МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”

**ИНТЕЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

ОТЧЁТ

По лабораторной работе №6

Выполнил:

Студент группы ИИ-22

Копанчук Евгений Романович

Проверил:

Скарубо А. О.

Брест - 2021

**Ход работы**

**“Одноключевая система 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.

Для начала сделаем калькулятор для нахождения значения P. Оно по условию задачи должно быть не меньше 9. Число А в моём варианте равно 5.

**Код программы:**

#include <iostream>

#include <cmath>

#include <vector>

using namespace std;

int main()

{

unsigned long long int fst\_ans, p, a, o = 1, k;

cin >> p;

vector <int> ans(p-1);

a = 5;

fst\_ans = a - a / p \* p;

while (o < p)

{

ans[o-1] = pow(a,o) - (unsigned long long int) pow(a,o) / p \* p;

o++;

}

for (int i = 0; i < p-1; i++)

for (int j = 0; j < p-2; j++)

if (ans[j] > ans[j+1])

{

k = ans[j];

ans[j] = ans[j+1];

ans[j+1] = k;

}

for (int i = 0; i < p-1; i++) cout << ans[i] << " ";

return 0;

}Поочерёдно перебрав значения, получаем число 17:



Теперь найдём значения Z(ij) и Z(ji):

**Код программы:**

#include <iostream>

#include <cmath>

using namespace std;

int main()

{

int i, j, number;

cout << "Введите ваш ключ i\n";

cin >> i;

cout << "Введите ключ другого пользователя j\n";

cin >> j;

cout << "Z(JI) = " << pow(j,i) - (int) pow(j,i) / 17 \* 17 << endl;

cout << "Z(IJ) = " << pow(i,j) - (int) pow(i,j) / 17 \* 17 << endl;

return 0;

}

