Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

**Лабораторная работа №7**

По дисциплине «Традиционные и интеллектуальные информационные технологии»

Тема: «Двухключевая система RSA»

**Выполнил:**

Студент 1 курса

Группы ИИ-21

Карагодин Д.Л.

**Проверил:**

Слинко Е.В.

Брест 2021

**Цель работы:** Построить двухключевую систему с использованием алгоритма RSA.

**Ход работы:**

1. **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.**

Фамилия: Карагодин

Имя: Даниил

P = 7, Q = 5

**Код программы:**

#include <iostream>

#include <cmath>

using namespace std;

int main() {

char symbols[3] = { 'P','A','K' };

int P = 7, Q = 5, N = P \* Q, L = (P - 1) \* (Q - 1), D, E;

for (D = 2;; D++) {if (L % D != 0) break;}

cout << "D:" << D << endl;

for (E = 1;; E++) {if ((E \* D) % L == 1) break;}

cout << "E:" << E << endl;

int s[3] ={

int(pow(3,E)) % N,

int(pow(2,E)) % N,

int(pow(1,E)) % N,};

cout << "Shifr text: " << s[0] << " "

<< s[1] << " " << s[2] << endl;

int ls[3] ={

int(pow(s[0],D)) % N,

int(pow(s[1],D)) % N,

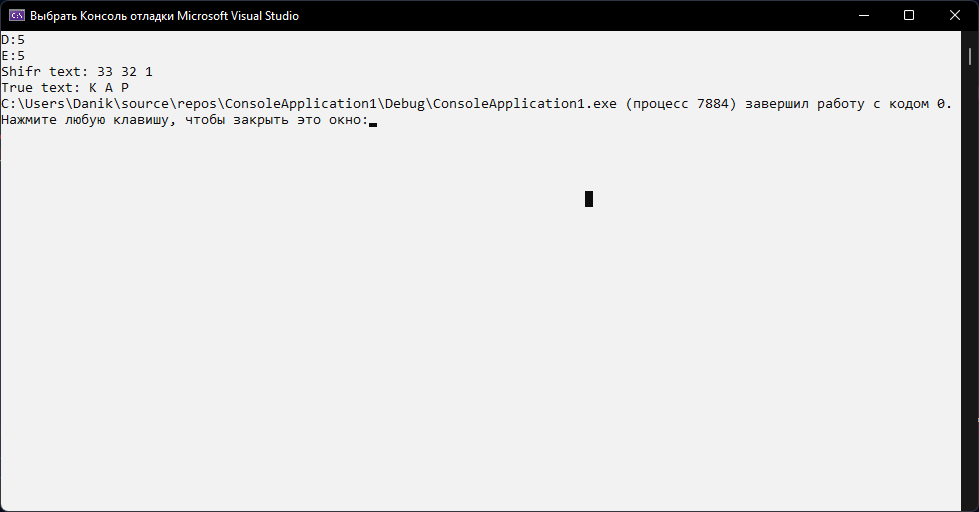
int(pow(s[2],D)) % N,};

cout << "True text: " << symbols[ls[0] - 1] << " "

<< symbols[ls[1] - 1] << " " << symbols[ls[2] - 1];

return EXIT\_SUCCESS;}

**Результат программы:**



**Вывод:** Построил двухключевую систему с использованием алгоритма RSA.