Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Дискретный логарифм и его применение в криптографии

название темы выпускной квалификационной работы

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента (ки) 2 курса 227 группы

направления 02.04.01 «Математика и компьютерные науки»

код и наименование направления

механико-математического факультета

наименование факультета

Прокудиной Светланы Сергеевны

фамилия, имя, отчество

Научный руководитель

доцент, к.ф.-м.н		Е.В. Сецинская
должность, уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Зав. кафедрой:

к.ф.-м.н., доцент		А.М. Водолазов
должность, уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Саратов 2017 г.

Введение. Криптография это наука изучающая тайнопись и методы ее раскрытия. Криптография считается разделом математики.

Цель магистерской работы изучить различные алгоритмы вычисления дискретного логарифма и произвести на базе полученых знаний вычиления дискретного логарифма.

Задачи магистерской работы:

1. Познакомится с алгоритмами вычисления дискретного логарифма.

2. Решить задачу нахождения дискретного логарифма с помощью этих алгоритмов.

3. Произвести оценку сложности алгоритмов.

Определим задачу дискретного логарифмирования, его проблему и алгоритмы решения существующие на данный момент.

Пусть есть a и b целые числа, а p — простое число

$$a^x \equiv b(mod\ p), \tag{1}$$

в группе $(Z/pZ)^*$. Мы будем предполагать, что порядок $a(mod\ p)$ равен $p-1$. Тогда уравнение разрешимо, и решение x является элементом $Z/(p-1)Z$.

Метод перебора медленный для больших чисел, поэтому применяются наиболее быстрые алгоритмы.

Задача дискретного логарифмирования имеет важные приложения в криптографии. Особенно важен случай $G = GF(q)^*$, где $q = p^l, p$ — простое число, $l \in N$, а также случай, когда G является группой точек эллиптической кривой над конечным полем.

Уже в конце 70х, в 80х вместе с развитием асимметричных шифров и подписей стали появляться все новые и новые алгоритмы с все большой и большой скоростью работы.

К примеру, ρ-алгоритм Полларда для вычисления дискретного логарифма.

Данная магистерская работа состоит из введения, трех разделов, заключения и списка литературы. Первый раздел состоит из двух подразделов. В ней показанны основные системы кодирования с открытым ключем (основные определения информации ее кодирования и методы шифрования информации с открытым ключем). Второй раздел состоит из трех подразделов. Он включает в себя различные методы вычисления дискретного логарифма в простых полях, полях Галуа и в конечных полях. Третий раздел состоит из двух подпунктов и включает в себя различные алгоритмы вычисления дискретного логарифма такие как алгоритм решета числового поля и метод Полларда.

В данной работе решены некоторые примеры с помощью алгоритмов вычисления дискретного логарифма. Даны различные оценки сложности данных алгоритмов.

Основное содержание работы. Идея шифрования с открытым ключом тесно связана с понятием однонаправленной (односторонней) функцией. На качественном уровне оно определяется так. Взаимно однозначное отображение $f : X \to Y$ двух текстов X и Y называется строго однонаправленной, если выполняется следующее условие: существует «эффективный» метод вычисления $f(x)$ для всех $x \in X$, но не существует «эффективного» метода для вычисления из соотношения $y = f(x)$ для всех $y \in f(X)$, где $f(X)$— образ множества X при отображении f.

Криптосистема Мэсси-Омуры для передачи сообщений. Предположим, что для нее решили использовать конечное поле F_q; оно зафиксировано и общеизвестно. Каждый пользователь системы втайне выбирает такое случайное целое w между 0 и $q-1$, что НОД $\{w, q-1\} = 1$ и с помощью алгоритма Евклида вычисляет обратное к нему число $d \equiv w^{-1}(mod\ q-1)$, то есть $dw \equiv 1(mod\ q-1)$. Если Алиса (пользователь A) намерена передать сообщение P Бобу, она сначала посылает ему элемент P^{w_A}. Это послание для Боба бессодержательно, так как он не знает d_A (или w_A, что то же самое) и не может восстановить P. Не пытаясь понять смысл сообщения, Боб возводит его в свою степень w_B и отсылает $P^{w_A w_B}$ обратно Алисе. Третий шаг состоит в том, что Алиса несколько «распутывает» сообщение, возводя его в степень d_A: так как $P^{d_A w_A} = P$, то, по сути дела, она отсылает Бобу P^{w_B}, который теперь может прочитать сообщение, возведя его в степень d_B.

Алгоритм Полига—Хеллмана.

1 шаг. Для каждого простого числа $q, q|p-1$, составляем таблицу чисел

$$r_{q,j} \equiv a^{\frac{j(p-1)}{q}} (mod\ p), j = 0, ..., q-1$$

2 шаг. Для каждого простого q, $q^\alpha|\, p-1$, находим $log_a b(mod\ q^\alpha)$.

Пусть

$$x \equiv log_a b(mod\ q^\alpha) \equiv x_0 + x_1 q + ... + x_{\alpha-1} q^{\alpha-1} (mod\ q^\alpha)$$

где $0 \leqslant x_i \leqslant q-1$. Тогда из (1) следует, что

$$b^{\frac{p-1}{q}} \equiv a^{\frac{x_0(p-1)}{q}} (mod\ p)$$

С помощью таблицы 1 шага находим x_0. Тогда выполнено сравнение

$$(ba^{-x_0})^{\frac{p-1}{q^2}} \equiv a^{\frac{x_i(p-1)}{q}} (mod\ p)$$

По таблице находим x_1, и так далее. Значение x_1, находится из сравнения

$$(ba^{-x_0 - x_1 q - ... - x_i q^{i-1}})^{\frac{p-1}{q^{i+1}}} \equiv a^{\frac{x_i(p-1)}{q}} (mod\ p)$$

3 шаг. Найдя $log_a b(mod\ q_i^{\alpha_i}), i = 1, ..., s$, находим $log_a b(mod\ p-1)$ по китайской теореме об остатках.

Алгоритм Адлемана.

1 этап. Сформировать факторную базу, состоящую из всех простых чисел $q, q \leq B = e^{const\sqrt{logploglogp}}$

2 этап. С помощью некоторого перебора найти натуральные числа r_i такие, что

$$a^{r_i} \equiv \prod_{\substack{q \leq B,\\ q-\text{простое}}} q^{\alpha_{iq}}\, (mod\ p)$$

Отсюда следует, что

$$r_i \equiv \sum_{\substack{q \leq B,\\ q-\text{простое}}} \alpha_{iq} log_a q\, (mod\ p-1) \tag{2.2}$$

3 этап. Набрав достаточно много соотношений (2.2), решить получившуюся систему линейных уравнений относительно неизвестных $log_a q$—дискретных логарифмов элементов факторной базы.

4 этап. С помощью некоторого перебора найти одно значение r, для которого

$$a^r \cdot b \equiv \prod_{q \le B} q^{\beta_q} \cdot p_1 \cdot ... \cdot p_k \, (mod\ p)$$

где $p_1, ..., p_k$ — простые числа «средней» величины, то есть $B < p_i < B_1$, где B_1 — также некоторая субэкспоненииальная граница, $B_1 = e^{const\sqrt{logploglogp}}$

5 этап. С помощью вычислений, аналогичных 2 и 3 этапам алгоритма, найти дискретные логарифмы $log_a p_i$, для фиксированных простых чисел средней величины $p_1, ..., p_k$ из 4 этапа.

6 этап. Определить искомый $log_a b$:

$$log_a b \equiv -r + \sum_{q \le B} \beta_q log_a q + \sum_{i=1}^{k} log_a p_i \, (mod\ p-1)$$

Алгоритм согласования.

1 шаг. Присвоить $H := \left[p^{\frac{1}{2}}\right] + 1$.

2 шаг. Найти $c \equiv a^H \, (mod\ p)$.

3 шаг. Составить таблицу значений $c^u \, (mod\ p)\, , 1 \leqslant u \leqslant H$, и упорядочить ее.

4 шаг. Составить таблицу значений $b \cdot a^v \, (mod\ p)\, , 1 \leqslant v \leqslant H$, и упорядочить ее.

5 шаг. Найти совпавшие элементы из первой и второй таблиц Для них

$$c^u \equiv b \cdot a^v \, (mod\ p)$$

откуда $a^{Hu-v} \equiv b \, (mod\ p)$.

6 шаг. Выдать $x \equiv Hu - v \, (mod\ p-1)$.

Определение 2.1. Пусть $r \in N, r = 2^{\alpha_0} p_1^{\alpha_1} ... p_t^{\alpha_t}$, есть разложение r на простые множители, $2 < p_1 < ... < p_t$. Определим функцию Кармайкла $\lambda(r)$:

$$\lambda(r) = \text{НОК} \left(\varphi_0 \left(2^{\alpha_0}\right), \varphi \left(p_1^{\alpha_1}\right) ... \varphi \left(p_t^{\alpha_t}\right)\right)$$

где φ—функция Эйлера, $\varphi_0(1) = \varphi_0(2) = 1, \varphi_0(4) = 2, \varphi_0(2^{\alpha_0}) = 2^{\alpha_0 - 2}$ при $\alpha_0 \geqslant 3$.

Нетрудно видеть, что при $a \in Z, (a, r) = 1$, выполнено сравнение $a^{\lambda(r)} = 1\,(mod\ r)$.

Дискретный логарифм по состовному модулю(в конечных кольцах).

Определение 2.2. Пусть $r \in Z_{>1}, a \in Z, (a, r) = 1$. Частное Ферма $Q(a, r)$ определяется соотношением

$$Q(a, r) \equiv \frac{a^{\lambda(r) - 1}}{r}\,(mod\ r)$$

здесь $\frac{a^{\lambda(r)-1}}{r}$ обозначает результат деления $a^{\lambda(r)-1}$ на r в кольце Z.

Лемма 2.1. Пусть $a, b \in Z$, $(a, r) = (b, r) = 1$. Тогда

$$Q(ab, r) = Q(a, r) + Q(b, r)\,(mod\ r)$$

Лемма 2.2. Число $R = \frac{r^2}{(\lambda(r), r)}$является периодом $Q(r, x)$.

Теорема 2.1 Пусть p — нечетное простое число, $\alpha \in Z_{\geqslant 2}, m = p^\alpha$. Пусть $g \in Z, g\,(mod\ m)$ —первообразный корень по модулю $m, b \in Z, (b, p) = 1$. Обозначим $x = [logb]_\alpha \in Z/\varphi(p^\alpha)\,Z$ — решение уравнения $g^x \equiv b\,(mod\ m)$. Тогда $[logb]_\alpha$ есть единственное по модулю $\varphi(p^\alpha)$ решение системы уравнений

$$\begin{cases} Q\left(g, p^{\alpha-1}\right) x \equiv Q\left(b, p^{\alpha-1}\right)\left(modp^{\alpha-1}\right) \\ x = [logb]_1\,(mod\ p - 1)\,. \end{cases}$$

где $[logb]_1$ означает решение уравнения $g^y \equiv b\,(mod\ p)$.

Теорема 2.2 Пусть $m = 2^\alpha$, где $\alpha \in Z_{\geqslant 5}$. Пусть $b \in Z, b$ нечетно,

$$b \equiv (-1)^{k_0}\,5^{k_1}\,(mod 2^\alpha)$$

где $k_0 = 0$ при $b \equiv 1\,(mod\ 4)\,, k_0 = 1$ при $b = 3\,(mod\ 4)$ и $0 \leqslant k_1 \leqslant 2^{\alpha-2} - 1$. Положим $[logb]_\alpha = k_1$. Тогда $[logb]_\alpha$ есть единственное по модулю $2^{\alpha-2}$ решение уравнения

$$xQ\left(5, 2^{\alpha-2}\right) \equiv Q\left(b, 2^{\alpha-2}\right)\left(mod\ 2^{\alpha-2}\right)$$

Лемма 2.4. Пусть q —нечетное простое число, $q-1=\prod_{j=1}^{n}p_j^{\alpha_j}$ разложение $q-1$ на простые множители. Пусть $u\in N, a,b\in\left(Z/q^uZ\right)^*, a\not\equiv (mod\ q^u)$. Пусть также g—первообразный корень по модулю q^u. Тогда выполнены следующие утверждения.

а) Если

$$ord\left(a\left(mod\ q^u\right)\right)=q^{u-1-\beta_0}\prod_{j=1}^{n}p_j^{\alpha_j-\beta_j}, \text{где} \beta_j\in Z_{\geqslant 0}$$

то

$$a\equiv g^{q^{\xi_0}\prod_{j=1}^{n}p_j^{\xi_j*l}}\left(mod\ q^u\right)$$

где $0<l<\phi\left(q^u\right)$. При этом, если $u>1$ и $\beta_0<u-1$ или если $u=1$, то $q\nmid l$; если $j>0$ и $\beta_i<\alpha_i$, , то $p_j\nmid l$.

б) Сравнение $a^x\ \equiv\ b\left(mod\ q^u\right)$ разрешимо тогда и только тогда, когда $ord\left(b\left(mod\ q^u\right)\right)$ делит $ord(a\left(mod\ q^u\right))$.

Лемма 2.6.

а) Найдется многочлен $g_1\left(x\right)$ (равный либо $g\left(x\right)$, либо $g\left(x\right)+f\left(x\right)$), такой, что $deg\ g_1\left(x\right)<n$ и $g_1\left(x\right)^{p^n-1}\not\equiv\left(mod\ f^2\right)$.

б) Если $h=h\left(x\right)\in Z/pZ, f\nmid h$, то при всех $j>0$

$$h^{p^j}\left(p^n-1\right)\equiv 1\left(mod\ f^{p^j}\right)$$

в) Если $j\geqslant 1, p^{j-1}<k\leqslant\ p^j$, то порядок ,любого обратимого по умножению элемента кольца R_n делит $p^j\left(p^n-1\right)$, и существует элемент такого порядка.

Лемма 2.7. Пусть $k\ >\ 1$. Тогда $|R_k|\ =\ p^{nk}, |R_k^*|\ =\ p^{n(k-1)}\left(p^n-1\right)$ Далее, при $p^{j-1}\ <\ k\ \leqslant\ p^j$ справедливо разложение R_k^* в прямое произведение циклических групп

$$R_k^*=\left\langle\xi_{k,0}\right\rangle_{p^n-1}\times\left\langle\xi_{k,1}\right\rangle_{p^{l_{k,1}}}\times ...\left\langle\xi_{k,s_k}\right\rangle_{p^{l_{k,s_k}}}$$

где $l_{k,1}+\ldots+l_{k,s_k}=n\left(k-1\right)$ и $j=l_{k,1}\geqslant l_{k,2}...l_{k,s_k}$ В частности, при $1<k\leqslant p,\ \ s_k=n(k-1)$ и

$$R_k^*=\left\langle\xi_{k,0}\right\rangle_{p^n-1}\times\left\langle\xi_{k,1}\right\rangle_p\times ...\left\langle\xi_{k,n(k-1)}\right\rangle_p$$

Теорема 2.5. Пусть $p/2 < k \leqslant p$, эмменты h_1, h_2 группы R_k^* имеют порядок p. Пусть (по лемме 2.7)

$$h_1 \equiv 1 + a(x) f(x) + ... + a_{k-1}(x) f(x)^{k-1} \left(mod\ f^k\right),$$

$$h_2 \equiv 1 + b(x) f(x) + ... + b_{k-1}(x) f(x)^{k-1} \left(mod\ f^k\right).$$

$deg\ a_i, deg\ b_i < n$. Если $b(x) \neq 0$ и уравнение $h_1 = h_2^y$ разрешимо, то $y_1 \equiv \left(a_1(x) b_1(x)^{-1}\right)^p (mod\ f(x))$

Теорема 2.6. Пусть $p/2 < k \leqslant p$. Пусть $h_1, h_2 \in R_k^*$, порядок h_1 равен pd_1, порядок h_2 равен pd_2, и $d_1|d_2$,и $d_2|p^n - 1$,значит $d_1|p^n - 1$. Пусть (по лемме 2.3)

$$h_1^{p^n-1} \equiv 1 + a_1(x) f(x) + ... + a_{k-1}(x) f^{k-1}(x) \left(mod\ f^k\right)$$

$$h_2^{p^n-1} \equiv 1 + b_1(x) f(x) + ... + b_{k-1}(x) f^{k-1}(x) \left(mod\ f^k\right)$$

$deg\ a_i, deg\ b_i < n$ и $b_1(x) \neq 0$,то

а) Предположим, что найдется $y_0 \in Z/pZ$ которого выполнено сравнение $y_0 \equiv \left(a_1 b1^{-1}\right)^p (mod\ f(x))$. Если

$$h_1^{p^n-1} \equiv \left(h_2^{p^n-1}\right)^{y_0}$$

то уравнение $h_1 = h_2^y$ разрешимо

б) Если класс вычетов $(a_1 b_1^{-1p})(mod\ f(x))$ не содержит элемента $y_0 \in Z/pZ$, им он содержит $y_0 \in Z/pZ$, но $h_1^{p^n-1} \neq (h_2^{p_n-1})^{y_0}$ то уравнение $h_1 = h_2^y$ неразрешимо.

Алгоритм решета числового поля Рассмотрим уравнения

$$a^x \equiv b\,(mod\ p) \tag{3.1}$$

где p — простое число; сложность алгоритма составляет эвристически $L_p\left[\frac{1}{3}, 3^{\frac{2}{3}}\right]$ арифметических операций.

Схема алгоритма. 1 этап. На этом этапе мы сводим решение уравнения (3.1) к решению уравнений

$$a^x \equiv s(mod\ p)$$

где s— некоторое конечное множество достаточно малых натуральных чисел. Грубо говоря, мы ищем одно $z \in N$, такое, что

$$a^z \cdot b \equiv \prod_j s_j \,(mod\ p)$$

где s_j— не очень большие простые числа, скажем, $s_j \leqslant L_p\left[\frac{2}{3}, const\right]$. Факторизацию $a^z \cdot b \equiv (mod\ p)$ мы можем проводить методой эллиптических кривых Ленстры. Тогда $s = \{s_j\}\,, log_a b \equiv -z + \sum_j log_a s_j (mod\ p-1)$.

2 этап. С помощью некоторой техники мы выбираем два многочлена $g_1(x), g_2(x) \in Z\,[x]\,, deg\ g_i = n, i = 1, 2$, имеющих общий корень $m(mod\ p)$. Мы обозначаем для $j = 1, 2$:

$\alpha_j \in C$ — фиксированный корень $g_j(x), h_j \in N$ —старший коэффициент $g_j(x), K_j \in Q(\alpha_j), \mathcal{O}_j = Z_{K_j}$— кольцо целых алгебраических чисел поля K_j.

а) $n_i = 2; g_1(x)$ — неприводимый многочлен второй степени; поле K- есть мнимое квадратичное одноклассное поле;

б) $n_2 = 1; g_2(x)$ — линейный многочлен вида $U_x + V, U, V \in Z$;

3 этап. (Выбор факторной базы.) Для $j = 1, 2$, мы находим факторные базы

$$F_j = \{\wp | \wp - \text{простые идеалы } \mathcal{O}_j, Norm\ \wp < B_j\} \cup \{h_j\}$$

Здесь B_j — некоторые постоянные, субэкспоненциально зависящие от p.

4 этап. С помощью некоторого просеивания мы находим множество пар $C = \{(c, d)\} \in Z^2$ такое, что для $i = 1, 2$, идеалы $(h_i(c + d\alpha_i))$ в кольце $\mathcal{O}_j$, гладки по отношению к факторной базе F_j При этом множество C должно быть достаточно велико,$|C| > |F_1| + |F_2|$.

5 этап. Для каждого $s \in S$ мы находим специальные соотношения. Для каждого простого идеала $\wp \in \mathcal{O}_1$, лежащего над s, мы находим пару чисел c, d такую, что идеал $(h_1(c + d\alpha))/\wp_1$ гладок по отношению к F_1 и идеал $(h_2(c + d\alpha_2))$ гладок по отношению к F_2

6 этап. Для каждого большого простого числа q, делящего $p - 1$ (мы считаем, что факторизация $p - 1$ нам известна), делаем следующее.

а) Вычисляем так называемые аддитивные характеры Широкауера (определение см. ниже) от элементов $(h_j(c + d\alpha_j)), j = 1, 2, (c, d) \in C$

б) Находим матрицу A с элементами из поля Z/qZ. Ее столбцы состоят из векторов показателей в разложении $(h_j(c+d\alpha_j))$ на простые идеалы и из значений аддитивных характеров.

в) Путем решения системы линейных уравнений $AX \equiv 0(mod\ q)$ находим элементы $\gamma_i = \mathcal{O}_i, i = 1, 2$, такие, что $\gamma_i = \delta_i^q, \delta_i^q \in \mathcal{O}_i, i = 1, 2$,

г) С помощью кольцевых эндоморфизмов

$$\varphi_j : Z\left[h_j\alpha_j\right] \to Z/pZ, \varphi_j\left(h_j\alpha_j\right) \equiv h_j m\left(mod\ p\right), j = 1, 2$$

мы переходим от q-х степеней в кольцах $\mathcal{O}_j$, к целым числам и находим $k, l \in Z$ такие, что $a^k b^l \equiv d^p(mod\ p)$. Из этого следует, что $k + lx \equiv 0(mod\, q)$, где $x(mod\, p{-}1)$ — решение (3.1). Отсюда мы находим значение $x(mod\ q)$.

7 этап. На 6 этапе мы нашли значение $x(mod\ q)$ для больших простых делителей q числа $p-1$. Предположим, что $p-1$ не делится на квадрат большого простого числа. Тогда недостающие значения $x(mod\ q^{\alpha_q})$, где q — небольшие простые числа $q^{\alpha_q} | \, p-1$, мы найдем с помощью алгоритма Полига— Хеллмана. Затем с помощью китайской теоремы об остатках мы найдем искомое значение $x(mod\ p-1)$.

ρ метод Поларда Мы хотим решить уравнение $a^x \equiv b\,(mod\ p)$. Для этого рассмотрим три числовые последовательности

$$\left\{u_i\right\}, \left\{v_i\right\}, \left\{z_i\right\}, i = 0, 1, 2, 3, ...$$

определенные следующим образом:

$$u_0 = v_0 = 0, z_0 = 1$$

$$u_{i+1} = \begin{cases} u_i + 1(mod\ p-1), \text{если } 0 < z_i < \frac{p}{3}, \\ 2u_i(mod\ p-1), \text{если } \frac{p}{3} < z_i < \frac{2}{3}p \\ u_i(mod\ p-1), \text{если } \frac{2}{3}pz_i < p. \end{cases}$$

$$v_{i+1} = \begin{cases} v_i + 1(mod\ p-1), \text{если } 0 < z_i < \frac{p}{3}, \\ 2v_i(mod\ p-1), \text{если } \frac{p}{3} < z_i < \frac{2}{3}p \\ v_i(mod\ p-1), \text{если } \frac{2}{3}pz_i < p. \end{cases}$$

$$z_{i+1} \equiv b^{u_i+1}a^{v_i+1}(mod\ p-1)$$

Здесь под $c(mod\ p)$ мы понимаем наименьший неотрицательный вычет в данном классе вычетов.

Далее мы рассматриваем наборы $(z_i, u_i, v_i, z_{2i}, u_{2i}, v_{2i}), i = 1, 2, 3, ...,$ и ищем номер i, для которого $z_i = z_{2i}$. Из последнего равенства следует, что

$$b^{u_{2i}-u_i} \equiv a^{v_{2i}-v_i}(mod\ p)$$

Если окажется, что $(u_{2i} - u_i, p-1) = 1$, то при $l \in Z, l(u_{2i} - u_i) \equiv 1(mod\ p)$ мы получим

$$b \equiv a^{l(v_i - v_{2i})}(mod\ p)$$

откуда искомый x равен $log_a b \equiv l(v_i - v_{2i}) \equiv 1(mod\ p-1)$. Эвристическая оценка сложности метода составляет $O(p^{\frac{1}{2}})$ операций.

Заключение В ходе выполнения дипломной работы были изучены материалы по теме «Дискретный логарифм и его применение в криптографии» и решена намеченная цель – изучение алгоритмов вычисления дискретного логарифма и вычисление с помощью этих алгоритмов дискретного логарифма. Для достижения этой цели, мной в ходе выполнения работы были решены следующие задачи:

1. Определены алгоритмы для вычисления дискретного логарифма, максимально полно покрывающий тему «Дискретный логарифм и его применение в криптографии»

2. Подробно разобраны примеры вычисления дискретного логарифма по выбранным алгоритмам.

3. Получены оценки сложности различных теоретико-числовых алгоритмов в задаче дискретного логарифмирования.