PRIYADARSHINI COLLEGE OF ENGINEERING
(Recognised by A.I.C.T.E., New Delhi & Govt. of Maharashtra, Affiliated to
R.T.M.Nagpur University)Near CRPF Campus, Hingna Road,
Nagpur-440 019, Maharashtra (India)
Phone : 07104 – 236381, 237307, Fax : 07104 – 237681,

Practical No. 10

Aim:- To implement RSA Algorithm.

Theory:

RSA algorithm is a symmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

Algorithm :

1. Choose two large Prime numbers P and Q
2. Calculate N= P * Q
3. Select the Public Key (i.e the encryption key) E such that it is not a factor of (P-1) and (Q-1) .
4. Select the Private Key (i.e. decryption key) D such that the following equation is true.
   (D * E) mod (P-1) *(Q-1) =1
5. For Encryption , Calculate the Cipher text CT from the plain text PT as follows
   $CT = PT^{E} \bmod N$
6. Send CT as the Cipher text to the receiver.
7. For decryption, Calculate the plain text PT from the Cipher text CT as follows.
   $PT= CT^{D} \bmod N$.

Sample input and Output:

Input :
P=7 , q=17 and PT =10

Output: CT = 40

Conclusion: RSA Algorithm is implemented sucessfully.

Viva Questions:

1. What is RSA in the field of Cryptography ?
2. How fast is RSA ?