Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

Институт Вычислительной математики и информационных технологий

ОТЧЕТ

по научно-исследовательской работе (производственной) практике

Обучающийся Гусев Виталий Евгеньевич гр.09-335 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО студента) (Группа) (Подпись)

Научный руководитель:

доцент КСАИТ Мубараков Б.Г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Подпись)

Руководитель практики от кафедры:

ст.преподаватель КСАИТ Тихонова О.О. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Подпись)

Оценка за практику \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Подпись)

Дата сдачи отчета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Казань – 2025

**ОГЛАВЛЕНИЕ**

[ВВЕДЕНИЕ……………………………………………………………………….. 3](#_heading=h.30j0zll)

[1. Название 1 главы](#_heading=h.17dp8vu)………………………………………………………………… [4](#_heading=h.17dp8vu)

[2. Название 2 главы](#_heading=h.3rdcrjn)………………………………………………………………. [5](#_heading=h.3rdcrjn)

[3. Название 3 главы](#_heading=h.26in1rg)………………………………………………………………. [6](#_heading=h.26in1rg)

[ЗАКЛЮЧЕНИЕ…………………………………………………………………… 7](#_heading=h.lnxbz9)

[СПИСОК ЛИТЕРАТУРЫ………………………………………………………... 8](#_heading=h.35nkun2)

[ПРИЛОЖЕНИЯ…………………………………………………………………... 9](#_heading=h.1ksv4uv)

**ВВЕДЕНИЕ**

Производственная практика проходила на кафедре системного анализа и информационных технологий Института вычислительной математики и информационных технологий КФУ с 21 марта 2025 года по 25 мая 2025 года.

Целью практики является исследование и реализация тестов для базовых и модифицированных алгоритмов дискретного логарифмирования с экспоненциальной и субэкспоненциальной сложностью.

Задачами практики являются:

1) разработать тесты для базовых и модифицированных методов дискретного логарифмирования,

2) программно реализовать тесты для базовых и модифицированных методов дискретного логарифмирования,

3) провести эксперименты на реализованных тестах для базовых и модифицированных методов дискретного логарифмирования.

1. **Название 1 главы**
2. **Название 2 главы**
3. **Название 3 главы**

# **ЗАКЛЮЧЕНИЕ**

В результате практики были реализованы и исследованы тесты для базовых и модифицированных алгоритмов дискретного логарифмирования.

За период практики были приобретены следующие компетенции (таблица N):

|  |  |  |
| --- | --- | --- |
| Компетенция | Расшифровка компетенции | Описание приобретенных знаний, умений и навыков |
| УК-1 | Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий | Получена способность осуществлять критический анализ проблемных ситуаций на основе системного подхода при разработке тестов дискретного логарифмирования |
| УК-6 | Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки | Приобретена способность реализовывать приоритеты собственной деятельности при разработке тестов дискретного логарифмирования на основе самооценки |
| ОПК-1 | Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий | Получен навык находить, формулировать и решать актуальные проблемы прикладной математики при разработке тестов дискретного логарифмирования |
| ОПК-2 | Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности | Получена способность применять компьютерные методы, современное программное обеспечение для решения задач профессиональной деятельности при разработке тестов дискретного логарифмирования |
| ОПК-3 | Способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования | Приобретена способность проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики при разработке тестов дискретного логарифмирования |
| ОПК-4 | Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности | Приобретён навык оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности при разработке тестов дискретного логарифмирования |

На основе тестов есть возможность сделать вывод, что определённые модифицированные алгоритмы дискретного логарифмирования показали лучше показатели в скорости выполнения или в затраченной памяти по сравнению с базовыми алгоритмами.

# **СПИСОК ЛИТЕРАТУРЫ**

1) Теоретический минимум и алгоритмы цифровой подписи / Молдовян Н. А. – Текст: непосредственный // Книжный Дом «ЛИБРОКОМ», 2010. — С. 304.

2) The infrastructure of a real quadratic field and its applications. Proceedings of the Number Theory Conference. / D. Shanks. – Текст: непосредственный // University of Colorado, Boulder, 1972. — С. 217-224.

3) An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographic Significance (англ.) / S. C. Pohlig and M. E. Hellman. - Текст: непосредственный // IEEE Transactions on Information Theory. — 1978. — Vol. 1, no. 24. — С. 106-110.

4) Theorems on factorization and primality testing / Pollard J.M. - Текст: непосредственный // Mathematical Proceedings of the Cambridge Philosophical Society. — 1974. — Т. 76, вып. 03. — С. 521–528.

5) A subexponential algorithm for discrete logarithms over all finite fields / Adleman L. M., Demarrais J. - Текст: непосредственный // Mathematics of computation. — 1993.

6) Теоретико-числовые алгоритмы в криптографии. / Василенко О.Н. - Текст: непосредственный // N— М.: МЦНМО, 2003. — C. 328.

7) Методы факторизации натуральных чисел. / Ишмухаметов Ш. Т. - Текст: непосредственный // — Казань: Казан. ун.. — 2011. — C. 190.

8) Applied Cryptography: Protocols, Algorithms, and Source Code in C. / Schneier, Bruce – Текст: непосредственный // Second Edition. — 2nd. — Wiley, 1996.

9) Методы факторизации натуральных чисел. / Ишмухаметов Ш. Т. - Текст: непосредственный // — Казань: Казан. ун.. — 2011. — C. 10.

10) Методы факторизации натуральных чисел. / Ишмухаметов Ш. Т. - Текст: непосредственный // — Казань: Казан. ун.. — 2011. — C. 52.

# **ПРИЛОЖЕНИЯ**

using DiscreteLogarithm.ExponentialAlgorithms;

using DiscreteLogarithm.MathFunctionsForCalculation;

using DiscreteLogarithm.ModifiedExponentialAlgorithms;

using DiscreteLogarithm.ModifiedSubExponentialAlgorithms;

using DiscreteLogarithm.SubExponentialAlgorithms;

using System.Diagnostics;

using System.Numerics;

using System.Security.Cryptography;

namespace DiscreteLogarithmCore

{

public partial class Form1 : Form

{

MathFunctions mathFunctions;

Shenks shenks;

ModifiedShenks modifiedShenks;

PoligHellman poligHellman;

ModifiedPoligHellman modifiedPoligHellman;

RoPollard roPollard;

ModifiedRoPollard modifiedRoPollard;

Adleman adleman;

ModifiedAdleman modifiedAdleman;

COS cos;

ModifiedCOS modifiedCOS;

GNFS gNFS;

ModifiedGNFS modifiedGNFS;

public Form1()

{

InitializeComponent();

mathFunctions = new MathFunctions();

}

private void button1\_Click\_1(object sender, EventArgs e)

{

BigInteger N;

bool theValuesAreCorrect = true;

gNFS = new GNFS();

gNFS.CheckingTheInputValues(textBox1.Text, label28, ref theValuesAreCorrect, out N);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

try

{

gNFS.CalculateGNFS(N, label28);

}

catch (Exception ex)

{

label28.Text = "Error";

}

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label28.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button2\_Click(object sender, EventArgs e)

{

BigInteger g;

BigInteger A;

BigInteger p;

bool theValuesAreCorrect = true;

shenks = new Shenks();

shenks.CheckingTheInputValues(textBox2.Text, textBox3.Text, textBox4.Text, label15, ref theValuesAreCorrect, out g, out A, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

shenks.CalculateShenks(g, A, p, label15);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label15.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button3\_Click(object sender, EventArgs e)

{

BigInteger a;

BigInteger b;

BigInteger p;

bool theValuesAreCorrect = true;

poligHellman = new PoligHellman();

poligHellman.CheckingTheInputValues(textBox7.Text, textBox6.Text, textBox5.Text, label16, ref theValuesAreCorrect, out a, out b, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

poligHellman.CalculatePoligHellman(a, b, p, label16);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label16.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button6\_Click(object sender, EventArgs e)

{

BigInteger N;

bool theValuesAreCorrect = true;

roPollard = new RoPollard();

roPollard.CheckingTheInputValues(textBox14.Text, textBox22, ref theValuesAreCorrect, out N);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

roPollard.CalculateRoPollard(N, textBox22);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

textBox22.Text += $"\n t = {stopwatch.ElapsedMilliseconds} мс \n{consumedInBytes} байт";

}

private void button7\_Click(object sender, EventArgs e)

{

BigInteger a = mathFunctions.Generate\_a(8);

List<BigInteger> p\_g = mathFunctions.Generate\_p\_g(16);

BigInteger A = mathFunctions.ExponentiationModulo(p\_g[1], a, p\_g[0]);

textBox16.Text = a.ToString();

textBox15.Text = p\_g[0].ToString();

textBox17.Text = p\_g[1].ToString();

textBox18.Text = A.ToString();

}

private void button8\_Click(object sender, EventArgs e)

{

BigInteger g;

BigInteger a;

BigInteger p;

bool theValuesAreCorrect = true;

mathFunctions.CheckingTheInputValues(textBox21.Text, textBox20.Text, textBox19.Text, label35, ref theValuesAreCorrect, out g, out a, out p);

if (!theValuesAreCorrect)

{

return;

}

mathFunctions.ExponentiationModuloWin(g, a, p, label35);

}

private void button4\_Click(object sender, EventArgs e)

{

BigInteger a;

BigInteger b;

BigInteger p;

bool theValuesAreCorrect = true;

adleman = new Adleman();

adleman.CheckingTheInputValues(textBox10.Text, textBox9.Text, textBox8.Text, label20, ref theValuesAreCorrect, out a, out b, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

adleman.CalculateAdleman(a, b, p, label20);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label20.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button5\_Click(object sender, EventArgs e)

{

BigInteger a;

BigInteger b;

BigInteger p;

bool theValuesAreCorrect = true;

cos = new COS();

cos.CheckingTheInputValues(textBox13.Text, textBox12.Text, textBox11.Text, label24, ref theValuesAreCorrect, out a, out b, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

cos.CalculateCOS(a, b, p, label24);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label24.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

async private void button9\_Click(object sender, EventArgs e)

{

BigInteger a;

BigInteger b;

BigInteger p;

bool theValuesAreCorrect = true;

modifiedShenks = new ModifiedShenks();

modifiedShenks.CheckingTheInputValues(textBox2.Text, textBox3.Text, textBox4.Text, label40, ref theValuesAreCorrect, out a, out b, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

await modifiedShenks.CalculateModifiedShenksAsync(a, b, p, label40);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label40.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button10\_Click(object sender, EventArgs e)

{

BigInteger a;

BigInteger b;

BigInteger p;

bool theValuesAreCorrect = true;

modifiedPoligHellman = new ModifiedPoligHellman();

modifiedPoligHellman.CheckingTheInputValues(textBox7.Text, textBox6.Text, textBox5.Text, label41, ref theValuesAreCorrect, out a, out b, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

modifiedPoligHellman.CalculatePoligHellman(a, b, p, label41);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label41.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button11\_Click(object sender, EventArgs e)

{

BigInteger N;

bool theValuesAreCorrect = true;

modifiedRoPollard = new ModifiedRoPollard();

modifiedRoPollard.CheckingTheInputValues(textBox14.Text, textBox23, ref theValuesAreCorrect, out N);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

modifiedRoPollard.CalculateRoPollard(N, textBox23);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

textBox23.Text += $"\n t = {stopwatch.ElapsedMilliseconds} мс \n{consumedInBytes} байт";

}

private void button12\_Click(object sender, EventArgs e)

{

BigInteger a;

BigInteger b;

BigInteger p;

bool theValuesAreCorrect = true;

modifiedAdleman = new ModifiedAdleman();

modifiedAdleman.CheckingTheInputValues(textBox10.Text, textBox9.Text, textBox8.Text, label43, ref theValuesAreCorrect, out a, out b, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

modifiedAdleman.CalculateAdleman(a, b, p, label43);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label43.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button13\_Click(object sender, EventArgs e)

{

BigInteger a;

BigInteger b;

BigInteger p;

bool theValuesAreCorrect = true;

modifiedCOS = new ModifiedCOS();

modifiedCOS.CheckingTheInputValues(textBox13.Text, textBox12.Text, textBox11.Text, label44, ref theValuesAreCorrect, out a, out b, out p);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

modifiedCOS.CalculateCOS(a, b, p, label44);

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label44.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button14\_Click(object sender, EventArgs e)

{

BigInteger N;

bool theValuesAreCorrect = true;

modifiedGNFS = new ModifiedGNFS();

modifiedGNFS.CheckingTheInputValues(textBox1.Text, label45, ref theValuesAreCorrect, out N);

if (!theValuesAreCorrect)

{

return;

}

Stopwatch stopwatch = new Stopwatch();

stopwatch.Start();

long before = GC.GetTotalMemory(false);

try

{

modifiedGNFS.CalculateGNFS(N, label45);

}

catch (Exception ex)

{

label45.Text = "Error";

}

long after = GC.GetTotalMemory(false);

int consumedInBytes = (int)(after - before);

consumedInBytes = consumedInBytes > 0 ? consumedInBytes : -consumedInBytes;

stopwatch.Stop();

label45.Text += $"\nt = {stopwatch.ElapsedMilliseconds} мс\n{consumedInBytes} байт";

}

private void button15\_Click(object sender, EventArgs e)

{

textBox2.Text = textBox17.Text;

textBox3.Text = textBox18.Text;

textBox4.Text = textBox15.Text;

}

private void button16\_Click(object sender, EventArgs e)

{

textBox7.Text = textBox17.Text;

textBox6.Text = textBox18.Text;

textBox5.Text = textBox15.Text;

}

private void button17\_Click(object sender, EventArgs e)

{

int byteCount = 8;

BigInteger generatedNumber = new BigInteger(RandomNumberGenerator.GetBytes(byteCount));

while (generatedNumber % 2 == 0 ||

generatedNumber % 3 == 0 ||

generatedNumber % 5 == 0 ||

generatedNumber % 7 == 0)

{

generatedNumber = new BigInteger(RandomNumberGenerator.GetBytes(byteCount));

}

generatedNumber \*= generatedNumber.Sign;

textBox14.Text = generatedNumber.ToString();

}

private void button18\_Click(object sender, EventArgs e)

{

textBox10.Text = textBox17.Text;

textBox9.Text = textBox18.Text;

textBox8.Text = textBox15.Text;

}

}

}