Министерство образования Республики Беларусь

Учреждение образования

Кафедра ИИТ

Лабораторная работа №7

По дисциплине «Традиционные и интеллектуальные информационные технологии»

# Тема: «Двухключевая система RSA »

Выполнил:

Студент 1 курса

Группы ИИ-23

Романюк А.П.

Проверила:

Слинко Е.В.

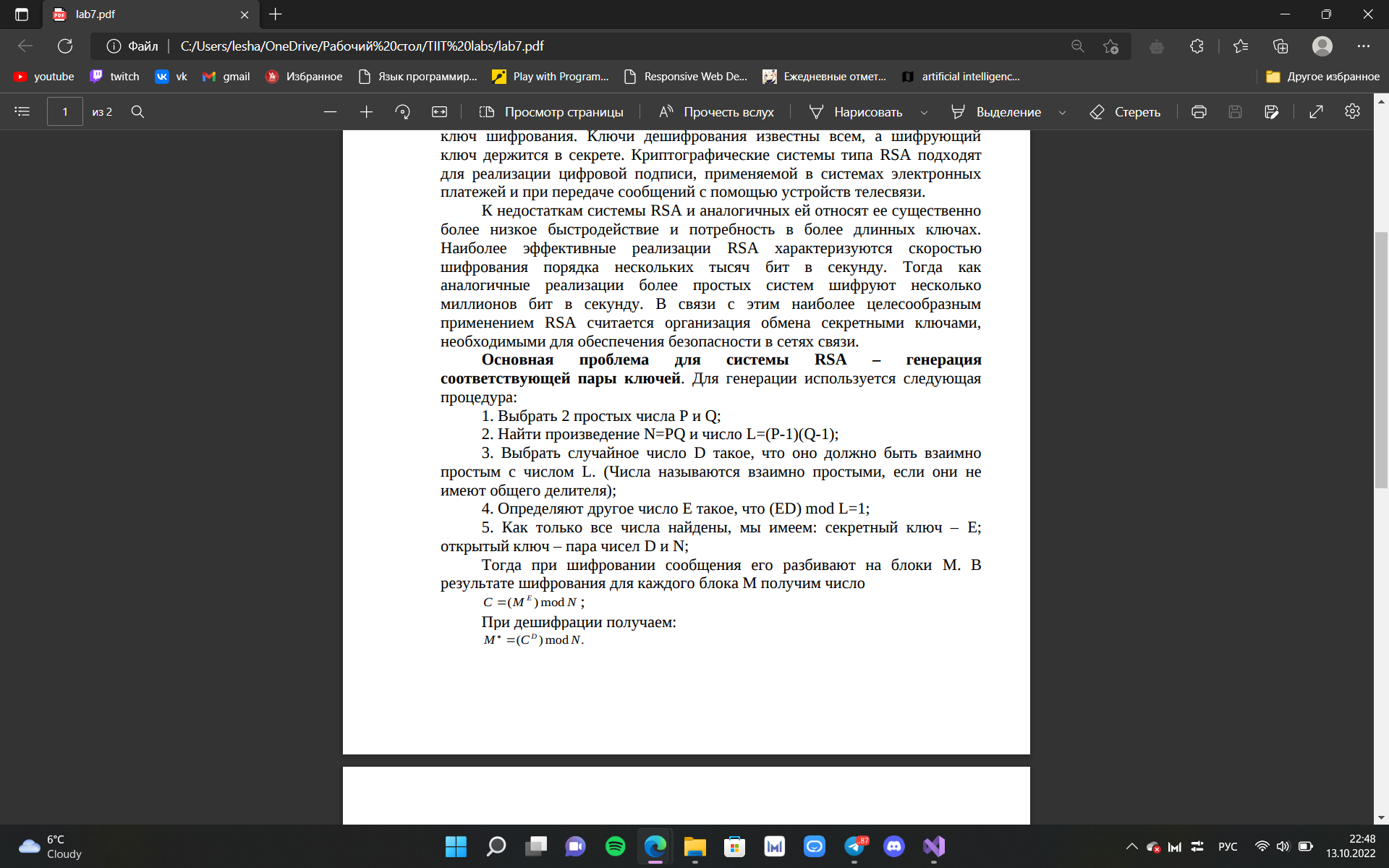
Вариант 8

Цель: 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.

Ход работы:

Написал программу шифрующую слова.

Алгоритм шифрования и дешифровки:



Код программы:

#include <iostream>

#include <cmath>

#include <string>

using namespace std;

int main()

{

long long int word[8], p, q, n, l, d = 0 , e = 0,k = 0;

long long int shifr[8];

string s;

cout << "Введите слово ";

cin >> s;

for (int i = 0; i < s.length(); i++)

word[i] = s[i] - 96;

cout << "Введите два простых числа ";

cin >> p >> q;

n = p \* q;

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

while (!k) { //подбираем взаимопростое число

d = d + 1;

if (l%d > 0) {

k = 1;

}

}

k = 0;

cout << "Открытый ключ " << d <<" "<<n << endl;

while (!k) { //подбираем закрытый ключ

e = e + 1;

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

k = 1;

}

}

cout << "Секретный ключ " << e << endl;

cout << "Закодированный текст ";

for (int i = 0; i < s.length(); i++) {//шифруем

shifr[i] = int(pow(word[i], e)) % n;

s[i] = shifr[i] + 96;

cout << s[i]<<" ";

}

cout << endl;

cout << "Расшифрованный текст ";

for (int i = 0; i < s.length(); i++) {//расшифруем

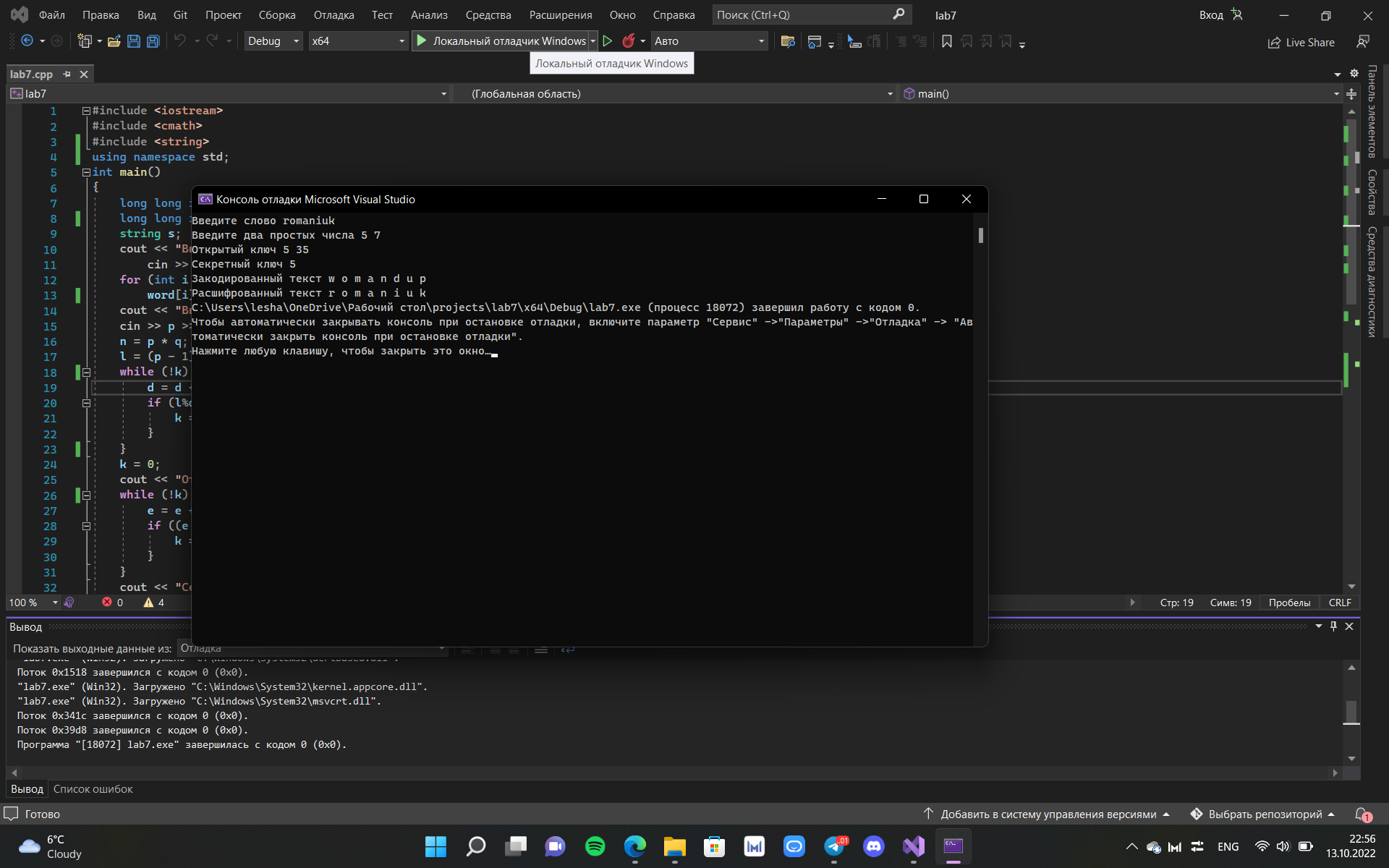
shifr[i] = int(pow(shifr[i], d)) % n;

s[i] = shifr[i] + 96;

cout << s[i] << " ";

}

}



Вывод:Написал программу для шифрования и дешифрования слов.