S-boxes in DES?	2M	CO2	BL1
	e)	What are the properties of digital signatures?	2M	CO3	BL1
	f)	How digital signature differs from authentication protocols?	2M	CO3	BL1
	g)	What is the role of secure socket layer?	2M	CO4	BL1
	h)	Define wireless security?	2M	CO4	BL1
	i)	State the reasons for using the PGP?	2M	CO5	BL4
	j)	List out the benefits of IP security?	2M	CO5	BL1

PART- B

(10*5 Marks = 50 Marks)

2		Discuss any four Substitution Technique and list their merits and demerits.	10M	CO1	BL1
		OR			
3	a)	Construct a Playfair matrix with the key largest. encrypt this message: MEET ME AT THE TOGA PARTY	5M	CO1	BL3
	b)	Explain the various active attacks? What security mechanisms are suggested to counter attack active attacks?	5M	CO1	BL2
4		Perform encryption and decryption using RSA Alg. for the following. P=17; q=11; e=7; M=88.	10M	CO2	BL5
		OR			
5		Give a detailed description of key generation and encryption of Data Encryption Standard (DES) algorithm	10M	CO2	BL1

6		Explain the process of deriving eighty 64-bitwords from 1024 bits for processing of a single blocks and also discuss single round function in SHA-512 algorithm. Show the values of W16, W17, W18 and W19.	10M	CO3	BL3
		OR			
7	a)	Explain HMAC algorithm. Comment on the security of HMAC	5M	CO3	BL5
	b)	Explain the authentication procedures defined by X.509 certificate?	5M	CO3	BL5
8		What protocols comprise SSL? What is the difference between an SSL connection and an SSL session?	10M	CO4	BL6
		OR			
9	a)	Explain Secure Electronic transaction with neat diagram.	5M	CO4	BL2
	b)	With a neat diagram explain the IEEE 802.11 Wireless LAN?	5M	CO4	BL1
10		In S/MIME, how does a receiver find out what cryptographic algorithms the sender has used when receives an S/MIME message.	10M	CO5	BL6
		OR			
11		How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.	10M	CO5	BL4

---oo0oo---

CO-Course Outcome **BL - Blooms Taxonomy Levels**