UG/PG Even Semester Examination, 2025

COMPUTER SCIENCE

(10th Semester)

Course No.: MCSC-1002

(Cryptography)

Full Marks: 70

Pass Marks: 28

Time: 3 hours

The figures in the right margin indicate full marks for the question. Answer any five questions selecting one from each unit.

UNIT-I

1. What are the various types of attacks? What is a worm? What are the significant differences between a Worm and a virus? What is DDOS attack? 7+2+3+2=14

2. What are substitution and Transposition techniques? Give two examples of each. 4+5+5=14

UNIT-II

3. What are the two types of key arrangement? Explain them with proper diagrams. What are their advantages and disadvantages? 4+7+3=14.

4. Draw the diagram of DES and explain in full. explain the concept of triple DES. 7+7=14

UNIT-III

5. Explain 1) IDEA, 2) Blowfish, 3) RC2, 4)AES 3.5*4= 14

6. Explain Deffie Hellman Key Exchange Algorithm with a proper example. 7+7=14

UNIT-IV

7. Explain the RSA algorithm with a proper example. 7+7=14

8. Write technical notes on: a) MD5, b)SHA 7+7=14

UNIT-V

9. Explain working of Kerboros V4 with proper diagrams. 14

10. Write notes on: Digital signature, digital –watermarking 7+7=14

*****