# M.Sc. (DDE) 4th Semester Examination, 2019

## (Old Syllabus)

## Subject: Computer Science

## Paper: MCS-401 (Elective-II: Cryptography and Network Security)

**Full Marks: 22.5** **Time: 1 Hour**

**Answer Question 1 and any *three* from the rest.**

1. (a) Explain S-Box substitution of single DES algorithm. (7.5)

   Or

   (b) Discuss RSA cryptosystem in brief. (7.5)

2. Discuss the Rail Fence Transposition Technique with example. (5)

3. Discuss Output Feedback Mode (OFB) encryption. (5)

4. Explain the “man in the middle” attack with an example. (5)

5. Explain Digital Signature in brief. (5)

6. Discuss any one Primality testing for large integers in brief. (5)