

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

Лабораторная работа №4

по дисциплине: «Теоретико-числовые методы в криптографии»

на тему: «Система сравнений первой степени.»

Выполнил обучающийся гр. ВКБ42

Михайлов Александр Сергеевич

          Проверила:

Ст. пр. Артамонова Е.А.

Ростов-на-Дону

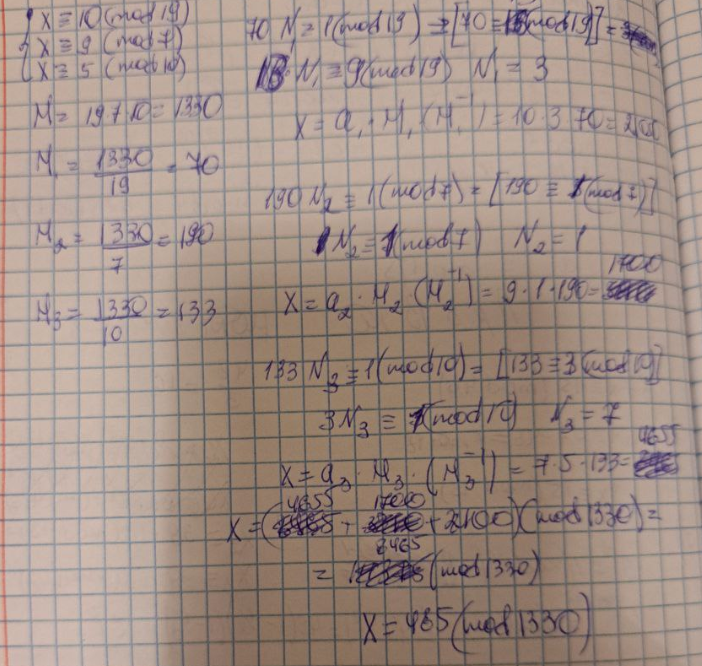
2024

Лабораторная работа №4

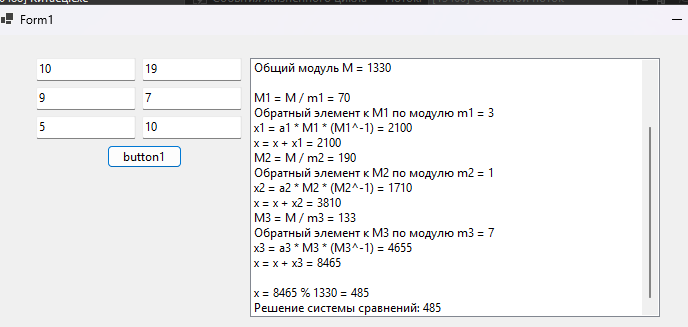
«Система сравнений первой степени.»

Вариант №20

**Ручная реализация.**



**Входные данные.**



**Листинг программы.**

using System.Windows.Forms;

using static System.Windows.Forms.VisualStyles.VisualStyleElement;

namespace Китаец

{

public partial class Form1 : Form

{

public Form1()

{

InitializeComponent();

}

private void button1\_Click(object sender, EventArgs e)

{

// Очищаем ListBox перед началом вычислений

ListBox1.Items.Clear();

// Считываем значения из TextBox'ов

int a1 = int.Parse(textBox1.Text);

int a2 = int.Parse(textBox2.Text);

int a3 = int.Parse(textBox3.Text);

int m1 = int.Parse(textBox4.Text);

int m2 = int.Parse(textBox5.Text);

int m3 = int.Parse(textBox6.Text);

// Выводим исходные данные

ListBox1.Items.Add("Исходные данные:");

ListBox1.Items.Add($"a1 = {a1}, m1 = {m1}");

ListBox1.Items.Add($"a2 = {a2}, m2 = {m2}");

ListBox1.Items.Add($"a3 = {a3}, m3 = {m3}");

ListBox1.Items.Add("");

// Решаем систему сравнений по китайской теореме

int result = ChineseRemainderTheorem(new int[] { a1, a2, a3 }, new int[] { m1, m2, m3 });

// Выводим результат

ListBox1.Items.Add($"Решение системы сравнений: {result}");

}

private int ChineseRemainderTheorem(int[] a, int[] m)

{

int M = 1;

foreach (int mi in m)

{

M \*= mi;

}

ListBox1.Items.Add($"Общий модуль M = {M}");

ListBox1.Items.Add("");

int x = 0;

for (int i = 0; i < a.Length; i++)

{

int Mi = M / m[i];

ListBox1.Items.Add($"M{i + 1} = M / m{i + 1} = {Mi}");

int Mi\_inv = ModInverse(Mi, m[i]);

ListBox1.Items.Add($"Обратный элемент к M{i + 1} по модулю m{i + 1} = {Mi\_inv}");

int xi = a[i] \* Mi \* Mi\_inv;

ListBox1.Items.Add($"x{i + 1} = a{i + 1} \* M{i + 1} \* (M{i + 1}^-1) = {xi}");

x += xi;

ListBox1.Items.Add($"x = x + x{i + 1} = {x}");

}

ListBox1.Items.Add("");

int result = x % M;

ListBox1.Items.Add($"x = {x} % {M} = {result}");

return result;

}

private int ModInverse(int a, int m)

{

int m0 = m;

int y = 0, x = 1;

if (m == 1)

return 0;

while (a > 1)

{

int q = a / m;

int t = m;

m = a % m;

a = t;

t = y;

y = x - q \* y;

x = t;

}

if (x < 0)

x += m0;

return x;

}

}

}

**Вывод по работе:**

В ходе выполнения лабораторной работы были изучены лекционный материал и алгоритм для решения систем сравнений первой степени.