***Министерство образования Республики Беларусь***

***Учреждение Образования***

***«Брестский Государственный Технический Университет»***

***Кафедра ИИТ***

**Лабораторная работа №7**

**По дисциплине «Традиционные и интеллектуальные**

**информационные технологии»**

**Тема:**

**«****Одноключевая система шифрования Диффи и Хеллмана»**

**Выполнил:**

Студент 1-го курса

Группы ИИ-15(1)

Волк И. А.

**Проверил:**

Анфилец С. В.

Брест 2018

Цель: познакомиться с одноключевой системой шифрования Диффи и Хеллмана.

***Задание:***

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.

Код программы:

#include "stdafx.h"

#include <Windows.h>

#include <iostream>

#include <conio.h>

#include <string>

#include <cmath>

using namespace std;

const int a = 3, p = 5;

int main()

{

// private numbers

int \* privateNumbers = new int[2];

privateNumbers[0] = 2;

privateNumbers[1] = 4;

for (int i = 0; i < 2; i++)

cout << "PrivateNumber #" << i + 1 << ": " << privateNumbers[i] << endl;

cout << endl;

// results

int \* results = new int[2];

results[0] = (int)pow(a, (double)privateNumbers[0]) % p;

results[1] = (int)pow(a, (double)privateNumbers[1]) % p;

for (int i = 0; i < 2; i++)

cout << "Result #" << i + 1 << ": " << results[i] << endl;

cout << endl;

// keys

int keys[2] = { (int)pow((double)results[0],(double)privateNumbers[1])%p,

(int)pow((double)results[1],(double)privateNumbers[0])%p };

for (int i = 0; i < 2; i++)

cout << "Key #" << i + 1 << ": " << keys[i] << endl;

// keys is equal

if (keys[0] == keys[1])

cout << "Keys is equal." << endl;

cout << endl;

char message[1024];

cout << "Enter the message: "; gets\_s(message);

cout << "Encrypted message: ";

int i = 0;

while (message[i] != '\0')

{

cout << (char)((int)message[i] + 1);

i++;

}

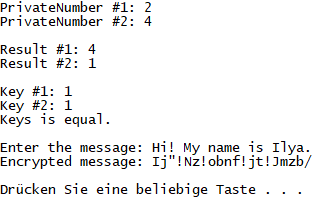
cout << endl << endl;

system("pause");

return 0;

}

Output:



Вывод: по ходу лабораторной работы познакомился с одноключевой системой шифрования Диффи и Хеллмана.