Министерство образования Республики Беларусь

Учреждение образования

Кафедра ИИТ

Лабораторная работа №6

По дисциплине «Традиционные и интеллектуальные информационные технологии»

# Тема: « **Одноключевая система шифрования Диффи и Хеллмана**»

Выполнил:

Студент 1 курса

Группы ИИ-23

Романюк А.П.

Проверила:

Слинко Е.В.

Вариант 8

Цель: Построить систему шифрования Диффи и Хеллмана для а=(количество согласных букв в фамилии студента), р больше или равно количеству всех букв в фамилии. Подобрать а и р самостоятельно методом проб и ошибок, выбрать два секретных числа Хi и Хj и для связи пользователей сети i и j вычислить числа Zij и Zji.

Ход работы:

Написал программу вычисляющую секретные ключи для общения двух пользователей.

Код программы:

#include <iostream>

#include <cmath>

using namespace std;

int main()

{

long long int a = 4, p = 11, xi, xj,yi,yj;

int zij, zji;

cout << "Введите ключ ";

cin >> xi;//первое секретное число

yi = int(pow(a, xi)) % p;//вычисляем публичное число 1 человека

cout << "Введите ключ ";

cin >> xj;//второе секретное число

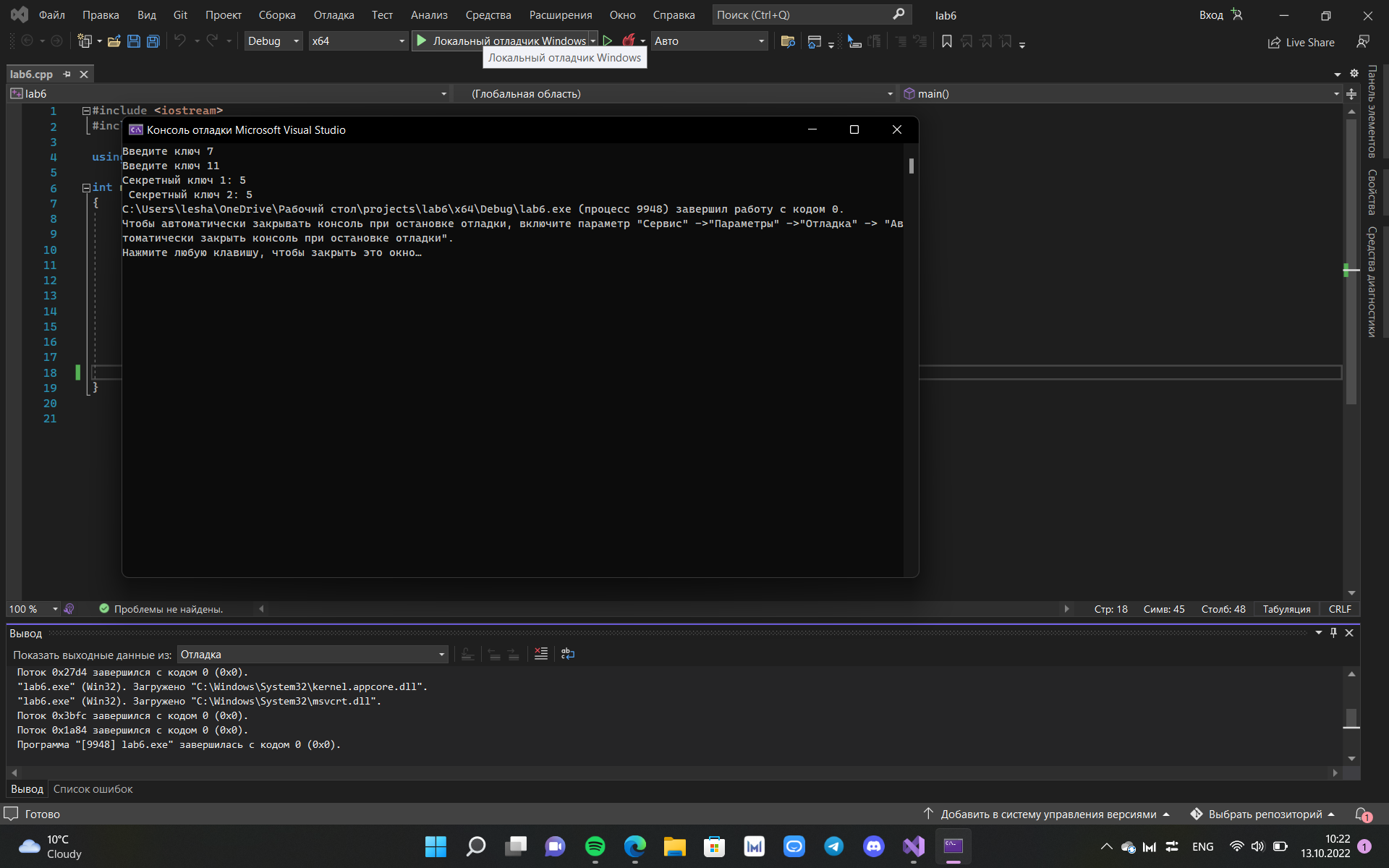
zij = int(pow(yi, xj)) % p;//вычисляем секретный ключ 1 человека

yj = int(pow(a, xj)) % p;//вычисляем публичное число 2 человека

zji = int(pow(yj,xi)) % p;//вычисляем секретный ключ 2 человека

cout <<"Секретный ключ 1: " << zij << " Секретный ключ 2: " << zji;

}



Вывод:Написал программу для вычисления секретных ключей.