**Information and Network Security**

**2CSDE54**

**Practical 6**

**21BCE020**

**Implementation of RSA Algorithm**

#include <iostream>

#include <algorithm>

#include <string>

#include <fstream>

#include <cctype>

#include <math.h>

using namespace std;

int character\_to\_number(const char& ch){

    char c = toupper(ch);

    if (c >= 'A' && c <= 'Z') return c - 'A';

}

pair<int, int> compute\_Qn(int p, int q){

    int n = p \* q;

    int Qn = (p - 1) \* (q - 1);

    pair<int, int> pair = make\_pair(n, Qn);

    return pair;

}

int compute\_d(int Qn, int e, int T1, int T2){

    while(e > 0){

        int Q = Qn / e;

        int R = Qn % e;

        int T = T1 - (T2 \* Q);

        Qn = e;

        e = R;

        T1 = T2;

        T2 = T;

    }

    return T1;

}

int encrypt(int M, int e, int n){

    return int(pow(M, e)) % n;

}

int decrypt(int C, int d, int n){

    return int(pow(C, d)) % n;

}

int main() {

    ifstream f1("rsa\_inp.txt");

    ifstream f2("parameters.txt");

    char inp;

    int p, q, e;

    f1>>inp;

    f2>>p>>q>>e;

    pair<int, int> pair = compute\_Qn(p, q);

    int n = pair.first;

    int Qn = pair.second;

    int d = compute\_d(Qn, e, 0, 1);

    int PT = character\_to\_number(inp);

    int CT = encrypt(PT, e, n);

    int DT = decrypt(CT, d, n);

    ofstream f3("CT.txt");

    ofstream f4("PT.txt");

    cout<<"Original Message: "<<inp<<endl;

    f3<<"Encrypted Text: "<<CT<<endl;

    f4<<"Decrypted Text: "<<PT<<endl;

    cout<<"Encrypted Text: "<<CT<<endl;

    cout<<"Decrypted Text: "<<PT<<endl;

    f1.close();

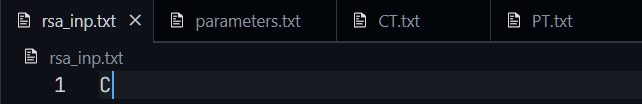
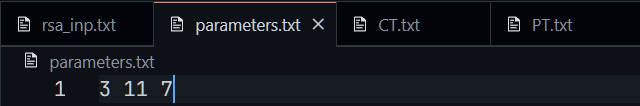
    f2.close();

    f3.close();

    f4.close();

}

**Text File Input:**

**** ****

**Text File Output:**