Experiment – 5

Name:Vivek Mote

Roll Number : 20141229

#include <bits/stdc++.h> using namespace std; int main()

{

cout<<"20141229 Vivek Mote \n"; cout<<"Implementation of RSA Algorithm \n"; cout << "Enter two prime numbers\n";

double num1, num2;

cin >> num1 >> num2; double n = num1 \* num2; double track;

double phi = (num1 - 1) \* (num2 - 1); double e = 7;

while (e < phi)

{

track = gcd((int)e, (int)phi); if (track == 1)

break; else

e++;

}

double d1 = 1 / e;

double d = fmod(d1, phi); double message; cout<<"Enter message\n";

cin>>message;

double c = pow(message, e); double m = pow(c, d);

c = fmod(c, n);

double c = pow(message, e); double m = pow(c, d);

c = fmod(c, n);

m = fmod(m, n);

cout << "Original Message = " << message; cout << "\n"<< "p = " << num1;

cout << "\n"<< "q = " << num2; cout << "\n"<< "n = pq = " << n; cout << "\n"<< "phi = " << phi; cout << "\n"<< "e = " << e;

cout << "\n"<< "d = " << d;

cout << "\n"<< "Encrypted message = " << c; cout << "\n"<< "Decrypted message = " << m; return 0;

}

