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

Макаревич Никита

**Проверила:**

Слинко Е.В.

Брест 2022

Вариант 2

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()

{

int p=11, a=5, xi,xj, yi, yj, zij, zji;

cout << "enter Xi: ";

cin >>xi;

yi = (int)pow(a,xi) % p;

cout << "Yi = " << yi << endl;

cout << "enter Xj: ";

cin >> xj;

yj = (int)pow(a, xj) % p;

cout << "Yj = " << yj << endl;

zij = (int)pow(yi, xj) % p;

zji = (int)pow(yj, xi) % p;

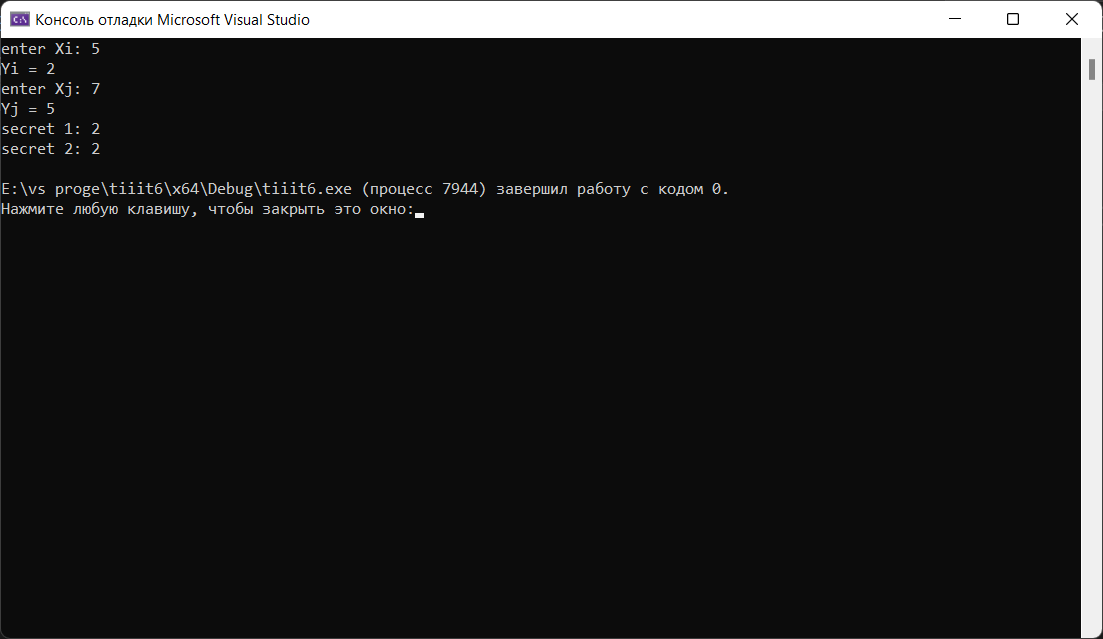
cout << "secret 1: " << zij << endl;

cout << "secret 2: " << zij << endl;

return 0;

}

Результат:



Вывод: Написал программу для вычисления секретных ключей.