Министерство образования Республики Беларусь

Учреждение образования

Кафедра ИИТ

Лабораторная работа №6

По дисциплине «Традиционные и интеллектуальные информационные технологии»

# Тема: « Двухключевая система RSA»

**Выполнил:**

Студент 1 курса

Группы ИИ-23

Макаревич Никита

**Проверила:**

Слинко Е.В.

Брест 2022

Вариант 2

Цель: Построить двухключевую систему с использованием алгоритма RSA и выполнить в ней операцию шифрования и дешифрования трех первых букв фамилии студента (при количестве букв меньше 3, недостающие буквы берутся из имени). Пара простых чисел P и Q выбирается из диапазона ближайших к количеству букв в фамилии и имени студента.

Ход работы:

Написал программу шифрующую слова.

Код программы:

#include <cmath>

#include <iostream>

using namespace std;

int nod(int a, int b)

{

while(a!=0 && b!=0)

{

if (a > b)

a = a % b;

else

b = b % a;

}

int c = a + b;

return c;

}

bool checkPrimeNumber(int);

bool checkPrimeNumber(int n) {

bool isPrimeNumber = true;

if (n == 0 || n == 1) {

isPrimeNumber = false;

}

else {

for (int i = 2; i < n; ++i) {

if (n % i == 0) {

isPrimeNumber = false;

break;

}

}

}

return isPrimeNumber;

}

int main()

{

int p, q, n, l, e, d, m[3] = { 1,12,14 }, error = 0, c[3], mm[3];

//{MAK}={AKM}={1,12,14}

do

{

cout << "enter p & q: ";

cin >> p >> q;

if (checkPrimeNumber(p) && checkPrimeNumber(q))

{

n = p \* q;

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

cout << "enter D: ";

cin >> d;

if (nod(d,l)==1)

{

cout << "enter E: ";

cin >> e;

if(e\*d%l==1)

{

c[0] = (int)pow(m[0], e) % n;

c[1] = (int)pow(m[1], e) % n;

c[2] = (int)pow(m[2], e) % n;

cout << "encrypted code: " << c[0] << " " << c[1] << " " << c[2] << endl;

cout << "D = " << d << " N = " << n << endl;

mm[0] = (int)pow(c[0], d) % n;

mm[1] = (int)pow(c[1], d) % n;

mm[2] = (int)pow(c[2], d) % n;

cout << "original code: " << mm[0] << " " << mm[1] << " " << mm[2] << endl;

error = 0;

}

else

{

error++;

cout << "something wrong..." << endl;

}

}

else

{

error++;

cout << "something wrong..." << endl;

}

}

else

{

error++;

cout << "something wrong..." << endl;

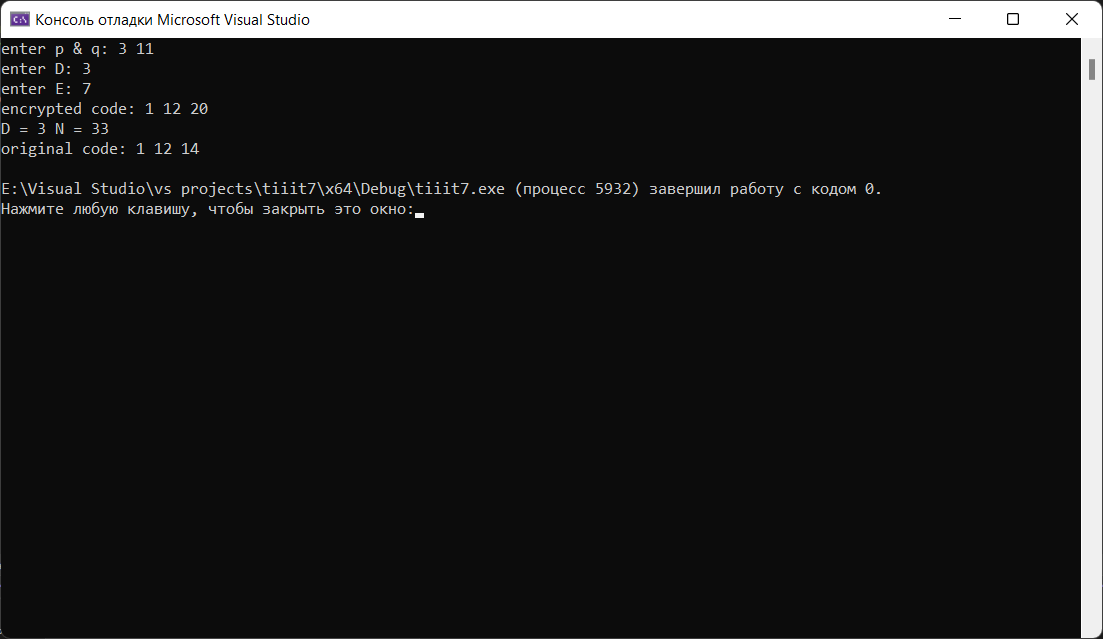
}

} while (error != 0);

return 0;

}

Результат:



Вывод: Написал программу для вычисления секретных ключей.