

**AHSANULLAH UNIVERSITY OF SCIENCE AND TECHNOLOGY**

Department of Computer Science and Engineering

Program: Bachelor of Science in Computer Science and Engineering

Course Code: CSE 4174

Course Title: Cyber Security Lab

Academic Semester: Spring 2023

Assignment Topic: RSA (Rivest-Shamir-Adleman) Algorithm

Submitted on:27th November 2023

Submitted by

Name: SHUVASHIS SARKER

Student ID: ***20200104116***

Lab Section: C1

**Question:**

Devise a program using the RSA algorithm demonstrating the key set up and encryption-decryption.

*Code:*

#include<bits/stdc++.h>

using namespace std;

long int p, q, n, t, flag, e[100], d[100], temp[100], j, m[100], en[100], i;

string msg;

int prime(long int);

void ce();

long int cd(long int);

void encrypt();

void decrypt();

void printValues();

void printPossibleValues();

int main()

{

cout << "\nEnter the value of p: ";

cin >> p;

flag = prime(p);

if (flag == 0)

{

cout << "\nWRONG INPUT\n";

return 0;

}

cout << "\nEnter the value of q: ";

cin >> q;

flag = prime(q);

if (flag == 0 || p == q)

{

cout << "\nWRONG INPUT\n";

return 0;

}

cout << "\nEnter the message: ";

fflush(stdin);

getline(cin,msg);

//cout <<msg;

for (i = 0; i<msg.length(); i++)

m[i] = msg[i];

n = p \* q;

t = (p - 1) \* (q - 1);

ce();

printValues();

printPossibleValues();

encrypt();

decrypt();

return 0;

}

void printValues()

{

cout << "\nThe value of n is " << n;

cout << "\nThe value of phi(n) is " << t;

cout << "\nThe value of e is " << e[0];

cout << "\nThe value of d is " << d[0];

cout << "\nEnter the message: " << msg << endl;

}

void printPossibleValues()

{

cout << "\nPOSSIBLE VALUES OF e AND d ARE\n";

for (i = 0; i < j - 1; i++)

cout << "\n" << e[i] << "\t" << d[i];

}

int prime(long int pr)

{

int i;

j = sqrt(pr);

for (i = 2; i <= j; i++)

{

if (pr % i == 0)

return 0;

}

return 1;

}

void ce()

{

int k;

k = 0;

for (i = 2; i < t; i++)

{

if (t % i == 0)

continue;

flag = prime(i);

if (flag == 1 && i != p && i != q)

{

e[k] = i;

flag = cd(e[k]);

if (flag > 0)

{

d[k] = flag;

k++;

}

if (k == 99)

break;

}

}

}

long int cd(long int x)

{

long int k = 1;

while (1)

{

k = k + t;

if (k % x == 0)

return (k / x);

}

}

void encrypt()

{

long int pt, ct, key = e[0], k, len;

i = 0;

len = msg.length();

while (i != len)

{

pt = m[i];

pt = pt - 96;

k = 1;

for (j = 0; j < key; j++)

{

k = k \* pt;

k = k % n;

}

temp[i] = k;

ct = k + 96;

en[i] = ct;

i++;

}

en[i] = -1;

cout << "\nThe encrypted message is: ";

for (i = 0; en[i] != -1; i++)

cout << (char)en[i];

cout << endl;

}

void decrypt()

{

long int pt, ct, key = d[0], k;

i = 0;

while (en[i] != -1)

{

ct = temp[i];

k = 1;

for (j = 0; j < key; j++)

{

k = k \* ct;

k = k % n;

}

pt = k + 96;

m[i] = pt;

i++;

}

m[i] = -1;

cout << "\nThe decrypted message is: ";

for (i = 0; m[i] != -1; i++)

cout << (char)m[i];

cout << endl;

}

