МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”

**ИНТЕЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

ОТЧЁТ

По лабораторной работе №7

Выполнил:

Студент группы ИИ-22

Копанчук Евгений Романович

Проверил:

Скарубо А. О.

Брест - 2021

**Двухключевая система RSA**

**Задание:** 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.

**Код программы:**

#include <iostream>

#include <cmath>

using namespace std;

int NOD(int a, int b){

while(a > 0 && b > 0)

if(a > b)a %= b;

else b %= a;

return a + b;

}

int coding(int M, int E, int N){

return (int) pow(M,E) % N;

}

int decoding(int C, int D, int N){

return (int) pow(C,D) % N;

}

int main(){

int P, Q;

cout << "Введите P и Q\n";

cin >> P >> Q;

int N = P\*Q;

int L = (P-1)\*(Q-1);

int D;

for (int i = 2; i < L; i++)

if (NOD(i,L) == 1) {

D = i;

break;

}

int E = 0;

while ((E\*D) % L != 1){

E++;

}

cout << "L = " << L << " N = " << N << " D = " << D << " E = " << E << endl;

unsigned long long int M, C;

for (int i = 1; i < 4; i++){

cin >> M;

C = coding(M,E,N);

cout << "C = "<< C << " M = " << decoding(C,D,N) << endl;

}

return 0;

}

