***Министерство образования Республики Беларусь***

***Учреждение Образования***

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

***Кафедра ИИТ***

**Лабораторная работа №8**

**По дисциплине «Традиционные и интеллектуальные**

**информационные технологии»**

**Тема:**

**«Двухключевая система RSA»**

**Выполнил:**

Студент 1-го курса

Группы ИИ-15(1)

Волк И. А.

**Проверил:**

Анфилец С. В.

Брест 2018

Цель: познакомиться с двухключевой системой шифрования RSA.

***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.

Код программы:

#include "stdafx.h"

#include <iostream>

#include <Windows.h>

#include <cmath>

#include <conio.h>

using namespace std;

int encryptCh(int, int, int);

char \* encrypt(int, int, char\*);

int decryptCh(int, int, int);

char \* decrypt(int, int, char\*);

int main()

{

int p = 3, q = 11;

int N = p\*q, L = (p - 1)\*(q - 1);

int e = 7, d = 3;

while (1)

{

system("cls");

char \* message = new char[1024];

cin >> message; cout << endl;

message = encrypt(e, N, message);

cout << "Encrypt: " << message << endl;

message = decrypt(d, N, message);

cout << "Decrypt: " << message << endl;

int input = \_getch();

if (input == 27)

break;

}

system("pause");

return 0;

}

char \* encrypt(int e, int N, char\* message)

{

int i = 0;

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

{

int chInt = (int)message[i] - 104;

double chDouble = pow((double)chInt, (double)e);

int chRes = (long long)chDouble % N;

message[i] = (char)chRes;

i++;

}

return message;

}

char \* decrypt(int d, int N, char\* message)

{

int i = 0;

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

{

int chInt = (int)message[i];

double chDouble = pow((double)chInt, (double)d);

int chRes = (long long)chDouble % N;

message[i] = (char)(chRes+104);

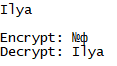
i++;

}

return message;

}

Output:



Вывод: по ходу лабораторной работы познакомился с двухключевой системой шифрования RSA.