# 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: 11**  Implement RSA algorithm to process blocks of plaintext (refer Figure 9.7 of the text book), where plaintext is a string of characters and let the block size be two characters. (Note: assign a unique code to each plain text character i.e., a=00, A=26). The program should support the following.   1. Accept string of characters as plaintext. 2. Encryption takes plaintext and produces ciphertext characters 3. Decryption takes ciphertext characters obtained in step ii and produces corresponding plaintext characters. 4. Display the result after each step | | | | | | | |
| Algorithm:   1. Generate *e,p,q* using random number generator. 2. Calculate n value , n=p×q. 3. Determine public and private keys *(e,n) and (d,n).* 4. Accept plain text in string format and assign numbers between 0 to 26 for characters (a to z) 5. Plain text in decimal string {p1,p2,p3….} is encrypted using public key as shown in fig 1.     Fig 1 Fig 2.   1. Transmit the cipher text in decimal format to server using through sockets for decryption.   Server should decrypt the cipher text {c1,c2,c3…} shown in fig 2. and print the string in character format back to screen. | | | | | | | |