



# 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 Section 2(f) & 12(B) of the UGC act, 1956

II B.Tech II Sem Regular End Examination, July 2022

## Cryptography and Network Security

(CSC)

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) | What are the examples of security attacks? | 2M | C01 | BL1 |
| b)    | List out the security services.            | 2M | C01 | BL1 |
| c)    | Tell about Blowfish.                       | 2M | C02 | BL1 |
| d)    | Define knapsack algorithm.                 | 2M | C02 | BL1 |
| e)    | Describe HMAC.                             | 2M | C03 | BL2 |
| f)    | What is the X.509 Authentication service?  | 2M | C03 | BL1 |
| g)    | Which email is best for privacy?           | 2M | C04 | BL1 |
| h)    | List the benefits of IP security.          | 2M | C04 | BL1 |
| i)    | Mention the requirements of web security.  | 2M | C05 | BL1 |
| j)    | Summarize intruders.                       | 2M | C05 | BL1 |

### PART- B

(10\*5 Marks = 50 Marks)

- |      |   |    |     |     |
|------|---|----|-----|-----|
| 2 a) | What are Security attacks and its types.          | 5M | C01 | BL1 |
| b)   | Discuss the cryptography concepts and techniques. | 5M | C01 | BL2 |

OR

- |      |   |     |     |     |
|------|---|-----|-----|-----|
| 3    | Compare the substitution techniques and transposition techniques.       | 10M | C01 | BL2 |
| 4 a) | Where are the block cipher operations used and Describe stream ciphers. | 5M  | C02 | BL1 |
| b)   | How RC4 differ from RC5 brief.  | 5M  | C02 | BL1 |

OR

- |   |  |     |     |     |
|---|--|-----|-----|-----|
| 5 | Explain Diffie-Hellman key exchange with an example. | 10M | C02 | BL4 |
|---|--|-----|-----|-----|

- |           |   |     |     |     |
|-----------|---|-----|-----|-----|
| 6         | a) Demonstrate Kerberos.  | 5M  | C03 | BL5 |
|           | b) Elaborate Secure Hash algorithm.   | 5M  | C03 | BL5 |
| <b>OR</b> |   |     |     |     |
| 7         | Develop Symmetric key distribution using symmetric & asymmetric encryption by an example. | 10M | C03 | BL6 |
| 8         | a) Make use of pretty good privacy and S/MIME.  | 5M  | C04 | BL3 |
|           | b) Determine Authentication header.   | 5M  | C04 | BL3 |
| <b>OR</b> |   |     |     |     |
| 9         | Illustrate combining security association and key management.                             | 10M | C04 | BL3 |
| 10        | a) Design secure socket layer (SSL).  | 5M  | C05 | BL6 |
|           | b) How to predict Trusted systems?  | 5M  | C05 | BL1 |
| <b>OR</b> |   |     |     |     |
| 11        | Analyze Firewall design principles.   | 10M | C05 | BL4 |

---oo0oo---