M.Sc. (DDE) 4th Semester Examination, 2020

(Old Syllabus)

Subject: Computer Science

Paper: MCS-401 (Cryptography and Network Security)

Full Marks: 22.5 Time: 1 Hour

Answer Question number 1 and any three questions from the rest.

1. **Explain the expansion permutation of single DES algorithm. (7.5)**

   Or

   Discuss RSA algorithm in brief message encrytion. (7.5)

2. **Discuss the concept of confusion and diffusion with example. (5)**

3. **Discuss Cipher Block Chaining (CBC) encryption. (5)**

4. **Explain the Diffie-Hellman key exchange algorithm example. (5)**

5. **Discuss Digital Signature in brief. (5)**

6. **Discuss PGP for email security. (5)**