# Siddaganga Institute of Technology, Tumkur-572103

Department of Computer Science and Engineering

**CRYPTOGRAPHY AND NETWORK SECURITY LAB (7CSL02)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Student Name: | | | USN: | Batch No: | | Date: | |
| **Evaluation:** | | | | | | | |
| **Write Up (10 marks)** | **Clarity in concepts (10 marks)** | **Implementation and execution of the algorithms (10 marks)** | | | **Viva (05 marks)** | | **Total (35 marks)** |
|  |  |  | | |  | |  |
|  | | | | | | | |
| Sl.No | Name of the Faculty In-Charge | | | | | | Signature |
| 1. |  | | | | | |  |
| 2. |  | | | | | |  |
| **Question No: 10**  Implement RSA algorithm using client-server concept. The program should support the following :   1. Client generates {PU, PR} and distributes PU to Server. 2. Sever encrypts message M using client’s public key {PU}. 3. Client decrypts the message sent by server using its private key {PR}. | | | | | | | |
| Encryption and decryption are of the following form, for some plaintext block M and cipher text block C    Algorithm:  Client side calculations    Sever side encryption    Client-side decryption | | | | | | | |