Course Code: 1971257 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

Information Security

(IT)

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)	Define security service.	2M	CO1	BL1
	b)	What are the uses of random number generation in Cryptography?	2M	CO1	BL1
	c)	What is Cryptanalysis?	2M	CO2	BL1
	d)	Compare hash function with MAC function.	2M	CO2	BL1
	e)	What is digital signature?	2M	CO3	BL1
	f)	Which problem was Kerberos designed to address?	2M	CO3	BL1
	g)	What is SSL?	2M	CO4	BL1
	h)	List the components of SET.	2M	CO4	BL1
	i)	Discuss about importance of firewall.	2M	CO5	BL4
	j)	Define computer virus.	2M	CO5	BL1

PART- B

(10*5 Marks = 50 Marks)

2	a)	Consider the following Plaintext : "CRYPTO" Secret Key: "NETWORK" Using hill cipher method, find the cipher text?	5M	CO1	BL1
	b)	Explain about traffic Confidentiality.	5M	CO1	BL1
		OR			
3		Discuss about the functionality of DES algorithm	10M	CO1	BL3

4		Users Alice and Bob use the Diffie-Hellman key exchange technique with a common price q=83 and a primitive root ὰ=5. a) If Alice has a private key X_A=6, what is Alice public key Y_A? b) If Bob has a private key X_B=10, What is Bob's public key Y_B? C) What is shared secret key?	10M	CO2	BL5
		OR			
5	a)	Explain in detail about working of SHA-512 algorithm	5M	CO2	BL1
	b)	What are the requirements of hash function?	5M	CO2	BL1
6		List the operations of PGP and explain along with key rings	10M	CO3	BL3
		OR			
7		What is the importance of digital signature standard? Explain its characteristics.	10M	CO3	BL5
8		Explain various ways of combining security associations.	10M	CO4	BL6
		OR			
9		Explain the operation of SSL handshake protocol & SSL alert protocol	10M	CO4	BL2
10		Discuss in detail about trusted system.	10M	CO5	BL6
		OR			
11		Explain various firewall configurations	10M	CO5	BL4

---oo0oo---

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