Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

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-21

Карагодин Д.Л.

**Проверил:**

Слинко Е.В.

Брест 2021

**Цель работы:** Построить систему шифрования Диффи и Хеллмана.

**Ход работы:**

1. **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.**

а = 5 , р = 9 (Карагодин).

**Код программы:**

#include <iostream>

#include <cmath>

using namespace std;

int main() {

int a=5, p=9, xi, xj, yi, yj, zi, zj, buffer;

cout << "Please,write first key(from 1 to 8): ";

cin >> xi;

cout<< "Please,write second key(from 1 to 8): ";

cin >> xj;

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

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

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

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

if (zi == zj) {cout<<"Secret key: " << zi;}

else { cout << "Error :("; }

return EXIT\_SUCCESS;

}

**Результат программы:**



**Вывод:** Построил систему шифрования Диффи и Хеллмана.