МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

**«Челябинский государственный университет»**

**(ФГБОУ ВО «ЧелГУ»)**

Математический факультет

Кафедра компьютерной безопасности и прикладной алгебры

**КУРСОВАЯ РАБОТА**

**Криптографические алгоритмы на эллиптических кривых**

Выполнил студент:

**Гутров Роман Михайлович**

группы МК-301

очной формы обучения

специальности

10.05.01 Компьютерная безопасность

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

«\_\_\_» июля 2023 г.

Научный руководитель:

Шалагинов Леонид Викторович

Должность: доцент

Ученая степень: доктор.физ.-мат. наук

Ученое звание: доцент

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

«\_\_\_» июля 2023 г.

Челябинск, 2023

**Оглавление**

[Введение 3](#_Toc140436736)

[1.Базовые определения 3](#_Toc140436737)

[2. Основы эллиптической криптографии. 4](#_Toc140436738)

[2.1 Эллиптическая кривая. 4](#_Toc140436739)

[2.2 Операции на эллиптической кривой 7](#_Toc140436740)

[3. Реализация класса эллиптической кривой 10](#_Toc140436741)

[4. Алгоритм ECDH (Elliptic Curve Diffie-Hellman) 10](#_Toc140436742)

[4.1 Схема работы 11](#_Toc140436743)

[4.2 Реализация 11](#_Toc140436744)

[4.2.1 Метод ECDH.gen\_main\_parameters() 11](#_Toc140436745)

[4.2.2 Метод ECDH. gen\_shared\_secret(POINT ) 12](#_Toc140436746)

[4.2.3 Метод ECDH. set\_main\_parameters(publicParameter pp) 12](#_Toc140436747)

[4.3 Применение и актуальность. 12](#_Toc140436748)

[5. Алгоритм Ленстры факторизации числа на эллиптической кривой 13](#_Toc140436749)

[5.1 Идея работы алгоритма 14](#_Toc140436750)

[5.2 Теоретическое обоснование 15](#_Toc140436751)

[5.3 Реализация алгоритма 16](#_Toc140436752)

[5.4 Способы ускорения и актуальность алгоритма. 17](#_Toc140436753)

[6.Криптография на эллиптических кривых. 19](#_Toc140436754)

[Заключение. 20](#_Toc140436755)

[Список литературы 22](#_Toc140436756)

[Приложение 23](#_Toc140436757)

# **Введение**

В современном информационном обществе защита данных и обеспечение безопасности являются важнейшими задачами. Криптография играет ключевую роль в обеспечении конфиденциальности, аутентификации и целостности информации. Среди различных методов криптографии особое внимание привлекают криптографические алгоритмы на эллиптических кривых (ЭК).

В данной курсовой работе будут исследованы и реализованы криптографические алгоритмы на основе эллиптических кривых. Будет рассмотрено устройство эллиптических кривых и операции с точками на них, а также применение двух важных алгоритмов: ECDH (Elliptic Curve Diffie-Hellman) и алгоритм факторизации, предложенный Х.В. Ленстрой.

В рамках исследования разберем устройство эллиптических кривых, включая их математическое определение, параметры и основные свойства. Углубимся в изучение арифметических операций, применяемых с точками на эллиптических кривых, таких как сложение, удвоение и умножение на скаляр. А также проведем реализацию этих операций и алгоритмов, что поможет нам более глубоко понять их принципы и возможности применения в криптографии.

Целью данной работы является изучение эллиптических кривых применяемых в криптографии, их свойств, операций с точками на них, а так же реализация протокола ECDH и алгоритма Ленстры.

**Основная часть**

# **1.Базовые определения**

Эллипти́ческая крива́я над полем K — неособая кубическая кривая на проективной плоскости над алгебраическим замыканием поля K, задаваемая уравнением 3-й степени с коэффициентами из поля K и «точкой на бесконечности».   
 Кривая Ленстры – кривая вида , называемая так же нормальной формой Вейерштрасса.

Точка на бесконечности – специальная точка, которая добавляется к множеству точек на эллиптической кривой и является ее нейтральным элементом в операции сложения точек. Обозначается как .

Порядок точки – число, определяющее сколько раз данная точка может быть сложена сама с собой до получения точки на бесконечности.

Порядок кривой (порядок группы кривой) – число, обозначающее количество точек, содержащихся на эллиптической кривой вместе с точкой на бесконечности.

B-гладкая точка – такая точка определенная на эллиптической кривой, порядок которой может быть разложен на простые множители, не превышающие B.

Редукция по простому делителю – один из шагов алгоритмов факторизации. Используется для проверки, делится ли исследуемое число на простой делитель

Сингулярная кривая – эллиптическая кривая, которая имеет особенности в одной или нескольких точках, т.е. имеет точки возврата или самопересечения.

Несингулярная (гладкая) кривая – кривая не имеющая особых точек.

Симметричное шифрование – способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации.

# **2. Основы эллиптической криптографии.**

## **2.1 Эллиптическая кривая.**

Эллиптическая кривая – геометрический объект, определяемый в подходящих аффинных координатах уравнением вида:   
.   
Но в данной работе будет рассматриваться только кривая в нормальной форме Вейерштрасса вида , над конечным полем , поскольку в исследуемых алгоритмах используется именно такая форма кривой.

Кривую называют сингулярной, если на ней существует хотя бы одна особая точка, в которой одновременно ∂f/∂x = 0 и ∂f/∂y = 0. В противном случае кривая называется несингулярной. Такие кривые являются гладкими (рисунок 1.), т.е. не имеют точек возврата и самопересечений, в любой их точке можно провести касательную. Именно эти кривые и представляют интерес для криптографии.

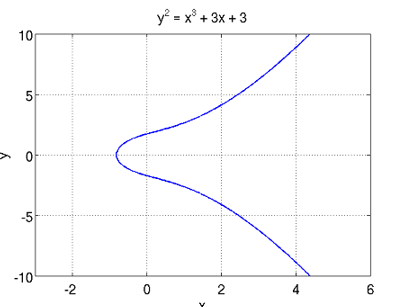


Рисунок 1. Гладкая эллиптическая кривая.

Из уравнения кривой можно вывести следующее равенство: , откуда следует симметричность относительно оси абсцисс, где точки пересечения – это корни кубического уравнения . Дискриминантом этого равенства является . При этом:

* если , то уравнение имеет три разных действительных корня α, β и γ. Типичный график – кривая из двух частей (Рисунок 2.);
* если , то уравнение имеет действительные корни α, β, β, два из которых одинаковы. В этом случае точка (β;0) – особая, а кривая сингулярная (Рисунок 3);
* если , то уравнение имеет один действительный корень α и два комплексных (Рисунок 4).

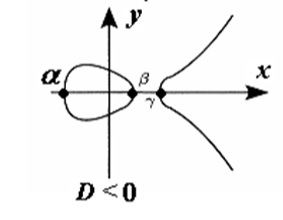


Рисунок 2.

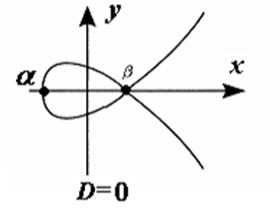


Рисунок 3.

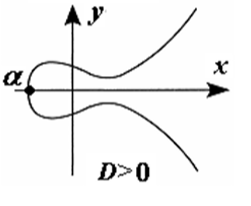


Рисунок 4.

Таким образом, если характеристика поля не равна двум и не равна трем, то кривая будет не сингулярной при условии что ее дискриминант не равен нулю. Отсюда вытекает следующее неравенство:

*.*

## **2.2 Операции на эллиптической кривой**

Все арифметические операции в эллиптической криптографии производятся над точками, определенными на этой кривой. Основной операцией является сложение.

Симметрия кривой относительно оси Ox дает наглядное определение обратной точки. А именно: обратной точкой для точки на эллиптической кривой называют точку

Замечательным свойством не сингулярных кривых является то, что любая прямая, проходящая через две различные точки кривой пересекает кривую в единственной точке. Кроме того, касательная к эллиптической кривой в любой точке (кроме точек перегиба) пересекает ее еще в одной точке. Такие особенности позволяют задать групповую операцию, называемую сложением точек эллиптической кривой. Суммой двух точек P и Q называется точка R = P + Q, обратная третьей точке пересечения эллиптической кривой и прямой, проходящей через точки P и Q (Рисунок 5).

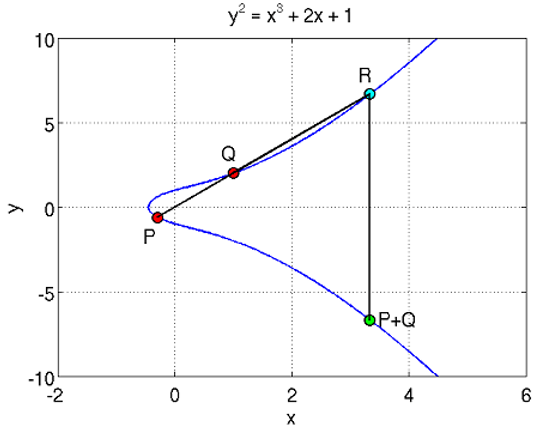


Рисунок 5. Сложение точек P и Q.

Если суммируемые точки P и Q совпадают, то P + Q = P + P = R, что равносильно удвоению точки R=2P. При P=Q секущая PQ превращается в касательную к кривой и геометрически удвоенная точка 2P – это точка, обратная к точке пересечения этой касательной и эллиптической кривой.

Тогда координаты точки R = P + Q = (x3, y3), можно найти выразив их через координаты точек P(x1, y1) и Q(x2, y2). При этом точки P и Q могут быть различными или совпадающими. В соответствии с этим имеем два случая:

1. . Запишем уравнение прямой PQ. Угловой коэффициент прямой PQ равен: .
2. При , . Угловой коэффициент прямой равен:

Данные формулы справедливы для всех полей, в том числе конечных, кроме полей характеристики 2 и 3. В последнем случае, приведение по модулю 2 или 3 приведет к.

Итак, чтобы построить группу точек эллиптической кривой, выберем в качестве нейтрального элемента группы точку, для которой положим: Тогда прямая, проходящая через точки P и -P, перпендикулярна к оси абсцисс и поэтому можно принять, что третья точка пересечения кривой уходит в бесконечность вдоль оси ординат. Поэтому точку O называют точкой на бесконечности (бесконечно удаленной точкой) кривой.

Согласно теореме Анри Пуанкаре, множество точек эллиптической кривой вместе с введенной точкой на бесконечности образует коммутативную группу относительно операции сложения точек: для этого есть все необходимые свойства – замкнутость, коммутативность, ассоциативность, наличие обратного элемента и нейтральный элемент.

Следовательно, множество точек, определенных на эллиптической кривой образуют группу по сложению. К группе точек также относится точка .

Таким образом мы можем определить группу для эллиптических кривых, где:

* элементы группы - это точки кривой;
* единичный элемент – это точка на бесконечности;
* обратная величина произвольной точки – это точка, симметричная относительно оси абсцисс;
* сложение задается правилом: лежащих на одной прямой. Откуда следует ассоциативность и коммутативность операции сложения.

Из вышеизложенных операций сложения и удвоения точки, а так же из того, что множество точек образует группу следует операция умножения точки на скаляр(число) в группе точек. Умножение точки на число - это сложение точки самой с собой раз.

В ходе умножения точки на порядок группы можно заметить, что некоторый момент сложения получается точка на бесконечности. Коэффициент полученный при -ом шаге сложения точки при умножении на исходный скаляр является порядком точки. Т.е. порядок точки – некоторое число при умножении на которое получается точка на бесконечности.

# **3. Реализация класса эллиптической кривой**

Поскольку реализация алгоритма Ленстры и прокола ECDH требует работы с эллиптической кривой, реализован класс “ELLEPTIC\_CURVE”. Этот класс представляет собой абстракцию, моделирующую математическое понятие эллиптической кривой. Класс содержит следующие поля:

* коэффициенты кривой;
* размер группы;
* базовая точка;
* порядок кривой и порядок базовой точки.

А также следующие методы:

* сложение двух точек методом удвоения и сложения;
* умножение точки на скаляр;
* проверка, принадлежит ли точка данной эллиптической кривой;
* нахождение всех точек эллиптической кривой;
* нахождение порядка заданной точки;
* генерация случайной базовой точки.

Класс полностью поддерживает действительные значения произвольной длины, ограничиваясь лишь размером постоянной памяти вычислительной машины.

# **4. Алгоритм ECDH (Elliptic Curve Diffie-Hellman)**

Протокол Ди́ффи-Хе́ллмана на эллиптических кривых (Elliptic curve Diffie–Hellman, ECDH) — криптографический протокол, позволяющий двум сторонам, имеющим пары открытый/закрытый ключ на эллиптических кривых, получить общий секретный ключ, используя незащищённый от прослушивания канал связи. Этот секретный ключ может быть использован как для шифрования дальнейшего обмена, так и для формирования нового ключа, который затем может использоваться для последующего обмена информацией с помощью алгоритмов симметричного шифрования.

## **4.1 Схема работы**

Пусть существуют два абонента: Алиса и Боб. Предположим, что Алиса хочет создать общий с Бобом секретный ключ для некоторого протокола симметричного шифрования, чтобы в дальнейшем шифровать передаваемый и дешифровать получаемый трафик. Но при этом канал связи между Бобом и Алисой может быть прослушан злоумышленником. Изначально у обоих абонентов должен быть согласованный набор публичных параметров необходимых для работы протокола. Каждая сторона генерирует пару закрытый ключ-открытый ключ. Закрытым ключом является большое число в диапазоне [1, n-1], где n – порядок базовой точки определенной на кривой. Открытый ключ – точка на эллиптической кривой получаемая умножением закрытого ключа на базовую точку . Таким образом, Алиса получает пару , Боб получает пару . Далее, Алиса вычисляет точку , Боб вычисляет точку . В итоге у Боба и Алисы получается один секретный ключ (x координата получившейся точки S), который затем дополнительно может быть хеширован.

Вычисленные абонентами ключи будут равны, т.к. . Алиса (Боб) сообщает только свой открытый ключ, следовательно, никто кроме нее не сможет вычислить закрытый ключ, кроме участника способного решить задачу дискретного логарифмирования на эллиптической кривой.

## **4.2 Реализация**

### **4.2.1 Метод ECDH.gen\_main\_parameters()**

На данном этапе генерируются:

* случайные коэффициенты “a” и “b” эллиптической кривой в интервале [1, n-1]. Где n – размерность группы кривой;
* случайная базовая точка , а так же вычисляется ее порядок;
* пара секретный ключ-публичный ключ ;

После чего заполняется и возвращается объект вспомогательной структуры “publicParameter”, которую можно передать абоненту, с целью синхронизировать параметры алгоритма.

### **4.2.2 Метод ECDH. gen\_shared\_secret(POINT )**

Принимает на вход публичный ключ второй стороны и на основе него, формирует общий секрет абонентов, путем умножения собственного секретного ключа абонента на точку .

### **4.2.3 Метод ECDH. set\_main\_parameters(publicParameter pp)**

Позволяет задать набор основных параметров, полученных от второй стороны, тем самым согласовав работу алгоритма у обоих абонентов.

После вызова соответствующих методов оба абонента имеют общий секрет, который может служить в качестве ключа симметричной криптографии.

## **4.3 Применение и актуальность.**

Одним из основных применений протокола ECDH является обеспечение конфиденциальности в криптографии. Он используется для безопасного обмена ключами между участниками, что позволяет им обмениваться зашифрованными сообщениями и обеспечивать конфиденциальность информации. Протокол ECDH обладает высоким уровнем безопасности благодаря использованию сложных математических проблем, связанных с дискретным логарифмированием на эллиптических кривых.

В контексте информационной безопасности, протокол ECDH находит широкое применение в сфере шифрования данных, аутентификации и установления защищенных каналов связи. Он обеспечивает защиту от атак, основанных на вычислительной сложности, таких как атаки на основе дискретного логарифмирования или факторизации чисел.

Протокол ECDH также актуален в контексте мобильных и интернет-приложений. Использование эллиптических кривых позволяет сократить размер ключей и уменьшить вычислительную нагрузку, что особенно важно для ограниченных устройств с ограниченными вычислительными ресурсами, таких как мобильные устройства.

Благодаря своей эффективности и безопасности, протокол ECDH нашел применение в различных протоколах и стандартах, включая TLS/SSL (Transport Layer Security/Secure Sockets Layer), SSH (Secure Shell) и другие. Он также является ключевым компонентом в криптографических системах, таких как цифровые подписи, обмен ключами и аутентификация.

В свете постоянного развития криптографических атак и роста вычислительной мощности, протокол ECDH остается актуальным и востребованным, так как он предлагает безопасный и эффективный способ установления общего секретного ключа.

# **5. Алгоритм Ленстры факторизации числа на эллиптической кривой**

Алгоритм Ленстры - это алгоритм факторизации чисел, основанный на свойствах эллиптических кривых. Он был разработан в 1987 году Хендриком Ленстрой и составляет важную часть области криптографии на эллиптических кривых.

Он используется для разложения целых чисел на простые множители и является одним из эффективных методов факторизации. Основан на использовании свойств групп точек на эллиптической кривой.

Алгоритм Ленстры имеет широкий спектр применений в криптографии и информационной безопасности. Он может быть использован для факторизации чисел в криптографических протоколах, что позволяет атакующим сторонам получить секретные ключи или нарушить безопасность системы. Поэтому разработка и использование сильных криптографических алгоритмов на основе эллиптических кривых, устойчивых к атакам алгоритма Ленстры, является важной задачей в области информационной безопасности.

## **5.1 Идея работы алгоритма**

Пусть уравнение взятое по модулю n задет эллиптическую кривую Если числа и – два простых делителя числа n, то вышеупомянутое уравнение будет верно и при взятии по модулю p или по модулю . То есть имеем две эллиптические кривые , которые задают, соответственно, две кривые, меньшие, чем . Заметим, что также являются группами с заданной операцией сложения. Пусть они содержат *Np* и *Nq* элементов, соответственно, тогда если:

1. *–* любая точка на исходной кривой
2. *–* положительные числа, такие что:
3. *–* минимальное из

То по теореме Лагранжа верно, что

1. – делитель *Np*

Для кривой утверждения аналогичны.

Порядок группы точек, лежащих на эллиптической кривой E  |�| над Z*p*, согласно теореме Хассе ограничен:

Для случайно выбранной кривой порядки *Np* и *Nq* являются случайными числами, ограниченными по теореме Хассе. Маловероятно, что большинство простых делителей *Np* и *Nq* совпадают, и вероятно, что при вычислении  встретится некоторый  ��=∞по модулю , но не по модулю , или наоборот. Если это так, то  не существует на исходной кривой, а в вычислениях было найдено такое *v*, что либо НОД (*v*, *p*) = *p*, либо НОД (*v*, *q*) = *q*, но не одновременно. Тогда НОД (*v*, *n*) является нетривиальным делителем числа *n*.

## **5.2 Теоретическое обоснование**

Пусть дано составное нечетное не делящееся на 3 число , и нам нужно найти его нетривиальный делитель .

**I Этап.** Сгенерируем случайную эллиптическую конфигурацию и базовую точку на ней.

Попытаемся с помощью пары разложить способом описанным во втором этапе. Если попытка окажется неудачной, выберем случайно и независимо другую пару и будем продолжать до тех пор, пока не найдем искомый нетривиальный делитель . Если вероятность неудачи при выборе одной пары равна , то вероятность того, что последовательностей выбранных пар окажутся неудачными (т.е. не позволят разложить на множители) равна , т.е. очень мала для больших . Таким образом, с высокой долей вероятности мы разложим за приемлемое число шагов.

**II Этап.** Сначала выберем и вычислим целое число , где - множество всех простых чисел не превосходящих ( – наибольшая степень числа такая, что ). Выбрав пару , пытаемся вычислить . Если в процессе вычислений для некоторых точки определены, а точка не определена, то существует простой делитель .

Пусть в процессе вычислений для некоторых точки определены, а точка . Тогда , т.е. . В этом случае при редукции по любому простому делителю получаем, что порядок точки в группе делит . В этом случае нетривиальный делитель числа найти не удается и необходимо вернуться к первому этапу.

Наконец, пусть в процессе вычислений точка найдена и оказалось, что . В этом случае при редукции по любому простому делителю по лемме 1 получаем условие , т.е. порядок точки в группе не делит В этом случае так же не удается найти нетривиальный делитель.

Итак, если для некоторого простого делителя порядок точки в группе является -гладким, то появляется возможность найти нетривиальный делитель числа .

## **5.3 Реализация алгоритма**

Дано: нечетное, не делящееся на 3 составное число

Выход: нетривиальный делитель числа.

Шаг 1. (Выбор кривой и базовой точки).

Выбираем случайным образом тройку и вычисляем .

Шаг 2. Вычисляем . Если , то найден нетривиальный делитель . Если , то переходим на шаг 1. Если , то задаем координаты базовой точки . Задаем значение переменной .

Шаг 3. В цикле по вычисляем коэффициент . Пользуясь операцией сложения точек на кривой, вычисляем точку . Если в результате прохода по циклу все точки определены и , то переходим на шаг 1.

Если в процессе вычисления требуется сложить точки , и при этом , то переходим на шаг 1.

Если в процессе вычисления требуется сложить точки , и при этом не определена, то переходим на шаг 4.

Шаг 4. Если , то вычислить . Если при этом , то найден нетривиальный делитель . Если , то перейти на шаг 1.

Если , то вычислить . Если при этом , то найден нетривиальный делитель . Если , то перейти на шаг 1.

Если же , то вычислить . Если при этом , то найден нетривиальный делитель . Если , то перейти на шаг 1.

## **5.4 Способы ускорения и актуальность алгоритма.**

Исходя из вышеизложенного, можно сделать вывод, что алгоритм Ленстры является вероятностным. Поскольку его эффективность полностью зависит от того, насколько удачно выбраны параметры эллиптической кривой и коэффициент B верхней границы. Так же, время факторизации числа зависит от размера делителей факторизуемого числа. Так, например, попытка факторизовать ключ протокола RSA, длиной 2048 бит, который состоит из двух больших простых множителей, займет неразумное время для алгоритма Ленстры, поскольку длина обоих множителей будет равна примерно тысячи бит. В связи с этим, было реализовано два метода направленных на уменьшение времени работы алгоритма.

Поскольку в наибольшей степени время работы зависит от удачно выбранной кривой, первое очевидное решение – запускать несколько экземпляров алгоритма с одним и тем же входным числом. Этот метод позволил ускорить время факторизации, в среднем, на 70%(при использовании 5 потоков) (Рисунок 6).

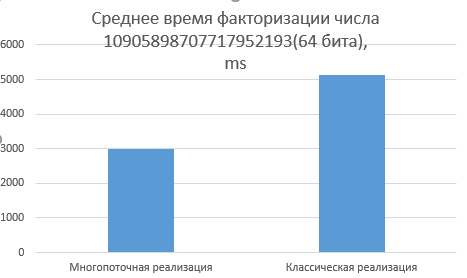


Рисунок 6. Среднее время факторизации классического алгоритма и его многопоточной реализации.

Поскольку время факторизации так же зависит от того, насколько быстро в цикле будет получена неопределенная точка , еще один способ ускорить работу алгоритма - разбить промежуток , на n равных отрезков. Далее, начиная с 3 шага, необходимо запустить цикл на одном из отрезков, в каждом из n потоков. Такой подход позволяет ускорить время работы алгоритма, в среднем на 45%(при использовании 5 потоков) (Рисунок 7).

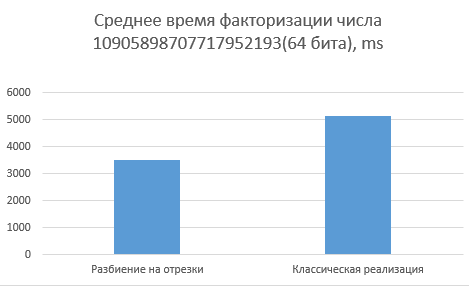


Рисунок 7. Среднее время факторизации классического алгоритма и его модернизированного варианта.

Стоит отметить, что предложенные улучшения имеют наибольший смысл в случае, если множители исходного числа имеют относительно большой размер (от 30 бит). В остальных же случаях скорость вычисления будет либо близка к классической реализации, либо меньше ввиду накладных расходов из-за работы с потоками.

Применение и актуальность алгоритма Ленстры факторизации на эллиптических кривых охватывает различные аспекты криптографии и информационной безопасности. Он остается актуальным в контексте повышения вычислительной мощности и появления новых методов оптимизации, которые позволяют решать более сложные задачи факторизации. На сегодняшний день алгоритм Ленстры является третьим по скорости факторизации чисел, его применение может иметь практическое значение при работе с криптографическими протоколами и системами, помогая оценить их уровень безопасности. Также, его применение может повысить скорость факторизации чисел, особенно в случае наличия специальных свойств числа, таких как небольшие множители. В свете постоянного развития вычислительной техники, он остается актуальным инструментом для факторизации чисел.

# **6.Криптография на эллиптических кривых.**

Криптография на эллиптических кривых является одной из наиболее эффективных и широко применяемых областей криптографии. Она основана на математических свойствах эллиптических кривых и предлагает множество протоколов и алгоритмов для обеспечения безопасности и конфиденциальности информации. В последние десятилетия она получила значительное внимание и широкое применение в различных криптографических протоколах и системах. На сегодняшний день криптография на эллиптических кривых используется для обмена секретными ключами по незащищенному каналу, получения цифровой подписи, шифрования данных, факторизации чисел.

Например, для получения цифровой подписи используется протокол ECDSA. Он обеспечивает возможность создания и проверки цифровых подписей, используя эллиптические кривые. Преимущества ECDSA включают высокую стойкость криптографии, эффективность и компактность подписей. Он широко применяется в системах аутентификации, цифровых сертификатах и обеспечении целостности данных.

Несмотря на все явные преимущества эллиптической криптографии, вроде меньшего размера секретного ключа, и высокой надежности, она имеет и некоторые проблемы. Одной из ключевых проблем является задача дискретного логарифмирования. Эта задача заключается в нахождении числа k, в выражении , где - базовая точка на эллиптической кривой, а - заданная точка на этой кривой. Рассмотрим задачу на примере конечной мультипликативной абелевой группы . Пусть задано уравнение . Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа , удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы. Это сразу даёт грубую оценку сложности алгоритма поиска решений сверху — алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы. Однако такой алгоритм крайне неэффективен и не позволит найти решение для группы с достаточно большим порядком, за разумное время. Существует большое количество алгоритмов для решения задачи дискретного логарифмирования, но на сегодняшний день нет известных эффективных алгоритмов для решения этой задачи за полиномиальное время. Таким образом для больших чисел и простых полей решение этой задачи может потребовать значительных вычислительных ресурсов и времени. В то время как в классической криптографии на основе модульной арифметики решение задачи дискретного логарифмирования является сложной задачей, на эллиптических кривых она оказывается существенно более трудоемкой. Благодаря этому свойству, эллиптическая криптография обеспечивает высокий уровень безопасности при использовании более коротких ключей.

# **Заключение.**

В ходе выполнения данной работы были изучены и реализованы два алгоритма: алгоритм Ленстры для факторизации чисел на эллиптических кривых и алгоритм эллиптического криптографического обмена ключами (ECDH) для установления общего секретного ключа.

Были исследованы эллиптические кривые, их параметры, математическое определение и свойства, а также изучены и реализованы арифметические операции на точках эллиптических кривых, включая сложение, удвоение и умножение на скаляр, что позволило более глубоко понять основы эллиптической криптографии.

Алгоритм Ленстры, основанный на методе факторизации чисел на эллиптических кривых, имеет свою актуальность в криптографии и информационной безопасности. Он предлагает эффективный способ разложения больших целых чисел на простые множители, что имеет важное значение для атак на криптографические системы, основанные на сложности факторизации чисел.

Алгоритм ECDH, основанный на вычислениях на эллиптических кривых, применяется для установления общего секретного ключа между двумя или более сторонами. Этот протокол обладает высокой стойкостью криптографии и эффективностью вычислений, что делает его важным инструментом для обеспечения безопасности обмена ключами.

Криптография на эллиптических кривых имеет ряд преимуществ, включая высокую стойкость криптографии при использовании коротких ключей, компактность и эффективность вычислений. Однако, она также имеет свои сложности и требует математической экспертизы для разработки и применения протоколов.

Использование криптографии на эллиптических кривых находит широкое применение в различных областях, включая защиту данных, аутентификацию, электронную коммерцию, мобильные приложения и другие. Она предлагает эффективные и надежные методы обеспечения безопасности информации.

В целом, криптография на эллиптических кривых является важной и перспективной областью в современной криптографии. Реализация алгоритмов Ленстры и ECDH, изучение эллиптических кривых и операций на них позволило лучше понять и применить принципы и методы этой области, что в дальнейшем может быть реализовано в проектах и научно-исследовательских работах на тему реализации безопасности, целостности и конфиденциальности информации.

# **Список литературы**

[1] Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии : монография / О. Н. Василенко. — 2-е изд., доп. — Москва : МЦНМО, 2006. — 336 с. — ISBN 5-94057-103-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/9303 (дата обращения: 16.07.2023). — Режим доступа: для авториз. пользователей.

[2] Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 396 с. — ISBN 978-5-507-45348-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/265178 (дата обращения: 16.07.2023). — Режим доступа: для авториз. пользователей.

[3] Эллиптическая криптография [Электронный ресурс]: Википедия. Свободная энциклопедия. - Режим доступа: [https://ru.wikipedia.org/elleptic\_crypt](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%BB%D0%B8%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F#%D0%A0%D0%B5%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F)

[4] ECDH [Электронный ресурс]: Википедия. Свободная энциклопедия. - Режим доступа: [https://ru.wikipedia.org/wiki/ECDH](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0_%D0%BD%D0%B0_%D1%8D%D0%BB%D0%BB%D0%B8%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%85_%D0%BA%D1%80%D0%B8%D0%B2%D1%8B%D1%85)

[5] Факторизация с помощью эллиптических кривых [Электронный ресурс]: Википедия. Свободная энциклопедия. - Режим доступа: [https://ru.wikipedia.org/wiki/lenstra](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%81_%D0%BF%D0%BE%D0%BC%D0%BE%D1%89%D1%8C%D1%8E_%D1%8D%D0%BB%D0%BB%D0%B8%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%85_%D0%BA%D1%80%D0%B8%D0%B2%D1%8B%D1%85)

# **Приложение**

Исходный код: [github](https://github.com/OrientPlus/COURSE_PAPER/tree/master/LENSTRA/lenstra).