Министерство образования и науки Российской Федерации

Сибирский государственный аэрокосмический университет

имени академика М. Ф. Решетнева

О. Н. Жданов

В. А. Чалкин

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

*Утверждено редакционно-издательским советом университета в качестве учебного пособия для студентов и магистрантов, обучающихся по специальностям 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» и 090106 «Информационная безопасность телекоммуникационных систем» очной формы обучения*

Красноярск 2011

УДК

ББК

Ж 42

Рецензенты:

кандидат физико-математических наук, доцент Н. А. Бушуева

(Сибирский федеральный университет);

доктор физико-математических наук, профессор А. М. Попов

(Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнёва)

Жданов, О. Н.

Ж 42 Эллиптические кривые и их применение в криптографии: учеб. Пособие / О. Н. Жданов, В. А. Чалкин; Сиб. гос. аэрокосмич. ун-т.-Красноярск, 2011.-

Пособие посвящено применению эллиптических кривых в криптографии. Рассматриваются: ключевой обмен, шифрование, алгоритм цифровой подписи (ЭЦП) по действующему в настоящее время стандарту Российской Федерации. Изложение иллюстрируется примерами, приводятся упражнения для самопроверки. Пособие содержит также сборник индивидуальных заданий для обучающихся . Для полноты изложения и для удобства читателей в Приложении даны выдержки из действующего стандарта ЭЦП и закона о цифровой подписи в РФ.

Для студентов и магистрантов, обучающихся по специальностям 090105 и 090106.

УДК

ББК

© Сибирский государственный аэрокосмический университет

имени академика М. Ф. Решетнева

©Жданов О. Н., Чалкин В. А., 2011

**Оглавление**

**Ведение**

**Глава 1. Алгебраические кривые**

§ 1. Алгебраические кривые и эллиптические кривые

§ 2. Группа точек эллиптической кривой

§ 3. Применение эллиптических кривых в задаче факторизации чисел.

**Глава 2. Криптосистемы на эллиптических кривых**

§1. Вспомогательные сведения

§ 2. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой

§ 3. Алгоритм цифровой подписи, основанный

на группе точек эллиптической кривой

**Глава 3. Аспекты практической реализации криптографических алгоритмов на эллиптических кривых**

§1. Эффективная реализация элементарных операций.

§2. Определение количества точек на кривой.

§3. Использование стандартных кривых.

**Индивидуальные задания по теме «применение эллиптических кривых в криптографии»**

**Темы лабораторных работ**

**Библиографический список**

**Приложения**

Приложение 1.Стандарт электронной цифровой подписи

Приложение 2.Закон Российской Федерации о цифровой подписи

**Введение**

В настоящее время значение методов и средств защиты информации возрастает. Это во многом связано с расширением электронного документооборота. Все больше используется электронная электронная цифровая подпись. Для повышения надежности систем аутентификации, систем подписи применяются самые современные результаты и методы алгебры и алгебраической геометрии. Так, действующий стандарт ЭЦП России основан на эллиптических кривых.

Настоящее пособие призвано заполнить пробел в учебно-методической литературе. В пособии приводятся основные сведения об эллиптических кривых, описываются схемы генерации общего ключа, шифрования данных и ЭЦП.

Теория эллиптических кривых является частью теории плоских алгебраических кривых –одного из важнейших разделов алгебраической геометрии. Имеются тесные связи теории эллиптических кривых с теорией эллиптических функций и с диофантовым анализом. Начало этой теории было положено в трудах древнегреческого математика Диофанта и в дальнейшем ее развитии приняли участие многие выдающиеся математики прошлого. Структуру группы на эллиптических кривых определил знаменитый математик Анри Пуанкаре.

Долгое время теория эллиптических кривых являлась областью чистой математики, не имевшей приложений. Однако в 1980-х годах были найдены приложения этой теории к построению алгоритмов факторизации больших чисел. И далее теория эллиптических кривых нашла применения как в классической криптографии ( генерация псевдослучайных последовательностей), так и в построении криптосистем с открытым ключом, в разработке протоколов распределения ключей и протоколов цифровой подписи.

Идея создания эллиптической криптографии была выдвинута в 1985 году независимо В.Миллером и Н.Коблицем. Интерес в криптографии к эллиптическим кривым обусловлен тем, что они являются богатым источником конечных абелевых групп, обладающих полезными структурными свойствами, а также тем, что на их основе обеспечиваются те же криптографические свойства, которыми обладают числовые или полиномиальные криптосистемы, но при существенно меньшем размере ключа.

Во многих отношениях эллиптические кривые – естественный аналог мультипликативных групп полей, но более удобный, так как существует бóльшая свобода в выборе эллиптической кривой, чем в выборе конечного поля.

Заметим еще, что изобретение концепции несимметричной криптографии (в частности, криптосистем на эллиптических кривых) повлекло быструю алгебраизацию криптографии, вовлечение в практику все новых алгебраических объектов. Следует отметить , что даже простая реализация новых криптографических алгоритмов требует достаточно серьезной математической подготовки. Для применения таких алгоритмов надо не только уметь выполнять операции в соответствующих алгебраических структурах, но и решать другие задачи, например, находить корни уравнений над конечными полями и выполнять операции над алгебраическими числами.

**Глава 1.**

**ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ**

Начнем с изложения основных определений и свойств эллиптических кривых. Мы ограничимся минимальным числом основных фактов, необходимых для понимания приложений к криптографии, уделяя больше внимания примерам и конкретным описаниям и меньше заботясь о доказательствах и общности. Более систематическое изложение этих вопросов можно найти в литературе (см. список).

**§ 1. Алгебраические кривые и эллиптические кривые**

В этом параграфе мы предполагаем, что 𝕂 – поле: либо поле ℝ вещественных чисел, либо поле ℚ рациональных чисел, либо поле *C* комплексных чисел, либо поле из 𝑞 = элементов, -простое(см. ниже пример кривой над . Напомним, что характеристикой поля 𝕂 называется такое натуральное число 𝑝 = char 𝕂, что

𝑝 ⋅ 1 = 0, где 1 и 0 – единичный и нулевой элементы 𝕂 соответственно.

*Алгебраической кривой порядка* 𝑛 *над полем* 𝕂 называется множество пар (𝑥, 𝑦) , 𝑥, 𝑦 ∊ 𝕂 , удовлетворяющих уравнению 𝐹(𝑥, 𝑦) = 0, где 𝐹(𝑥, 𝑦)—многочлен степени 𝑛 с коэффициентами из 𝕂. Напомним, что *степенью одночлена* называется сумма степеней входящих в него переменных, а *степенью многочлена*—максимальная из степеней составляющих его одночленов.

**Пример 1**.

Степень одночлена 5𝑥2𝑦3 равна 5, а степень многочлена 5𝑥2𝑦3 + 7𝑥𝑦5 + 3 равна 6.

Пары (𝑥, 𝑦) элементов поля 𝕂, удовлетворяющие уравнению кривой, называются ее *точками.*

Точка (𝑥0, 𝑦0) кривой 𝐹(𝑥, 𝑦) = 0 называется *неособой*, если значения частных производных многочлена 𝐹 в ней не равны нулю одновременно. Частные производные определяются известными формальными правилами дифференцирования, применяемыми к многочленам над произвольным полем (линейность дифференцирования и правило Лейбница), из которых следует: если многочлен 𝐹(𝑥, 𝑦) записан по степеням 𝑥 как 𝐹(𝑥, 𝑦) = (𝑦) + (𝑦)𝑥 + … + (𝑦), то (𝑦) + 2(𝑦)𝑥 + … + 𝑛(𝑦) и аналогичная формула имеет место для частного дифференцирования по

переменной 𝑦.

Кривая называется *неособой,* или *гладкой*, если все её точки неособые. В любой такой точке (, ) к ней можно провести *касательную*, т. е. прямую, определяемую уравнением

(𝑥 – ) ⋅ (, ) + (𝑦 - ) ⋅ (, ) = 0.

Гладкая кривая третьего порядка над полем 𝕂 называется *эллиптической кривой* над тем же полем, если на ней есть хотя бы одна точка. Но если даже точек нет, то они могут появиться, если рассмотреть эту кривую над каким-нибудь **расширением поля 𝕂.**

Ньютон доказал, что над полем действительных чисел любую эллиптическую кривую можно преобразовать к виду = + 𝑎𝑥 + 𝑏 (получившему позже название *формы Вейерштрасса*) с помощью замены координат вида

𝑥´ = , 𝑦´ = ,

где ≠ 0- линейные функции (*проективная замена координат*).

В случае произвольного поля всякую эллиптическую кривую можно преобразовать к виду

+ 𝑥𝑦 + 𝑦 = + + 𝑥 + , ∈ 𝕂, (1)

также называемую формой Вейерштрасса.

Будем обозначать 𝐸(𝕂) множество точек (𝑥, 𝑦) ∈ 𝕂2, удовлетворяющих этому уравнению, и содержащее, кроме того, *бесконечно удалённую* точку, обозначаемую 𝒪.Мы понимаем бесконечно удаленную точку как точку, расположенную бесконечно далеко в положительном направлении оси О𝑦 и рассматриваем ее как третью точку пересечения множества 𝐸(𝕂) и любой вертикальной линии. Всякая вертикальная линия пересекается с множеством 𝐸(𝕂) в точках (𝑥1,𝑦1) , (𝑥1,𝑦2), 𝒪.

Если -расширение поля 𝕂, то 𝐸() обозначает множество точек (𝑥, 𝑦) ∈ , удовлетворяющих(1), вместе с точкой 𝒪. В определение эллиптической кривой удобно включить и требование её гладкости и для *алгебраически замкнутого расширения* поля 𝕂 (т. е. такого расширения, в котором любой многочлен имеет корень). Иными словами, два уравнения

𝑦 - 3 - 2𝑥 - = 0,

(2)

2𝑦 + 𝑥 + = 0

**не должны удовлетворяться одновременно ни в одной точке (𝑥, 𝑦) ∈ 𝐸().**

**Замечание 1.О нумерации и названии.**

В частном случае, когда = = = = 0, = -1, эллиптическая кривая

= – 𝑥.

над полем ℝ действительных чисел при больших 𝑥 ведёт себя как функция

𝑦 = , которая может быть параметризована подстановкой 𝑥 = , 𝑦 = . Если считать, что 𝑥 имеет степень 2, а 𝑦 имеет степень 3, индексы коэффициентов в (1) определяют степени, которые должны быть даны коэффициентам, чтобы это уравнение стало однородным, т. е. чтобы степень каждого члена была равна 6 (в общем случае эллиптическая кривая не имеет рациональной параметризации). Кривой = 𝑓(𝑥) соответствует *эллиптический интеграл*

,

не выражающийся через элементарные функции.

Напомним, что эллиптическим интегралом называют интеграл вида

,

где 𝐺(𝑥)-многочлен третьей или четвёртой степени, не имеющий кратных корней, а 𝑅(𝑥, 𝑦)-рациональная функция двух переменных. Впервые такие интегралы появились при вычислении дуг различных кривых, в частности, эллипсов, ещё в XVII веке. В 1752 году Л. Эйлер доказал, что сумма интегралов

где 𝑓(𝑥)-произвольный многочлен четвёртой степени, равен одному интегралу:

причём 𝛾 выражается рационально через 𝛼 и 𝛽. Как было выяснено Абелем и Якоби в двадцатых годах девятнадцатого столетия, ***это равенство объясняется наличием группового закона на эллиптической кривой с уравнением* = 𝑓(𝑥).**

**Дискриминант и 𝑗-инвариант**

Общее уравнение кривой (1) можно упростить.При этом, однако, необходимо наложить ограничения на характеристику поля.

Введем (стандартные ) обозначения:

𝑏2=𝑎12+4𝑎2 , 𝑏4=2𝑎4+𝑎1𝑎3 ,

(3)

𝑏6=𝑎32+4𝑎6 , 𝑏8=𝑎12𝑎6+4𝑎2𝑎6‒𝑎1𝑎3𝑎4+𝑎2𝑎32‒𝑎42 ,

и

= - 24, = - + 36 - 216. (4)

Предположим вначале, что char 𝕂 ≠ 2. Выделив в (1) полный квадрат по 𝑦 и заменив 𝑦 + (𝑥 + ) на 𝑦, получим уравнение

= 4 + + 2𝑥 + , (5)

где , , определяются формулами (3).

Предположим теперь, что к тому же char 𝕂 ≠ 3. Заменим (𝑥, 𝑦) в (5) на , в результате получим уравнение

= - 27𝑥 -54 , (6)

где и имеют вид (4).

Хотя в первую очередь нас интересуют рациональные решения уравнения (1), т. е. случай char 𝕂 = 0, мы предпочитаем рассматривать уравнение (1), а не более простые (5) и (6). Причина состоит в следующем. Пасть дана эллиптическая кривая, заданная уравнением вида(1) с целыми коэффициентами. Часто нужно рассматривать эту кривую не над полем ℚ, а над полем , что можно сделать, так как коэффициенты уравнения, задающего кривую, целые. Такой переход от поля ℚ к полю называется *редукцией кривой по модулю* 𝑝. Если 𝑝 = 2 или 𝑝 = 3, то одна из замен переменных, приводящих уравнение(1) к виду (6)не определена, так как в одной из них есть множитель , а в другой . поэтому, рассматривая над или вместо кривой, заданной уравнением (1), кривую (6), мы, фактически, рассматриваем совершенно другую кривую.

Проиллюстрируем сказанное примером.

**Пример 2**.

Рассмотрим эллиптическую кривую, заданную уравнением 𝑦2 ‒ 9𝑦 = 𝑥3 ‒ 27. Прибавив к обеим частям уравнения и выделяя полный квадрат в левой части, получим: (𝑦‒)2 = 𝑥3‒. Сделаем замену: 𝑦1 = 𝑦‒ , 𝑥1 = 𝑥 , получим уравнение: 𝑦12 = 𝑥13-. И после замены : 𝑦2 =𝑦1 , 𝑥2 =𝑥1 имеем уравнение 𝑦22 = 𝑥23‒24·33, имеющее вид (6). В этой замене содержатся множители , , . Как следует из теоремы 1 (см.ниже), кривая 𝑦2‒9𝑦=𝑥3‒27 остается неособой после редукции по модулю любого простого числа, за исключением 3, тогда как кривая

𝑦22 = 𝑥23‒24·33 остается неособой после редукции по модулю любого простого числа, за исключением 2 и 3. Таким образом, при переходе от кривой 𝑦2 ‒ 9𝑦 = 𝑥3 ‒ 27 к кривой 𝑦2 = 𝑥3- ⋅ (мы возвращаемся к обозначениям переменных 𝑥 и 𝑦) теряется информация, которая может быть получена редукцией по модулю 2.

Для любого поля 𝕂 определим *дискриминант* Δ кривой (1) формулой

Δ = - - 8 - 27 + 9, (7)

где имеют вид (3). Дискриминант кривой, заданной уравнением (5), определим этой же формулой (7), только в качестве чисел будем рассматривать коэффициенты уравнения (5). Если характеристика поля 𝕂 не равна 2 или 3, мы можем найти Δ из соотношения

1728Δ = - , (8)

где в качестве используются их выражения через коэффициенты и .

**Замечание2.**

Если использовать (6) как исходное уравнение кривой, то по формуле (7) её дискриминант Δ равен - . Формула же (8) даёт значение, отличающееся от этого в раз. Это объясняется тем, что при переходе от уравнения (5) к уравнению (6) мы меняли масштаб.

**Пример 3.**

Дискриминант кривой 𝑦2 ‒ 9𝑦 = 𝑥3 ‒ 27 равен Δ = - , а дискриминант кривой 𝑦2 = 𝑥3 - 24 ∙ 33 равен Δ = - , т. е. кривая 𝑦2 = 𝑥3 - 24 ∙ 33- особая по модулю 2, а кривая 𝑦2 ‒ 9𝑦 = 𝑥3 ‒ 27- нет.

Для дальнейшего нам понадобится дискриминант многочлена.

Напомним, что дискриминантом многочлена

𝑓(𝑥) = + + … + 𝑥 + называется величина

где - корни многочлена 𝑓(𝑥).

Рассмотрим многочлен

𝑓(𝑥) = - 𝛼 + 𝛽𝑥 – 𝛾 = (𝑥 - )( 𝑥 - )( 𝑥 - ) (9)

третьей степени от одной переменной над полем 𝕂 с корнями , принадлежащими - алгебраическому замыканию поля 𝕂. По формулам Виета:

𝛼 = + + , 𝛽 = + + , 𝛾 = .

**Утверждение1.**

*Дискриминант* 𝑑 *многочлена*

𝑓(𝑥) = - 𝛼 + 𝛽𝑥 – 𝛾

*равен*

𝑑 = det ,

*где*

= 𝛼, = - 1𝛽,

= - 3𝛼𝛽 + 3𝛾, = - 4𝛽 + 2 + 4𝛼𝛾.

Доказательство проводится прямыми вычислениями.

Упражнение: провести подробные вычисления.

**Следствие.** *Дискриминант многочлена третьей степени*

𝑓(𝑥) = + 𝑝𝑥 + 𝑞 *равен* 𝑑 = - 4 - 27.

**Пример 4.** Дикриминант произвольного многночлена.

Пусть коэффициенты многочлена третьей степени принадлежат ℝ. Его дискриминант 𝑑 равен нулю тогда и только тогда, когда многочлен имеет кратные корни.

Мы определили дикриминант для кубического многочлена с коэффициентом при 𝑥3, равном 1. Для произвольного многочлена определим дискриминант 𝑑 следующим образом. Разделим данный многочлен на коэффициент при 𝑥3 и дикриминант полученного многочлена объявим дискриминантом исходного.Если в кубическом многочлене заменить 𝑥 на , то дискриминант умножится на C6 , так как каждый корень умножится на C.

**Утверждение2** .

Пусть char 𝕂 ≠2, и пусть 𝑑𝑏 и 𝑑𝑐 --дискриминанты многочленов, стоящих в правых частях уравнений (5) и (6) соответственно, а 𝛥—дискриминант кривой, заданной уравнением (5). Тогда

𝑑𝑐 = , (10.1)

𝛥 = . (10.2)

**Доказательство.**

Рассмотрим случай char 𝕂 ≠3. Уравнение (6) получается из уравнения (5) композицией замен вида 𝑥⟶𝑥+𝑥0 , при которых дискриминант не меняется, и замены 𝑥 на , при которой дискриминант умножается на C6 . Таким образом получается формула (10.1). Из следствия и формулы (8) имеем:

𝑑𝑐=‒4(‒27𝑐4)3‒27(‒54𝑐6)2 =2239123 𝛥.

Таким образом, (10.2) следует из (10.1).

Теперь рассмотрим случай char 𝕂 =3. Из следствия непосредственно получаем: 𝑑𝑐=0. Поэтому (10.1) выполняется. Дискриминант 𝑑𝑏 по определению равен дискриминанту многочлена - 𝛼 + 𝛽𝑥 – 𝛾 , где 𝛼= ‒ ‒ , 𝛽=‒ , 𝛾 = ‒ . Так как в поле 𝕂 выполняется равенство 3 = 0, то из утверждения 1 следует, что

= 2 - - = - - - ,

где

= 𝛼, = + 𝛽, = , = - 𝛽 - + 𝛼𝛾,

и

𝛼 = - , 𝛽 = - , 𝛾 = - .

Постановка даёт

= - + - 𝛾 = + - .

В то же время, можно проверить, что независимо от характеристики поля

4 = - . (11)

Это равенство, в частности, используется, чтобы показать, что из формулы (7) следует (8). Следовательно, для поля 𝕂 характеристики 3

𝛥 = - + = - + + . (12)

Сравнив это уравнение с (11), мы видим, что 𝛥 = . Отсюда следует равенство (12).

**Теорема 1.** *Кубическая кривая, заданная уравнением (1), является особой тогда и только тогда, когда её дискриминант 𝛥 равен 0.*

Доказательство теоремы 1 опирается на сформулированные ранее утверждения. С подробным доказательством можно ознакомиться по [1,с. 80-83].

*Допустимой заменой переменных* (*над полем* 𝕂) в уравнении Вейерштрасса (1) назовём замену

𝑥 = 𝑥′ + 𝑟, 𝑦 = 𝑦′ + 𝑠 𝑥′ + 𝑡 (13)

где 𝑢, 𝑟, 𝑠, 𝑡 принадлежит 𝕂 и 𝑢 ≠ 0.

Легко проверить, что замена переменных, обратная к допустимой, также является допустимой. С точностью до умножения переменных на константы кривая, заданная в форме Вейерштрасса, после допустимой замены переменной переходит в кривую в форме Вейерштрасса. Говорят, что две эллиптические кривые, связанные допустимой заменой переменных, *изоморфны*.

**Примеры эллиптических кривых , имеющих небольшие дискриминанты.** В таблицах 1 и 2 приведены списки всех, с точностью до допустимых замен переменных над ℚ, эллиптических кривых, которые задаются уравнениями с целыми коэффициентами, по абсолютной величине не превосходящими 9 и для которых ∣𝛥∣<100. Тройка (𝛥, , ) может быть использована для определения того, эквивалентны ли над ℚ две эллиптические кривые с небольшими дискриминантами. Именно, две эллиптические кривые над ℚ с одинаковыми тройками (𝛥, , ) связаны преобразованием (13), так как замены переменных, которые переводят уравнение (1) в уравнение (6, обратимы. Обратно, если эллиптические кривые связаны преобразованием (13), то отношение их дискриминантов равно , а так как коэфициенты целые и ∣𝛥∣<100, это возможно только при 𝑢 = ± 1, но тогда дискриминанты, а также коэффициенты и , у этих кривых одинаковые. Следовательно, тройка (𝛥, , ) является полным инвариантом класса эквивалентности для кривых, имеющих описанные выше ограничения.

|  |  |  |  |
| --- | --- | --- | --- |
| Эллиптическая кривая | 𝛥 |  |  |
| + 𝑦 = –  + 𝑥𝑦 = - + 𝑥  + 𝑦 = + + 𝑥  + 𝑥𝑦 + 𝑦=  + 𝑦 =  + 𝑥𝑦 – 𝑦 =  + 𝑦 = + – 𝑥  + 𝑥𝑦 = + + 𝑥  + 𝑦 = +  = - + 𝑥  = + +𝑥  + 𝑥𝑦 + 𝑦 = -  + 3𝑥𝑦 – 𝑦 =  + 𝑥𝑦 = - + 𝑥  + 𝑥𝑦 = - 2𝑥 + 1  + 𝑥𝑦 = + 𝑥  = + 𝑥  + 𝑦 = - 5 - 4𝑥 – 1  + 3𝑥𝑦 + 𝑦 = -  + 𝑥𝑦 - 𝑦= +  + 𝑦 = + 𝑥  + 4𝑥𝑦 – 𝑦 = | - 11  -15  -19  -26  -27  -28  -35  -39  -43  -48  -48  -53  -54  -55  -61  -63  -64  -67  -83  -89  -91  -91 | 16  1  -32  -23  0  25  64  -23  16  -32  -32  -15  153  -39  97  -47  -48  592  -47  49  -48  352 | -152  -161  8  -181  -216  -253  -568  235  -280  -224  224  -297  -1917  -189  -1009  71  0  14408  199  -521  -216  -6616 |

**Таблица 1.** Список уравнений кривых с целыми коэффициентами, по абсолютной величине не превосходящими 9, для которых -100<𝛥<0.

|  |  |  |  |
| --- | --- | --- | --- |
| Эллиптическая кривая | 𝛥 |  |  |
| + 7𝑥𝑦 + 2𝑦 = + 4 + 𝑥  + 3𝑥𝑦 = + 𝑥  + 𝑦 = – 𝑥  + 2𝑥𝑦 - 3𝑦 = - 1  + 𝑥𝑦 = - 3 + 𝑥  + 9𝑥𝑦 - 9𝑦 = + 9 - 5𝑥 – 3  = – 𝑥  + 𝑥𝑦 = – 𝑥  + 𝑥𝑦 = - – 𝑥  + 3𝑥𝑦 - 𝑦 = -  = - 2𝑥 +1  = - 2𝑥 – 1  = + – 𝑥  = - – 𝑥  + 𝑥𝑦 = + – 𝑥  + 5𝑥𝑦 + 𝑦 = | 15  17  37  37  57  62  64  65  73  79  80  80  80  80  89  98 | 3841  33  48  160  73  15873  48  49  57  97  96  96  64  64  73  505 | -238049  -81  -216  -2008  539  -1999809  0  -73  243  -881  -864  864  -352  352  -485  -11341 |

**Таблица 2.** Список уравнений кривых с целыми коэффициентами, по абсолютной величине не превосходящими 9, для которых 0<𝛥<100.

Определим 𝑗-инвариант эллиптической кривой формулой

𝑗= **.** (14)

При допустимых заменах переменных новые значения коэффициентов и и дискриминанта 𝛥 не зависят от параметров 𝑟, 𝑠 и 𝑡. Следовательно, 𝑗-инвариант не меняется при допустимых заменах переменных.

**Пример 5.**

Предположим, что характеристика поля 𝕂 не равна ни 2, ни 3. Рассмотрим кривую = + 𝑝𝑥 + 𝑞, где 𝑝, 𝑞 ∈ 𝕂.

Для неё = - 48𝑝 = - 864𝑞. (См. замечание) По формуле (8)

𝛥 = = - ( + 27).

Формула (14) даёт

𝑗 = 1728 . (15)

Таким образом, 𝑗-инвариант любой эллиптической кривой вида

= + 𝑎𝑥 равен 1728. Аналогично, 𝑗-инвариант любой кривой вида = + 𝑎 равен 0. Для кривой = – 𝑥 +9 имеем 𝑝 = - 1 и 𝑞 = 9. Тогда формула (15) даёт 𝑗 = - .

**Теорема 2.** *Предположим, что характеристика поля* 𝕂 *не равна* 2 *или* 3. *Тогда справедливы следующие утверждения.*

(𝑎) *Если две эллиптические кривые связанны допустимой заменой переменных, то они имеют одинаковые* 𝑗-*инварианты.*

(𝑏) *Если задано число*  ∈ 𝕂*, то существует эллиптическая кривая над* 𝐾 *с* 𝑗-*инвариантом, равным .*

(𝑐) *Если поле* 𝕂 *алгебраически замкнуто и две эллиптические кривые имеют одинаковые* 𝑗-*инварианты, то они связаны допустимой заменой переменных.*

**Доказательство.** Пункт (𝑎) непосредственно следует из определения 𝑗-инварианта.

Для пункта (𝑏) достаточно привести примеры. Как было указано выше, 𝑗-инвариант любой эллиптичеакой кривой вида

= + 𝑎𝑥 равен 1728, а 𝑗-инвариант любой кривой вида = + 𝑎 равен 0. Для других значений рассмотрим кривую

= - 𝑥 - .

Легко проверить, что она неособая и, следовательно, эллиптическая. Для неё 𝑝 = 𝑞 = - . Согласно формуле (15) в этом случае 𝑗-инвариант кривой равен .

Доказательство пункта c) оставляем читателю в качестве упражнения.

**Пример 6**.

Рассмотрим кривую𝛦, заданную над полем 𝔽7  уравнением = + 𝑥 + 3. Вычисляя определенные ранее константы, найдем: 𝛥( 𝛦)=3 и 𝑗(𝛦)=5. Сделаем замену переменных 𝑥=4 𝑥′+3, 𝑦=𝑦′+2 𝑥′+5. Получим изоморфную кривую 𝛦′ , заданную уравнением (𝑦′)2 +4 𝑥′ 𝑦′+3 𝑦′=( 𝑥′)3 + 𝑥′+1. Легко убедиться, что 𝑗(𝛦′)=5.

**Замечание к теореме 2**.

Совокупность утверждений a ) и c) равносильна следующему утверждению: Изоморфные над полем 𝕂 кривые имеют один и тот же -𝑗инвариант и любые кривые с совпадающими 𝑗 -инвариантами изоморфны над *алгебраическим замыканием* . (Напомним, что если дано поле 𝕂, то алгебраическое замыкание получается присоединением всех корней алгебраических уравнений с коэффициентами из поля 𝕂).

При этом условие алгебраической замкнутости существенно, то есть кривые с одним и тем же -инвариантом не обязательно изоморфны над основным (не являющимся алгебраически замкнутым)полем. Проиллюстрируем это следующим примером.

**Пример 7.**

Для кривой над полем 𝔽7, заданной уравнением

𝛦′′: (𝑦′′)2 =(𝑥′′)3 +4𝑥′′+4,

𝑗 -инвариант равен 5, как и у кривой = + 𝑥 + 3. Но эти кривые не изоморфны над 𝔽7 , поскольку замена переменных, задающая изоморфизм, выглядит как

𝑥=3𝑥′′ и 𝑦=𝑦′′, но ∉ 𝔽7 .

Итак, 𝛦 и 𝛦′′ определены над полем 𝔽7 , но не изоморфны над ним. Эти кривые будут изоморфны над любым алгебраическим расширением поля 𝔽7 , содержащим элемент , например, над полем = .

**Эллиптические кривые над полем вещественных чисел.**

Характерные формы эллиптической кривой над полем действительных чисел приведены на рис. 1(кривая с отрицательным дискриминантом) и на рис. 2(кривая с положительным дискриминантом).

𝑌 𝑌

𝑋 𝑋

**Рис. 1.** Эллиптическая кривая **Рис. 2.** Эллиптическая кривая

с отрицательным дискри- с положительным дискри-

минантом минантом.

**Упражнения к § 1.**

1. Доказать, что множество допустимых преобразований координат образует группу относительно операции композиции преобразований.
2. Доказать, что множество всех эллиптических кривых над данным полем разбивается на классы эквивалентности относительно отношения изоморфизма
3. Доказать, что любая эллиптическая кривая над полем 𝕂 характеристики, отличной от 2, изоморфна кривой вида

= + + 𝑥 + , ∈ 𝕂.

1. Доказать, что любая эллиптическая кривая над полем 𝕂 характеристики ≠2,3 изоморфна кривой вида

= + , ∈ 𝕂.

1. Доказать, что любая эллиптическая кривая над полем 𝕂 характеристики 2 изоморфна кривой вида

+ 𝑥𝑦 = + + , ∈ 𝕂,

(несуперсингулярные кривые)

или кривой вида

+ 𝑦 = + + , ∈ 𝕂.

(суперсингулярные кривые)

**§ 2. Группа точек эллиптической кривой**

Перед обсуждением конкретных примеров эллиптических кривых над различными полями мы отметим чрезвычайно важное свойство точек эллиптической кривой: они образуют абелеву группу относительно операции сложения точек, о которой будет подробнее сказано ниже. Чтобы объяснить наглядно, как это получается, мы временно будем полагать, что 𝕂 = ℝ. т.е. что эллиптическая кривая – обычная плоская кривая (с добавлением еще одной точки 𝒪 «в бесконечности»).

**Определение.**

Пусть 𝛦 – эллиптическая кривая над полем вещественных чисел и пусть 𝑃 и 𝑄 – две точки на 𝛦. Определим точки -𝑃 и 𝑃+𝑄 по следующим правилам:

1. Точка 𝒪 – тождественный элемент по сложению («нулевой элемент») группы точек. В следующих пунктах предполагается, что ни 𝑃, ни 𝑄 не являются точками в бесконечности.

2. Точки 𝑃 = (𝑥, 𝑦) и - 𝑃 имеют одинаковые *-*координаты, а их

*у* -координаты различаются только знаком, т.е. – (𝑥, 𝑦) = (𝑥, - 𝑦). Из (1) сразу следует, что (𝑥, - 𝑦) – также точка на 𝛦.

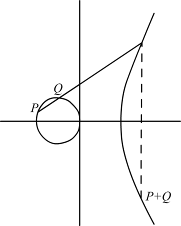
3. Если 𝑃 и 𝑄 имеют различные -координаты, то прямая 𝑙 = имеет с 𝛦 еще в точности одну точку пересечения 𝑅 (за исключением двух случаев: когда она оказывается касательной в *Р*, и мы тогда полагаем 𝑅 = 𝑃, или касательной в 𝑄, и мы тогда полагаем 𝑅 = 𝑄). Определяем теперь 𝑃 + 𝑄 как точку -𝑅, т.е. как отражение от оси 𝑥 третьей точки пересечения. Геометрическое построение, дающее 𝑃 + 𝑄, приводится ниже в примере 7.

4. Если 𝑄 = -𝑃 (т. е. -координата 𝑄 та же, что и y 𝑃, а 𝑦-координата отличается лишь знаком), то полагаем 𝑃 + 𝑄 = 𝒪 («точке в бесконечности»; это является следствием правила 1).

5. Остается возможность 𝑃 = 𝑄. Тогда считаем, что 𝑙– касательная к кривой в точке 𝑃. Пусть 𝑅 – единственная другая точка пересечения 𝑙 с 𝛦. Полагаем 𝑃 + 𝑄 = -𝑅 (в качестве 𝑅 берем 𝑃, если касательная прямая в 𝑃 имеет «двойное касание», т. е. если 𝑃 есть точка перегиба кривой).

**Пример 8.**

На рис. 3 изображена эллиптическая кривая = – 𝑥 в плоскости 𝑥𝑂𝑦 и приведен типичный случай сложения точек 𝑃 и 𝑄. Чтобы найти 𝑃 + 𝑄, проводим прямую и в качестве 𝑃+ 𝑄 берем точку, симметричную относительно оси 𝑥 третьей точке, определяемой пересечением прямой и кривой. Если бы 𝑃совпадала с 𝑄, т.е. если бы нам нужно было найти 2𝑃, мы использовали бы касательную к кривой в 𝑃: тогда точка 2𝑃 симметрична третьей точке, в которой эта касательная пересекает кривую.



**Рис. 3.** Пример геометрического построения суммы точек эллиптической кривой

Теперь мы покажем, почему существует в точности еще одна точка, в которой прямая 𝑙, проходящая через 𝑃 и 𝑄, пересекает кривую; заодно мы выведем формулу для координат этой третьей точки и тем самым – для координат 𝑃 + 𝑄.

Обозначим ( - координаты точек 𝑃, 𝑄 и 𝑃 + 𝑄соответственно. Мы хотим выразить и через и .

Предположим, что мы находимся в ситуации п. 3 определения операции сложения точек, и пусть  есть уравнение прямой, проходящей через *Р* и *Q* (в этой ситуации она не вертикальна). Тогда и . Точка на *l*, т. е. точка , лежит на эллиптической кривой тогда и только тогда, когда

.

Таким образом, каждому корню кубического многочлена  соответствует точка пересечения. Мы уже знаем, что имеется два корня  и , так как  и  – точки *Р* и *Q* на кривой. Так как сумма корней нормированного многочлена (т.е. многочлена, старший коэффициент которого равен 1) равна взятому с обратным знаком коэффициенту при второй по старшинству степени многочлена, то в нашем случае третий корень – это. Тем самым получаем выражение для , и, следовательно, *Р + Q* = , или, в терминах ,:

 (16)



Ситуация в п. 5 аналогична рассмотренной, только теперь  – производная  в точке *Р*. Дифференцирование неявной функции, заданной уравнением (1), приводит к формуле , и мы получаем следующие формулы для координат удвоенной точки:

, (17)

.

Заметим, что если бы мы суммой точек *Р* и *Q* назвали точку *R* , то так определенная операция не удовлетворяла бы очевидному свойству

*P* +*Q = R* ⟹ *P* = *R* – *Q .*

**Пример 9.** Пусть *Р* = (-3, 9) и *Q* = (-2, 8) – точки на эллиптической кривой . Найти *Р + Q* и 2*Р*.

**Решение.** Подстановка ,в первое из уравнений (4) дает ; тогда второе из уравнений (16) дает . Непосредственной подстановкой координат точки *P* + *Q* = (6, 0) в уравнение кривой можно убедиться в том, что она также лежит на ней. Далее, подставляя , ,  в первое из уравнений (17), получаем для -координаты точки 2*Р* значение 25/4, а второе из уравнений (17) дает для *у*-координаты значение -35/8. Точка 2*P* = (25/4, -35/8) также принадлежит рассматриваемой кривой.

Существует несколько способов доказать, что множество точек на эллиптической кривой с определенной выше операцией сложения образует абелеву группу. Можно использовать результаты из проективной геометрии, из комплексного анализа двоякопериодических функций или алгебраическое доказательство, использующее теорию дивизоров на кривых. Доказательства каждого из этих типов можно найти в источниках, указанных в списке литературы.

Если 𝑛 – целое число, то, как и в любой абелевой группе, 𝑛*P* обозначает сумму 𝑛 точек *Р* при *n* > 0 и сумму |𝑛| точек -*Р*, если.

Еще несколько слов о «точке в бесконечности» 𝒪. По определению, это нейтральный элемент группового закона. В графической интерпретации следует себе представлять ее расположенной на оси 𝑦 в предельном направлении, определяемом все более «крутыми» касательными к кривой. Она является «третьей точкой пересечения» с кривой для любой вертикальной прямой: такая прямая пересекается с кривой в точках вида ,  и в точке 𝒪. Мы изложим сейчас более естественный способ введения точки 𝒪.

Под *проективной плоскостью* мы понимаем множество классов эквивалентности троек (*X*, *Y, Z*) (не все компоненты равны нулю), при этом две тройки называются эквивалентными, если одна из них – скалярное кратное другой, т.е. (*X*, *Y*, *Z*) ~ (*X*, *Y*, *Z*). Такой класс эквивалентности называется проективной точкой. Если проективная точка имеет ненулевую компоненту *Z*, то существует, причем только одна, тройка в ее классе эквивалентности, имеющая вид (*х*, *у*, 1): просто полагаем *х* = *X/Z*, *у = Y/Z*. Тем самым проективную плоскость можно представить как объединение всех точек (*х*, *у*) обычной («аффинной») плоскости с точками, для которых *Z* = 0. Эти последние точки составляют то, что называется бесконечно удаленной прямой; наглядно ее можно, себе представить на плоскости как «горизонт». Любому алгебраическому уравнению кривой в аффинной плоскости *F*(*x*, *y*) = 0 отвечает уравнение  = 0, которому удовлетворяют соответствующие проективные точки: нужно заменить *х* на *X/Z*, у – на *Y/Z* и умножить на подходящую степень *Z*, чтобы освободиться от знаменателей. Например, если применить эту процедуру к аффинному уравнению (1) эллиптической кривой, то получится «проективное уравнение» . Этому уравнению удовлетворяют все проективные точки (*X*, *Y*, *Z*) с *Z*0, для которых соответствующие аффинные точки (*х*, *у*), где *х* = *X/Z*, *y* = *Y/Z*, удовлетворяют (1). Помимо них, какие еще точки бесконечно удаленной прямой удовлетворяют последнему уравнению? Если положить в уравнении *Z* = 0, то уравнение примет вид  = 0, т.е. *X* = 0. Но единственный класс эквивалентности троек с *X* = 0, *Z* = 0 – это класс тройки (0, 1, 0). Это и есть точка, которую мы обозначили 𝒪; она лежит на пересечении оси *у* с бесконечно удаленной прямой.

**Эллиптические кривые над полем комплексных чисел.**

Алгебраические формулы (16)-(17) для сложения точек на эллиптической кривой над вещественными числами на самом деле имеют смысл над любым полем. В полях характеристики 2 или 3 можно вывести аналогичные равенства. Можно показать, что точки эллиптической кривой над любым полем образуют абелеву группу по сложению, определенную по этим формулам.

В частности, пусть *Е* – эллиптическая кривая, определенная над полем ℂ комплексных чисел, т. е. *Е* – множество пар (𝑥, 𝑦) комплексных чисел, удовлетворяющих уравнению (1), вместе с точкой в бесконечности 𝒪. Мы называем *Е* «кривой», однако с точки зрения обычных геометрических представлений она двумерна, т.е. представляет собой поверхность в четырехмерном вещественном пространстве, координатами в котором являются действительные и мнимые части точек 𝑥 и 𝑦. Покажем теперь, как можно наглядно представить себе *Е* в качестве поверхности.

Пусть *L* – решетка в комплексной плоскости. Это означает, что *L* – абелева группа, состоящая из всех целочисленных линейных комбинаций двух данных комплексных чисел  и  (где  и  «заметают» плоскость, т.е. не лежат на одной прямой, проходящей через начало координат): *L* = ℤ** + ℤ (здесь ℤ – множество целых чисел). Например, если  = 1,  = *i*, то *L* – множество всех гауссовых целых чисел, т.е. квадратная сетка, состоящая из всех комплексных чисел с целыми действительными и мнимыми частями.

Если задана эллиптическая кривая (1) над полем комплексных чисел, то, как оказывается, существуют решетка *L* и функция комплексного переменного, называемая «р-функцией Вейерштрасса» и обозначаемая , co следующими свойствами:

1.  аналитична всюду, кроме точек *L*, в каждой из которых имеет полюс второго порядка.

2.  удовлетворяет дифференциальному уравнению  и, следовательно, при любом *z*  *L* точка  лежит на эллиптической кривой *Е*.

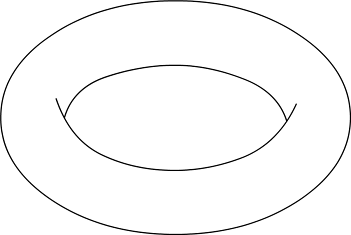
3. Два комплексных числа и  дают одну и ту же точку  на *Е* тогда и только тогда, когда .

4. Отображение, которое любой точке *z  L* ставит в соответствие точку  на *Е*, а любой точке *z  L* – точку в бесконечности 𝒪, дает взаимно однозначное соответствие между *Е* и факторгруппой ℂ/L комплексной плоскости по подгруппе *L*.

5. Это взаимно однозначное соответствие есть изоморфизм абелевых групп, иными словами, если  соответствует точке *Р*  *Е* , а  – точке *Q  Е*, то  +  соответствует точке *Р + Q*.

Таким образом, можно представлять себе абелеву группу *Е* как комплексную плоскость «по модулю» некоторой решетки. Чтобы эту последнюю группу изобразить наглядно, заметим, что у каждого класса эквивалентности  + *L* существует один и только один представитель в «фундаментальном параллелограмме», состоящем из комплексных чисел вида , 0  𝑎, *b* < 1 (если, например, *L* – гауссовы числа, то фундаментальный параллелограмм – это единичный квадрат). Так как разность между противоположными точками на параллельных сторонах границы параллелограмма есть точка решетки, они равны в ℂ/L, и их можно считать «склеенными». Наглядно это означает, что мы сгибаем параллелограмм так, чтобы одна из сторон соприкоснулась с противоположной (получая при этом часть цилиндра), и затем, вновь сгибая полученную цилиндрическую трубку, склеиваем противоположные окружности – и получаем тор («бублик»), изображенный на рис. 4.

Как группа, тор есть произведение двух экземпляров группы окружности, т.е. его точки можно параметризовать парой углов . Точнее, если тор получен из решетки *L* = , то следует представить элемент из ℂ/L в виде , полагая *а* = , *b* = . Таким образом, можно рассматривать эллиптическую кривую над комплексными числами как двумерное обобщение окружности в вещественной плоскости.



**Рис. 4.** Геометрическая интерпретация эллиптической кривой

над полем комплексных чисел

Фактически эта аналогия идет значительно дальше, чем может показаться. «Эллиптические функции» (которые показывают, как по точке (*х*, *у*)  *Е* найти то комплексное число *z*, для которого), как оказывается, имеют свойства, аналогичные свойствам известной функции Arcsin(*z*) (которая показывает, как найти вещественное число, которое соответствует точке единичной окружности при «наматывании» вещественной прямой на окружность). При рассмотрении эллиптических кривых с точки зрения теории алгебраических чисел обнаруживается глубокая аналогия между координатами «точек, делящих эллиптические кривые на 𝑛 частей» (т.е. таких точек *P*, что 𝑛*P* = 𝒪) и точками, делящими на 𝑛 частей единичную окружность (которые соответствуют корням степени 𝑛 из единицы в комплексной плоскости).

**Точки конечного порядка.**

*Порядком* 𝑛 точки *Р* на эллиптической кривой называется такое наименьшее натуральное число, что 𝑛*P =* 𝒪; разумеется, такого конечного 𝑛 может и не существовать, в этом случае мы будем говорить о точке бесконечного порядка. Часто требуется найти точки конечного порядка на эллиптической кривой, в особенности, на эллиптических кривых, определенных над полем рациональных чисел ℚ.

**Пример 10**. Найти порядок точки *Р* = (2, 3) на .

**Решение.** Применяя (17), находим, что 2*Р* = (0, 1), и вновь, с помощью (17), что 4*Р* = 2(2*Р*) = (0, -1). Поэтому 4*Р* = -2*P* и, следовательно,

6*P* = 𝒪.Тем самым порядок *Р* может быть равен 2, 3 или 6. Но 2*Р* = (0,1)  𝒪, а если бы *Р* имела порядок 3, то было бы 4*Р* = *Р*, что неверно. Итак, *Р* имеет порядок 6.

**Эллиптические кривые над полем рациональных чисел.**

Если в уравнении (1) 𝑎 и *b* – рациональные числа, то естественно рассматривать рациональные решения (𝑥, 𝑦), т.е. эллиптическую кривую над полем ℚ рациональных чисел.

Прежде всего заметим, что 𝑎 и 𝑏 можно считать целыми числами. Действительно, пусть 𝑎= , 𝑏= (эти дроби не предполагаются несократимыми). Положим 𝑦= , 𝑥= .

Тогда исходное уравнение запишется в виде =+𝑝𝑞3+𝑟 , коэффициенты этого уравнения—целые.

В 1901 году А.Пуанкаре высказал гипотезу: все рациональные точки 𝛦(ℚ) эллиптической кривой 𝛦

= + 𝑎𝑥+𝑏 , 𝑎 , 𝑏⋴ℤ ,

Могут быть получены из некоторого конечного их числа операциями сложения точек. Точная формулировка в алгебраических терминах такова:

**Теорема 3.** *На эллиптической кривой* 𝐸 *, заданной уравнением с целыми коэффициентами, группа* 𝐸(ℚ) *рациональных точек является конечнопорожденной абелевой группой.*

Строгое доказательство гипотезы Пуанкаре получил английский математик Л.Морделл в 1922 году.

Согласно теореме, каждая из таких групп есть сумма конечной «подгруппы кручения» Tors*E*(ℚ) (точек конечного порядка) и подгруппы, порожденной конечным числом точек бесконечного порядка: . Число (минимальное) образующих бесконечной части называется *рангом* *r*; оно равно нулю тогда и только тогда, когда вся группа конечна.

Изучение ранга *r* и других свойств группы точек эллиптической кривой над ℚ связано со многими интересными вопросами теории чисел и алгебраической геометрии. Например, известный с древних времен вопрос «Существует ли прямоугольный треугольник с рациональными сторонами, площадь которого равна данному целому 𝑛?» эквивалентен следующему: «Верно ли, что ранг эллиптической кривой  больше нуля?» Случай 𝑛 = 6 и прямоугольного треугольника со сторонами 3, 4 и 5 соответствует точке *Р* = (-3, 9) из примера 8, которая является точкой бесконечного порядка на эллиптической кривой .

Ранг 𝑟 вычислен для многих эллиптических кривых над ℚ. В большинстве случаев он мал, чаще всего он равен 0,1,2,3. В таблицах 3 и 4 приводятся значения рангов кривых =+𝑎𝑥 и =+𝑎 для некоторых значений 𝑎.

|  |  |
| --- | --- |
| Ранг | Значение параметра 𝑎 |
|  | 𝑎 = 1, 2, 4, 6, 7, 10, 11, 12, 22,  -1, -3, -4, -8, -9, -11, -13, -18, -19 |
|  | 𝑎 = 3, 5, 8, 9, 13, 15, 18, 19, 20,  -2, -5, -6, -7, -10, -12, -14, -15, -20 |
|  | 𝑎 = 14, 33, 34, 39, 46, -17, -56, -65, -77 |
|  | 𝑎 = -82 |

**Таблица 3.** Ранги эллиптических кривых 𝛦, задаваемых уравнениями .

|  |  |
| --- | --- |
| Ранг | Значение параметра 𝑎 |
|  | 𝑎 = 1, 4, 6, 7, 13, 14, 16, 20, 21,  -1, -3, -5, -6, -8, -9, -10, -14, -432 |
|  | 𝑎 = 2, 3, 5, 8, 9, 10, 11, 12, 18,  -2, -4, -7, -13, -15, -18, -19, -20, -21 |
|  | 𝑎 = 15, 17, 24, 37, 43, -11, -26, -39, -47 |
|  | 𝑎 = -113, 141, 316, 346, 359, -174, -307, -362 |

**Таблица 4.** Ранги эллиптических кривых 𝛦, задаваемых уравнениями .

В настоящее время неизвестно, существуют ли эллиптические кривые сколь угодно большого ранга.

Структуру подгруппы кручения Tors 𝛦(𝑄) во многом проясняет следующее утверждение.

**Теорема 4.** *Пусть* 𝛦 –*эллиптическая кривая*

=+𝑎𝑥+𝑏, *где* 𝑎 *и* 𝑏 –*целые числа*. *Если* (𝑥,𝑦) –*точка конечного порядка в* 𝛦, *то ее координаты* 𝑥 *и* 𝑦 *являются делителями дискриминанта* 𝛥=⎯ ( + 27).

Эта теорема дает эффективный алгоритм нахождения подгруппы Tors 𝛦(ℚ) . Рассмотрим конечное множество всех делителей дискриминанта 𝛥 и найдем все целочисленные решения кубического уравнения +𝑎𝑥+𝑏⎯=0.

Тогда все точки конечного порядка (за исключением 𝒪) содержатся среди найденного множества точек .

Полное описание структуры подгрупп кручения дает следующая теорема, доказанная американским математиком Б.Мазуром в 1976 году.

**Теорема 5.** Пусть 𝛦—эллиптическая кривая над полем рациональных чисел. Тогда Tors 𝛦(ℚ) изоморфна одной из следующих групп:

1. Tors 𝛦(ℚ)≅ℤ/𝑛ℤ , 1≦𝑛≦10 или 𝑛=12,
2. Tors (ℚ)≅ℤ/2ℤ⨁ℤ/2𝑛ℤ , 1≦𝑛≦4.

**Эллиптические кривые над конечным полем.**

Будем предполагать, что 𝕂 – конечное поле , с элементами. Пусть *Е* – эллиптическая кривая, определенная над .

Если 𝕂 – поле характеристики 2, то *эллиптическая кривая над* 𝕂 – это множество точек, удовлетворяющих уравнению либо типа

 (18а)

либо типа

 (18б)

(здесь кубические многочлены в правых частях могут иметь кратные корни), вместе с «точкой в бесконечности» 𝒪.

Если 𝕂 – поле характеристики 3, то *эллиптическая кривая над* 𝕂 – это множество точек, удовлетворяющих уравнению

 (19)

(где кубический многочлен справа не имеет кратных корней), вместе с «точкой в бесконечности» 𝒪.

Любая эллиптическая кривая над полем 𝕂 характеристики ≠2,3 изоморфна кривой вида

= + 𝑎𝑥 + (см.упражнения к § 1).

Особый интерес для криптографии представляет объект, называемый эллиптический группой по модулю 𝑝, где 𝑝 является простым числом. Такая группа определяется следующим образом. Выберем два неотрицательных целых числа, 𝑎и 𝑏, которые меньше 𝑝 и удовлетворяют условию

+ (mod 𝑝) ≠ 0

Тогда обозначает эллиптическую группу по модулю 𝑝, элементами которой (𝑥, 𝑦) являются пары неотрицательных целых чисел, которые меньше 𝑝 и удовлетворяют условию



вместе с «точкой в бесконечности» 𝒪. Далее мы, говоря об эллиптической кривой, если не оговорено противное, будем иметь в виду именно эллиптическую группу по модулю 𝑝.

**Пример 11.**

Пусть 𝑝 = 23. Рассмотрим эллиптическую кривую . В этом случае 𝑎 = 𝑏 = 1и мы имеем:

4 ⋅ + 27 ⋅ (mod 23) ≠ 0,

что удовлетворяет условиям эллиптической группы по модулю 23.

Рассматриваются только целые значения от (0, 0) до (𝑝, 𝑝) в квадранте неотрицательных чисел, удовлетворяющих уравнению по модулю 𝑝. В таблице 7 представлены точки (отличные от 𝒪), являющиеся элементами . В нашем случае такой список можно создать по следующим правилам.

1. Вычисляем значения  (см. таблицу 5).

|  |  |
| --- | --- |
| *y* | (mod 23) |
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 16 |
| 5 | 2 |
| 6 | 13 |
| 7 | 3 |
| 8 | 18 |
| 9 | 12 |
| 10 | 8 |
| 11 | 6 |
| 12 | 6 |
| 13 | 8 |
| 14 | 12 |
| 15 | 18 |
| 16 | 3 |
| 17 | 13 |
| 18 | 2 |
| 19 | 16 |
| 20 | 9 |
| 21 | 4 |
| 22 | 1 |

**Таблица 5.** Значения  для 𝑦 от 0 до 22

2.Вычисляем значения  (см. таблицу 6).

|  |  |
| --- | --- |
| *x* |  |
| 0 | 1 |
| 1 | 3 |
| 2 | 11 |
| 3 | 8 |
| 4 | 0 |
| 5 | 16 |
| 6 | 16 |
| 7 | 6 |
| 8 | 15 |
| 9 | 3 |
| 10 | 22 |
| 11 | 9 |
| 12 | 16 |
| 13 | 3 |
| 14 | 22 |
| 15 | 10 |
| 16 | 19 |
| 17 | 9 |
| 18 | 9 |
| 19 | 2 |
| 20 | 17 |
| 21 | 14 |
| 22 | 22 |

**Таблица 6.** Значения  для 𝑥от 0 до 22

Теперь сравниваем числа в правых столбцах таблиц 1 и 2. Число, попавшее в оба столбца, определяет две точки кривой. Так, число 1 содержится и в правом столбце таблицы 5, и в правом столбце таблицы 6. Число 1 определяет точки (0,1) и (0,22); число 8 дает тоже две точки, находим по левым столбцам их координаты: это (3,10) и (3,13), и т.д. Получаем таблицу 7. Пара чисел (𝑥, 𝑦), для которой , включается в нашу таблицу соответствий: это точка кривой.

|  |  |  |
| --- | --- | --- |
| (0, 1) | (6, 4) | (12, 19) |
| (0, 22) | (6, 19) | (13, 7) |
| (1, 7) | (7, 11) | (13, 16) |
| (1, 16) | (7, 12) | (17, 3) |
| (3, 10) | (9, 7) | (17,20) |
| (3, 13) | (9, 16) | (18,3) |
| (4, 0) | (11, 3) | ' (18,20) |
| (5, 4) | (11, 20) | (19,5) |
| (5, 19) | (12, 4) | (19,18) |

**Таблица 7.** Точки кривой 

Легко видеть, что эллиптическая кривая может иметь не более 2*q* + 1 различных -точек, т.е. точку в бесконечности и не более чем 2*q* пар (*х*, *у*), *х*, *у* , удовлетворяющих (1) (или (18) или (19), если *р* = 2 или 3). А именно, для каждого из *q* возможных значений 𝑥 имеется не более двух значений 𝑦, удовлетворяющих (1).

Но так как лишь у половины элементов имеются квадратные корни, естественно ожидать (если бы  были случайными элементами поля), что количество -точек примерно вдвое меньше этого числа. Точнее, пусть  – квадратичный характер . Это – отображение, переводящее *x *  в 1 или -1 в зависимости от того, является или нет элемент 𝑥 квадратом элемента из (полагаем также (0) = 0). Например, если *q* – это простое число *р*, то (𝑥) =  называется символом Лежандра. В любом случае число решений 𝑦 **  уравнения  = 𝑢 равно 1 + (𝑢) и, значит, число решений уравнения (с учетом точки в бесконечности) равно

 (20)

Следует ожидать, что  одинаково часто принимает значения 1 и -1. Вычисление суммы очень похоже на «случайное блуждание», когда мы подбрасываем монету *q* раз, продвигаясь на шаг вперед, если выдал герб, и назад – если решка. Из теории вероятностей известно, что после *q* бросаний результат случайного блуждания оказывается на расстоянии порядка от исходного положения. Сумма  ведет себя в чем-то аналогично случайному блужданию. Точнее, удалось доказать, что она ограничена величиной . Этот результат – теорема Хассе.

**Теорема 6(Хассе).** Пусть *N* – число -точек на эллиптической кривой, определенной над . Тогда

. (21)

В дополнение к числу *N* элементов на эллиптической кривой над  нам бывает нужно знать строение этой абелевой группы. Она не обязательно циклическая, но можно показать, что она всегда является произведением двух циклических групп. Это означает, что группа изоморфна произведению *р*-примарных групп вида ℤ/, где произведение берется по всем простым делителям *N* (здесь ). Под типом абелевой группы -точек на 𝛦 мы понимаем список  – порядков циклических *р*-примарных сомножителей в упомянутом представлении в виде произведения (если  = 0, то опускаем). Найти тип не всегда легко.

**Пример 12.** Найти тип для кривой  над .

**Решение**. Находим сначала число точек *N*. Из свойств квадратичного характера  и (-1) = -1 следует, что в сумме (20) члены для 𝑥 и для -𝑥 взаимно уничтожаются: . Следовательно, *N* = *q* + 1 = 72. Далее, имеется в точности четыре точки порядка 2 (включая «бесконечную» точку 𝒪): они соответствуют корням многочлена  (см. упражнение 4а). Это означает, что 2-примарная часть группы имеет тип (4, 2) и, таким образом, тип группы – это (4, 2, 3, 3) или (4, 2, 9), в зависимости от того, равно 9 или 3 число точек порядка 3. Следовательно, остается выяснить, существует ли 9 точек порядка 3. Заметим, что условие 3*Р* = 𝒪 при *Р*  𝒪 эквивалентно условию 2*Р* = ±*Р*, т.е. тому, что *x*-координаты точек 2*Р* и *Р* одинаковы. Согласно (17) это означает, что , т.е. . Упрощая, получаем  Это уравнение имеет, самое большее, 4 корня в . Каждый корень может давать не более двух точек (при *у* = , если  есть квадрат по модулю 71), и если было бы 4 корня, то получилось бы 9 точек порядка 3 (включая точку 𝒪). В противном случае должно было бы быть меньше 9 точек порядка 3 (и, стало быть, в точности 3 таких точки). Но если корень 𝑥 биквадратного уравнения таков, что есть квадрат по модулю 71, то для другого его корня -𝑥 получаем, что  не есть квадрат. Значит, число точек порядка 3 не может быть равно 9 и потому тип группы – (4, 2, 9).

**Расширения конечных полей, гипотеза Вейля.**

Если эллиптическая кривая определена над , то она определена также над , *r* = 1,2,… и имеет смысл рассматривать -точки, т.е. решения (1) над расширениями поля. Отправляясь от поля как поля, над которым задана *Е*, определяем число  как число -точек на *Е* (таким образом,  есть число точек с координатами в нашем «основном поле»).

Для чисел  можно рассмотреть «производящий ряд» *Z*(*T*; *E*/) – формальный степенной ряд в ℚ[*T*]:

𝑍(𝑇, 𝐸/) = , (22)

где *Т* – неизвестная; обозначение *E*/ указывает эллиптическую кривую и поле, которое мы берем в качестве основного, а сумма в правой части берется по всем *r* = 1,2,…. Можно показать, что ряд справа (рассматриваемый как бесконечное произведение экспоненциальных степенных рядов ) имеет положительные целые коэффициенты. Этот степенной ряд называется *дзета-функцией* эллиптической кривой (над ) и представляет собой весьма важный объект, связанный с *Е*.

«Гипотеза Вейля» (ныне теорема Делиня, P. Deligne) в значительно более общем контексте (алгебраические многообразия произвольной размерности) утверждает, что дзета-функция имеет весьма специальный вид. В случае эллиптической кривой *E*/ Вейль (А. Weil) получил следующее утверждение:

**Теорема 7 (теорема Вейля для эллиптической кривой).** Дзета-функция есть рациональная функция от *Т* вида

𝑍(𝑇, 𝐸/) = , (23)

где от эллиптической кривой *Е* зависит лишь целое число 𝑎. Значение 𝑎 связано с числом *N* =  соотношением *N* = *q* + 1 - 𝑎. Кроме того, дискриминант квадратного трехчлена в числителе отрицателен (т.е. – теорема Хассе), таким образом, этот трехчлен имеет два комплексно сопряженных корня  и , оба по модулю равные  (точнее, корнями являются 1/ и 1/, а ,  — корни «возвратного» уравнения).

**Пример 13.** Легко вычисляется дзета-функция эллиптической кривой  над , так как имеется всего три -точки. Она равна . Таким образом, числа, обратные корням числителя – это . Отсюда следует формула

 (24)

**3амечание.** Если записать числитель (23) в виде  и затем взять производную от логарифмов обеих частей (заменяя левую часть по формуле (22), определяющей дзета-функцию) и сравнить коэффициенты при одинаковых степенях полученного ряда и исходного ряда, определяющего дзета-функцию, то нетрудно убедиться, что формула (23) эквивалентна последовательности соотношений

, *r* = 1,2,... (25)

Так как  и (=, наряду с 𝑎, определяются значением *N* =, то число точек над полем однозначно определяет число точек над любым его расширением. Таким образом, теорему Вейля для эллиптических кривых можно использовать, в частности, для нахождения числа точек над расширениями высокой степени.

**Краткий обзор способов построения кривых**

Соотношение(25) дает возможность по значению  вычислить значения  для всех . Величины =образуют так называемую последовательность Люкá и для их вычисления используются простые рекуррентные соотношения:



Отсюда следует самый простой способ построения эллиптической кривой и определения ее порядка.

Выберем небольшое конечное поле *GF* (2l) и в качестве базового конечного поля возьмем расширение этого небольшого поля степени *k*, т.е. базовое поле имеет вид *GF*(2m), *m=kl* для некоторого *k.* Для каждого допустимого значения *w* порядка кривой над *GF*(2l) вычислим величину  − порядок некоторой эллиптической кривой над полем *GF*(2m). Допустимые значения *w* определяются неравенством Хассе, . Перебор значений *w* продолжаем до тех пор, пока не найдем такое значение *N*, которое содержит большой простой делитель. Порядок эллиптической кривой в криптографических применениях должен удовлетворять также дополнительному условию, о котором речь пойдет ниже. Теперь перебором по парам (𝑥*,𝑦*), 𝑥, 𝑦0 остается найти эллиптическую кривую над малым полем, имеющую выбранный порядок *w*, число точек кривой над малым полем легко найти полным перебором.

**Пример 14.**

Построим эллиптическую кривую. Возьмем небольшое поле GF(28) и построим эллиптическую кривую над расширением этого небольшого поля степени *k*=23 т.е. над полем GF(2184). Область перебора в данном случае есть интервал (225,289), при *w*=230 находим

******,

******

Далее,

,

где



− простое число. Перебором находим, что порядок *w*=230 над небольшим полем имеет эллиптическая кривая



Следовательно, полученная эллиптическая кривая, если ее рассматривать над полем *GF*(2184), имеет порядок *N*, содержащий простой множитель *u* .

Этот метод позволяет строить эллиптические кривые только в расширениях малых полей, т.е. применим не ко всем полям, но главный его недостаток состоит в том, что он дает небольшое множество эллиптических кривых, Так, для 𝑚=168 вообще нет кривых, пригодных для криптографических применений. Однако этот метод вполне пригоден для получения начального набора эллиптических кривых для экспериментальных целей.

Второй метод − метод комплексного умножения, более универсален(но и более сложен). В этом методе существенно используется кольцо эндоморфизмов эллиптической кривой.

Третий метод построения эллиптических кривых по существу самый логичный, мы выбираем наугад эллиптическую кривую и вычисляем ее порядок до тех пор, пока не найдем кривую с нужными свойствами. Р. Схоф предложил полиномиальный алгоритм определения порядка произвольной эллиптической кривой над простым конечным полем нечетной характеристики.

Приведем еще два полезных утверждения о порядке эллиптической кривой над конечным полем.

**Теорема 8.** *Для порядка эллиптических кривых над полем* 𝐺𝐹(𝑞),

𝑞 = , *справедливы следующие утверждения*: *порядок имеет вид*

𝑞 + 1 – 𝑡, *где* 𝑡 *удовлетворяет одному из условий*

1. 𝑡 ≢ 0(mod 𝑝) *и*  ≤ 4𝑞,
2. 𝑛 *нечётно и либо* 𝑡 = 0, *либо* = 𝑝𝑞 *при* 𝑝 = 2, 3,
3. 𝑛 *чётно и либо* 𝑡 = 4𝑞, *либо* = 𝑞 *при* 𝑝 ≢ 1(mod 3), *либо* 𝑡 = 0 *при* 𝑝 ≢ 1(mod 4).

**Определение.** Если 𝑝 делит 𝑡, то кривая называется *суперсингулярной*, иначе она называется *несуперсингулярной*.

Из этой теоремы следует, что для суперсингулярных кривых = 0, 𝑞, 2𝑞, 3𝑞, 4𝑞. Структура групп суперсингулярных кривых описывается следующей теоремой.

**Теорема 9.** *Если* = 𝑞, 2𝑞, 3𝑞, *то группа циклическая*. *Если* = 4𝑞, *то* *группа изоморфна* *в случае* 𝑡 = , *или изоморфна* *в случае* 𝑡 = - . *Если* 𝑡 = 0, 𝑞 ≢ 3(mod 4), *то группа циклическая*. *Если* 𝑡 = 0, 𝑞 ≡ 3(mod 4), *то группа или циклическая или изоморфна* .

В заключение этого параграфа заметим, что существует много аналогий между группой -точек на эллиптической кривой и мультипликативной группой . Например, по теореме Хассе они имеют примерно одинаковое число элементов.

**Однако абелевы группы, которые строятся по эллиптическим кривым, имеют одно значительное преимущество, которое объясняет их ценность для криптографии: для одного и того же большого *q* существует богатый выбор различных эллиптических кривых с разными значениями *N*. Эллиптические кривые составляют богатый источник «естественно возникающих» конечных абелевых групп, и это открывает большие возможности для применения в криптографии.**

**УПРАЖНЕНИЯ к § 2.**

**1.** Пусть 𝐸 – эллиптическая кривая, определенная над ℂ, уравнение (1) которой имеет коэффициенты 𝑎, 𝑏 ∈ ℝ; тогда точки 𝐸 с вещественными координатами образуют подгруппу. Описать все возможные виды структуры такой подгруппы комплексной кривой 𝐸 (которая как группа изоморфна произведению окружности на себя). Привести пример для каждой из них.

**2.** Сколько точек 𝑃 порядка 𝑛 (т.е. таких, что 𝑛*P* = 𝒪) имеется на эллиптической кривой над ℂ? Сколько таких точек на эллиптической кривой над ℝ?

**3.** Привести пример эллиптической кривой над ℝ, имеющей в точности 2 точки порядка 2, и пример кривой, имеющей в точности 4 точки порядка 2.

**4.** Пусть *Р* – точка на эллиптической кривой над ℝ. Предположим, что *Р* не есть точка в бесконечности. Найти геометрическое условие, эквивалентное тому, что *Р* – точка порядка а) 2; б) 3; в) 4.

**5.** Каждая из следующих точек имеет конечный прядок на данной эллиптической кривой над ℚ*.* Найти в каждом случае порядок *P*.

a) *P* = (0, 16) на .

б) *P* =  на .

в) *P* = (3, 8) на .

г) *P* = (0, 0) на  .

**6.** Вывести формулы сложения, аналогичные (16)-(17), для эллиптических кривых над полем характеристики 2, 3 (см. уравнения (18),(19)).

**7.** Доказать, что число -точек на каждой из следующих эллиптических кривых равно *q* + 1:

а) , когда *q*  3 (mod 4);

б) , когда *q*  2 (mod 3) (*q* нечетно);

в) , когда *q*  2 (mod 3) (здесь *q* может быть четным).

**8.** Для всех степеней нечетных простых чисел до 27 включительно найти порядок и тип группы -точек на эллиптических кривых  и  (в последнем случае – при *р*  3). В некоторых случаях нужно будет проверить, сколько точек имеют порядок 3 или 4.

**9.** Пусть  и пусть эллиптическая кривая *E* над имеет уравнение :

а) Выразить координаты -*Р* и 2*Р* в терминах координат *Р*.

б) Показать, что при *q* = 16 каждая *Р* *Е* есть точка порядка 3.

в) Показать, что любая точка *Е* с координатами в фактически есть точка с координатами в . Далее с помощью теоремы Хассе при *q* = 4 и 16 определить число точек на кривой.

**10.** Вычислить дзета-функцию кривой  над для *р* = 2, 3, 5, 7, 11, 13. (сначала показать, что  = 1) Пусть *N*(*x*) =  обозначает норму комплексного числа. В терминах нормы найти простую формулу для .

**§ 3. Применение эллиптических кривых в задаче факторизации чисел.**

В этом параграфе мы опишем алгоритм разложения целых чисел на простые множители, основанный на арифметических свойствах эллиптических кривых над конечными полями. Алгоритм разработан Ленстрой.

Предварительно рассмотрим вопрос вычисления кратной точки на кривой и докажем одно вспомогательное утверждение.

**Кратные точки.** Рассмотрималгоритм вычисления точки 𝑘𝑃*.* Представим число 𝑘 в двоичном виде

𝑘 = + ⋅ 2 + ⋅ + … + ⋅ , = 0,1.

Далее, положим

= 𝑃,

= 2 = 2𝑃,  
 …………………

= = ,

Откуда

Таким образом, мы можем вычислить 𝑘𝑃 самое большее за шагов, каждый из которых представляет собой сложение точек на кривой.

**Пример 15**. Чтобы найти 100𝑃, представляем 100 в виде :

100 =

Далее,

.

Теперь

100𝑃 =

Мы нашли точку 100𝑃, произведя 6 удвоений и 2 сложения точек на кривой.

**Замечания.**

1. Приведенная оценка времени работы не является наилучшей, особенно для конечных полей характеристики *р* = 2. Нам, однако, достаточно этой оценки.

2. Если известно число *N* точек на эллиптической кривой *Е* и если *k* > *N*, то в силу равенства *NP* = 𝒪 мы можем заменить *k* его наименьшим неотрицательным вычетом по модулю *N* (*k* mod *N*)(напомним, что ). Рене Шуф (R. Schoof) предложил алгоритм, вычисляющий *N* за *O*() двоичных операций.

Докажем теперь свойство точек эллиптической кривой, необходимое для алгоритма Ленстры.

**Теорема 10.** *Пусть* *эллиптическая кривая задана уравнением*

(26)

*коэффициенты* 𝑎 *и* 𝑏 *которого - целые числа и пусть* 𝑃 = (𝑥, 𝑦)-*точка на этой кривой с рациональными координатами. Тогда* 𝑥 *и* 𝑦 *имеют вид*

𝑥 = , 𝑦 =

*где* 𝑚, 𝑛, 𝑒 – *целые числа*, 𝑒>0 *и* (𝑚, 𝑒) = (𝑛, 𝑒) = 1.

**Доказательство.**

Запишем рациональные числа 𝑥 и 𝑦 в виде несократимых дробей

𝑥 = , 𝑦 = ,

где 𝑀 > 0 и 𝑁 > 0. Подставляя 𝑥 и 𝑦 в уравнение кривой (26), получаем

или

(27)

Так как является делителем всех слагаемых в правой части этого равенства, то но (𝑛, 𝑁) = 1; следовательно,

Покажем теперь, что . Прежде всего, из равенства (27) непосредственно следует, что , а так как (𝑚, 𝑀) = 1, то . Используя этот факт и равенство (27), находим что т. е. что . И, наконец, ещё раз используя равенство (27), получаем, что , откуда .

Итак, мы показали, что и , поэтому . Кроме того, в процессе доказательства мы установили, что . Таким образом, если положить 𝑒 = , то│

.

Следовательно,

𝑥 = , 𝑦 = ,

что и требовалось доказать.

Теперь, основываясь на алгоритме вычисления кратной точки и на теореме , опишем факторизационный алгоритм Ленстры.

Прототипом алгоритма Ленстры является алгоритм Полларда. Алгоритм Полларда основан на том, что нетривиальные элементы в ℤ/𝑝ℤ образуют группу (ℤ/𝑝ℤ)∗ порядка 𝑝⎯1. Поэтому, если 𝑝⎯1│𝑘 , то в этой группе выполняется равенство =1.

Идея Ленстры состоит в том, чтобы заменить группу (ℤ/𝑝ℤ)∗ группой точек эллиптической кривой 𝐸(), а число 𝑎 –точкой 𝑃∈ 𝐸(). Как и в алгоритме Полларда, мы выбираем число 𝑘, являющееся произведением небольших простых чисел в небольших степенях. Если окажется, что число элементов в 𝐸() делит 𝑘, мы будем иметь в этой группе равенство 𝑘𝑃=𝒪*.* И точно так же, как в алгоритме Полларда, это равенство в общем случае позволит нам найти нетривиальный делитель числа 𝑛.

Опишем преимущество алгоритма Ленстры в сравнении с алгоритмом Полларда.

Если мы ограничимся только одной кривой 𝐸 с целыми коэффициентами и будем рассматривать её редукции по модулю различных простых чисел, то никакого преимущества по сравнению с алгоритмом Полларда мы не получим. В самом деле, для фиксированной 𝐸 мы достигнем успеха, если найдётся такой простой делитель 𝑝, 𝑁 является произведением небольших простых чисел. Эта ситуация вполне аналогична той, с которой мы встретились в алгоритме Полларда. Но если в алгоритме Полларда не удаётся быстро достичь успеха, его работа должна быть остановлена. В алгоритме Ленстры существуют дополнительные, очень широкие возможности продолжать работу: **имеется свобода в выборе** **новой эллиптической кривой.** Так как числа 𝑁 при фиксированном 𝑝 изменяются в достаточно широких пределах для различных кривых 𝐸, то в принципе можно надеяться во всех случаях достигнуть успеха.

Формально алгоритм Ленстры заключается в следующем.

**Шаг 1.** *Выбираем целые числа* 𝑏, , , *лежащие между* 1 *и* 𝑛.

**Шаг 2.** *Полагаем*

𝑐 = - - (mod 𝑛) (28)

*и рассматриваем кубическую кривую*

𝐸 : = + 𝑏𝑥 + 𝑐, 𝑏, 𝑐 ∈ ℤ (29)

*и точку* 𝑃 = (, ) *на ней*.

**Шаг 3.** *Вычисляем наибольший общий делитель*

, (30)

*т. е. проверяем, являются ли редукции кривой* 𝐸 *эллиптическими* ( – *это взятый с обратным знаком дискриминант многочлена*  + 𝑏𝑥 + 𝑐). *Если*  = 𝑛, *возвращаемся к началу и выбираем новое* 𝑏. *Если* 1 < < 𝑛, *получим нетривиальный делитель числа* 𝑛. *Если же*  = 1, *переходим к следующему шагу*.

**Шаг 4.** *Выбираем число* 𝑘, *являющееся произведение небольших*

*простых чисел в небольших степенях. Например*,

𝑘 = НОК,

*где* 𝑀- *некоторое натуральное число.*

**Шаг 5.** *Вычисляем*

𝑘𝑃 = .

**Шаг 6.** *Вычисляем* 𝐷 = . *Если* 1 < 𝐷 < 𝑛, *то* 𝐷 *является нетривиальным делителем числа* 𝑛. *Если* 𝐷 = 1, *либо возвращаемся к шагу* 4 *и увеличиваем* 𝑘, *либо возвращаемся к шагу* 1 *и выбираем новую кривую*. *Если* 𝐷 = 1, *возвращаемся к шагу* 4 *и уменьшаем* 𝑘.

В настоящее время существуют алгоритмы проверки натуральных чисел на простоту, использующие эллиптические кривые над конечными полями. Эта область теории эллиптических кривых бурно развивается и далека еще от завершения.

**Литературные указания.**

Материал первой главы изложен по источникам [1], [2], [3],[4[, [5]. Теорию эллиптических кривых с комплексным умножением можно изучить по руководству [4] . Современное , подробное изложение теории алгебраических кривых, в частности, эллиптических кривых, свойств кривых содержится в [12]. С алгоритмами проверки на простоту можно ознакомиться по книге [5].Для углубленного изучения теоретико-числовых алгоритмов полезной является книга [13].

**Глава 2. Криптосистемы на эллиптических кривых**

Большинство продуктов и стандартов, в которых для шифрования и проверки подлинности применяются методы криптографии с открытым ключом, базируется на алгоритме RSA. Однако число битов ключа, необходимое для надежной защиты данных при использовании RSA за последние годы резко возросло, что обусловило соответствующий рост загрузки систем, использующих RSA. Криптография на основе эллиптических кривых (ECC – Elliptic Curve Cryptography) – появившийся сравнительно недавно подход, способный конкурировать с RSA.

Привлекательность подхода на основе эллиптических кривых в сравнении с RSA заключается в том, что с использованием эллиптических кривых обеспечивается эквивалентный уровень защиты при значительно меньшем числе разрядов, вследствие чего уменьшается загрузка процессора. В то же время, степень доверия к методам криптографии с использованием эллиптических кривых еще не настолько высока, как степень доверия к RSA.

Операция сложения в криптографии на основе эллиптических кривых является аналогом операции умножения по модулю простого числа в RSA, а многократное повторное сложение – аналогом возведенияв степень. Чтобы построить криптографическую систему, используя эллиптические кривые, нужно найти «трудную проблему», соответствующую разложению на множители произведения двух простых чисел или дискретному логарифмированию.

Цель этого параграфа – описание построения криптографических систем с открытым ключом, основанных на конечной абелевой группе точек эллиптической кривой, определенной над . Прежде чем описывать криптосистемы, нужно обсудить некоторые вспомогательные понятия.

**§1. Вспомогательные сведения**

**Представление открытого текста.**

Мы намереваемся кодировать наши открытые тексты точками некоторой заданной эллиптической кривой *Е*, определенной над конечным полем .Мы хотим это осуществить простым и систематическим способом так, чтобы открытый текст 𝑚(который можно рассматривать как целое число из некоторого интервала) можно было легко прочитать, зная координаты соответствующей точки . Заметим, что это «кодирование» – не то же самое, что засекречивание. Позднее мы будем рассматривать способы шифрования точек  открытого текста. Однако законный пользователь системы должен быть в состоянии восстановить 𝑚 после расшифрования точки шифртекста.

Следует сделать два замечания. Во-первых, не известно детерминированного полиномиального (по log *q*) алгоритма для выписывания большого числа точек произвольной эллиптической кривой *E* над .В примере 10 мы выписали все точки, проведя полный перебор всех возможных вариантов, но это невозможно(по крайней мере, за разумное время) для *p* порядка 2 160,а именно таков должен быть размер *p* для обеспечения надежности при формировании цифровой подписи. Однако, как мы увидим далее, существуют вероятностные алгоритмы с малой вероятностью неудачи. Во-вторых, порождать случайные точки на *Е* недостаточно: чтобы закодировать большое число возможных сообщений 𝑚, необходим какой-то систематический способ порождения точек, которые были бы связаны с 𝑚 определенным образом, например, чтобы *x*-координата имела с 𝑚 простую связь.

Приведем один возможный вероятностный метод представления открытых текстов как точек на эллиптической кривой *Е*, определенной над , где  предполагается большим (и нечетным – см. упражнение 8 к § 1 Главы 1). Пусть  – достаточно большое целое число, настолько, что можно считать допустимым, если попытка представить в нужном нам виде элемент («слово») открытого текста 𝑚 оказывается неудачной в одном случае из ; практически достаточно = 30 или, в крайнем случае,  = 50. Пусть элементы нашего сообщения 𝑚 – целые числа, . Предположим также, что выбранное нами конечное поле имеет *q* элементов, *q* > *М*. Записываем целые числа от 1 до *М* в виде , где  и устанавливаем взаимно однозначное соответствие между такими числами и некоторым множеством элементов из . Например, можно записать такое число как *r*-значное числе в *р*-ичной системе счисления и, отождествляя цифры в этой записи с элементами , рассматривать их как коэффициенты многочлена степени не выше *r* - 1 над , соответствующего элементу поля . Таким образом, числу  (здесь ) ставится в соответствие многочлен который, будучи рассмотрен по модулю некоторого фиксированного неприводимого многочлена степени *r* над , дает элемент .

Итак, при данном 𝑚 для каждого *j* = 1,2,…, 𝑘 мы получаем элемент 𝑥 из , соответствующий 𝑚𝑘 + 𝑗. Для такого 𝑥 вычисляем правую часть уравнения



и пытаемся найти квадратный корень из . Извлечение квадратного корня в поле – это отдельная интересная задача, которой уделено достаточное внимание в соответствующей литературе (см. список литературы).

Если мы находим такое 𝑦, что , то берем . Если  не оказывается квадратом, то увеличиваем *j* на 1 и повторяем попытку с соответствующим значением 𝑥. Если мы находим 𝑥, для которого  – квадрат прежде, чем *j* превысит , то мы можем восстановить 𝑚 по известной точке (𝑥, 𝑦) с помощью формулы , где  – целое число, соответствующее 𝑥 при установленном взаимно однозначном соответствии между целыми числами и элементами . Так как  – квадрат приблизительно в 50% случаев(точнее, вероятность того, что  есть квадрат, фактически равна *N*/(2*q*), однако *N*/(2*q*) очень близко к 1/2) , то вероятность того, что метод не приведет к результату и мы не найдем точки  с *x*-координатой, соответствующей целому числу  между  и , равна примерно .

Настоящее пособие содержит индивидуальные задания. Для их выполнения выбрана кривая , т.е. (mod 751). Для 𝑝=751 нетрудно найти все точки кривой. Некоторым точкам этой кривой поставлены в соответствие буквы русского алфавита , латинского алфавита, а также специальные знаки. Это—пример другого подхода к кодированию.

**Дискретный логарифм на *Е*.**

**Определение.** Пусть *Е* – эллиптическая кривая над , и *В* – точка на *Е*. Задачей дискретного логарифмирования на *Е* (с основанием 𝑃) называется задача нахождения для данной точки 𝑄  *Е* такого целого числа 𝑛  *Z* (если оно существует), что 𝑛𝑃 = 𝑄.

Стойкость криптографических систем, определенных на эллиптических кривых, определяется сложностью решения задачи дискретного логарифмирования в группе ее точек, т.е. сложностью решения уравнения  относительно *n*, где точки *P* и *Q* принадлежат одной циклической подгруппе. Как и в любой конечной абелевой группе, эту задачу можно решить за  элементарных операций. В этой группе невозможно построить субэкспоненциальные алгоритмы решения этой задачи на тех принципах, использование которых привело к успеху в случае конечных полей.

Вполне возможно, что задача дискретного логарифмирования на эллиптической кривой окажется более трудной для решения, чем задача дискретного логарифмирования в конечных полях. Наиболее сильные методы, разработанные для конечных полей, по-видимому, не работают в случае эллиптических кривых. Это обстоятельство особенно отчетливо проявляется в случае полей характеристики 2. Специальные методы решения задачи дискретного логарифмирования в позволяют сравнительно легко вычислять дискретные логарифмы и, следовательно, вскрывать соответствующие криптосистемы, если *r* не выбрано очень большим. Аналогичные системы, использующие эллиптические кривые над (см. ниже), судя по всему, **являются столь же надежными при значительно меньших значениях *r***.

До 1990 г. единственными известными алгоритмами дискретного логарифмирования на эллиптических кривых были те, которые работают в любой группе и не используют особенности ее строения. Эти алгоритмы с экспоненциальным временем работы применимы к случаям, когда порядок группы делится на большое простое число. Однако в 1993 году Менезес (Menezes), Окамото (Okanoto) и Вэнстон (Vanstone) предложили новый подход к задаче дискретного логарифмирования на эллиптической кривой *Е*, определенной над . показали, что эта задача сводится к задаче дискретного логарифмирования в некотором расширении  исходного конечного поля.  т.е. за полиномиальное время можно построить соответствующий изоморфизм. Метод Менезеса--Окамото- Вэнстоуна основан на том, что так называемое спаривание Вейля позволяет изоморфно вложить группу точек простого порядка 𝑢 (равного большому простому делителю порядка кривой *N*) в мультипликативную группу расширения основного поля. Необходимое условие для такого вложения, очевидно, следующее: 𝑢 должно делить порядок мультипликативной группы поля вложения, т.е. для некоторого *k* простое число𝑢 должно делить . Это и есть условие Менезеса -Окамото- Вэнстона. В [17] показано, что это условие фактически и достаточное. Это условие легко проверяется, поэтому всегда можно выбрать кривую с произвольно большим *k* и, следовательно, исключить применимость субэкспоненциального алгоритма для решения задачи дискретного логарифмирования на данной кривой. Заметим, что это верно только для несуперсингулярных кривых. Именно по этой причине суперсингулярные кривые непригодны для криптографических применений. Следует упомянуть еще один эффективный алгоритм решения задачи дискретного логарифмирования на кривых с следом 1, предложенный Н.Смартом [18]). В этом случае порядок кривой равен порядку основного поля и с помощью аппарата формальных групп исходная задача дискретного логарифмирования сводится к вычислению

*p*-адического логарифма, т.е. очень простой задаче. Таких кривых очень мало, кроме того, легко избежать применения таких групп. Поэтому этот алгоритм не представляет практической угрозы для криптографических систем на эллиптических кривых. Следовательно, для решения задачи дискретного логарифмирования на эллиптических кривых известны только алгоритмы экспоненциальной сложности. Именно это свойство делает их столь привлекательными для криптографических применений, в частности, позволяет использовать ключи небольшого размера.

Таким образом, основные преимущества криптосистем на эллиптических кривых заключаются в том, что неизвестны субэкспоненциальные алгоритмы вскрытия этих систем, если в них не используются суперсингулярные кривые, а также кривые, порядки которых делятся на большое простое число.

**§ 2. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой**

Теперь мы опишем аналоги некоторых широко распространенных систем с открытым ключом, основанные на задаче дискретного логарифмирования на эллиптической кривой, определенной над конечным полем .

**Аналог ключевого обмена Диффи-Хеллмана.**

Предположим, что абоненты А и Б хотят договориться о ключе, которым будут впоследствии пользоваться в некоторой классической криптосистеме. Прежде всего, они открыто выбирают какое-либо конечное поле и какую-либо эллиптическую кривую *Е* над ним. Их ключ строится по случайной точке *Р* на этой эллиптической кривой. Если у них есть случайная точка *Р*, то, например, ее *x*-координата дает случайный элемент , который можно затем преобразовать в *r*-разрядное целое число в *р*-ичной системе счисления (где ), и это число может служить ключом в их классической криптосистеме . Они должны выбрать точку *Р* так, чтобы все их сообщения друг другу были открытыми и все же никто, кроме них двоих, ничего бы не знал о *Р*.

Абоненты (пользователи) А и Б первым делом открыто выбирают точку *В*  *Е* в качестве «основания»; *B* играет ту же роль, что образующий *q* в системе Диффи-Хеллмана для конечных полей. Мы, однако, не требуем, чтобы *B* была образующим элементом в группе точек кривой *E*. Эта группа может и не быть циклической. Даже если она циклическая, можно не тратить время на проверку того, что *В* – образующий элемент (или даже на нахождение общего числа *N* точек, которое не понадобится в последующем). Нам хотелось бы, чтобы порожденная *В* подгруппа была большой, предпочтительно того же порядка величины, что и сама *Е*. Позже мы рассмотрим этот вопрос. Пока что предположим, что *В* – взятая открыто точка на *Е* весьма большого порядка (равного либо *N*, либо большому делителю *N*).

Чтобы образовать ключ, А вначале случайным образом выбирает целое число 𝑎, сравнимое по порядку величины с *q* (которое близко к *N*); это число он держит в секрете. Он вычисляет 𝑎𝐵  *Е* и передает эту точку открыто. Абонент Б делает то же самое: он выбирает случайно *b* и открыто передает 𝑏𝐵  *Е*. Тогда используемый ими секретный ключ – это *Р* = 𝑎𝑏𝐵  *Е*. Оба пользователя могут вычислить этот ключ. Например, А знает 𝑏𝐵(точка была передана открыто) и свое собственное секретное 𝑎*.* Однако любая третья сторона знает лишь 𝑎𝐵 и 𝑏𝐵. Кроме решения задачи дискретного логарифмирования – нахождения 𝑎 по 𝐵 и 𝑎𝐵 (или нахождения 𝑏 по 𝐵и 𝑏𝐵) по-видимому, нет способа найти 𝑎𝑏𝐵, зная лишь 𝑎𝐵 и 𝑏𝐵.

**Пример 16.**

Возьмем *р* = 211,  (что соответствует кривой ) и *B* = (2, 2). Можно подсчитать, что 241*B* = 𝒪. Личным ключом пользователя А является = 121, поэтому открытым ключом А будет  = 121(2, 2) = (115, 48). Личным ключом пользователя Б является  = 203, поэтому его открытым ключом будет 203(2, 2) = (130, 203). Общим секретным ключом является 121(130, 203) = 203(115, 48) = (161,169).

общий секретный ключ представляет собой пару чисел. Если этот ключ предполагается использовать в качестве сеансового ключа для традиционного шифрования, то из этой пары чисел необходимо генерировать одно подходящее значение. Можно, например, использовать просто координату 𝑥 или некоторую простую функцию от 𝑥.

**Аналог системы Мэсси-Омуры.**

Как и в случае конечного поля, это криптосистема с открытым ключом для передачи элементов сообщения 𝑚, которые мы теперь предположим представленными точками  фиксированной (и не скрываемой) эллиптической кривой *Е* над (*q* берется большим). Предполагается также, что общее число *N* точек на *Е* вычислено и не составляет секрета. Каждый пользователь системы секретно выбирает такое целое случайное число *е* между 1 и *N*, что НОД(*e*, *N*) = 1. Используя алгоритм Евклида, он находит затем обратное  к числу *е* по модулю *N*, т.е. такое целое число *d*, что *de*  1(mod N). Если А хочет послать Б сообщение , то он сначала посылает ему точку  (индекс А указывает на пользователя А). Это ничего не говорит Б, который, не зная ни , ни, , не может восстановить . Однако, не придавая этому значения, он умножает ее на свое  и посылает обратно А. На третьем шаге А должен частично раскрыть свое сообщение, умножив  на . Так как 𝑁 = 𝒪 и = 1(mod *N*), при этом получается точка , которую А возвращает Б. Тот может теперь прочитать сообщение, умножив точку  на .

Заметим, что злоумышленник может узнать ,  и  Если бы он умел решать задачу дискретного логарифмирования на *Е*, то он мог бы определить  по первым двум точкам, вычислить = (mod *N*) и =.

**Аналог системы Эль-Гамаля.**

Это другая криптосистема с открытым ключом для передачи сообщений . Как и в описанной выше системе ключевого обмена, мы исходим из данных несекретных:

а) конечного поля ;

б) определенной над ним эллиптической кривой *Е*;

в) точки-«основания» *В* на ней (знать общее число *N* точек на *Е* не нужно).

Каждый из пользователей выбирает случайное целое число 𝑎, которое держит в секрете, затем находит и делает общедоступной точку 𝑎𝐵.

Чтобы послать Б сообщение , А выбирает случайно целое число *k* и посылает пару точек {*kB*,  + *k**В*} (где *В* — открытый ключ Б). Чтобы прочитать сообщение, Б умножает первую точку из полученной пары на свое секретное число  и вычитает результат умножения из второй точки:

 + *k*(*В*) – (*kB*) = .

Таким образом, А посылает замаскированное  вместе с «подсказкой» 𝑘𝐵, при помощи которой можно снять «маску» *k**В*, если знать секретное число . Злоумышленник, который умеет решать задачу дискретного логарифмирования на *Е*, может, конечно, найти  зная *В* и *В*.

**Пример 17.**

Рассмотрим случай *р* = 751, (-1,188) (что соответствует кривой  и G = (0, 376)). Предположим, что пользователь А собирается отправить пользователю Б сообщение, которое кодируется эллиптической точкой  = (562,201), и что пользователь А выбирает случайное число k = 386. Открытым ключом Б является  = (201,5). Мы имеем 386(0,376) = (676,558) и (562,201) + 386(201, 5) = (385, 328). Таким образом, пользователь А должен послать шифрованный текст {(676, 558), (385, 328)}.

**Выбор кривой и точки.**

Существуют различные способы выбора эллиптической кривой и (в системах Диффи-Хеллмана и Эль-Гамаля) точки *В* на ней.

**1) Случайный выбор (*Е*, *В*).** Взяв какое-либо большое конечное поле , можно следующим образом осуществить одновременный выбор *Е* и *В* = (*x*, *у*)  *Е*. Будем предполагать, что характеристика *р* поля больше 3, так что эллиптическая кривая задана уравнением (1) из § 1; при *q* =  или  нетрудно сделать очевидные изменения . Выбираем сначала случайным образом три элемента из в качестве 𝑥, 𝑦, 𝑎. Далее полагаем . Убеждаемся в том, что кубический многочлен  не имеет кратных корней, что равносильно проверке условия . Если это условие не выполняется, берем другую случайную тройку 𝑥, 𝑦, 𝑎. Полагаем *В* = (𝑥, 𝑦). Тогда *В* – точка на эллиптической кривой .

Число *N* точек кривой можно найти несколькими способами. Первый полиномиальный алгоритм для вычисления 𝑁(*Е)*, построенный Рене Шуфом (Rene Schoof), является даже детерминированным. Он основывается на нахождении значения 𝑁(*Е*) по модулю *l* для всех простых чисел *l*, меньших некоторой границы. Для этого анализируется действие автоморфизма Фробениуса (отображения в *р*-ю степень) на точках порядка *l*.

В статье Шуфа оценка времени работы была фактически *O*(), т. е. хотя и полиномиальной, однако быстро растущей. Вначале казалось, что алгоритм не имеет практического значения. Однако с тех пор многие пытались повысить скорость алгоритма Шуфа: Миллер (V. Miller), Элкис (N. Elkis). Бухман (J. Buchman), Мюллер (V. Muller), Менезес (A. Menezes), Чарлап (L. Charlap), Коули (R. Coley) и Роббинс (D.Robbins). Кроме того. Эткин (А.О.L. Atkin) разработал другой метод, который, хотя и не гарантирует полиномиального времени работы, на практике дает весьма удовлетворительные результаты. В результате всех этих усилий стало возможным вычислять порядок произвольной эллиптической кривой над , если *q* – степень простого числа, записываемая 50 или даже 100 знаками. Более подробно это обсуждается в главе 3 настоящего пособия. Некоторые методы нахождения числа точек на эллиптической кривой рассматриваются в работах из приведенного в конце пособия списка литературы.

Следует также отметить, что хотя для реализации систем Диффи-Хеллмана или Эль-Гамаля знать *N* не нужно, на практике желательно быть уверенным в их надежности, которая зависит от того, имеет ли *N* большой простой делитель. Если *N* есть произведение малых простых чисел, то для решения задачи дискретного логарифмирования можно использовать метод Полига-Силвера-Хеллмана. Заметим, что метод Полига-Силвера-Хеллмана решает задачу дискретного логарифмирования в любой конечной абелевой группе (в отличие от алгоритма вычисления индекса, который зависит от особенностей ). Таким образом, нужно знать, что *N* не есть произведение малых простых чисел и не похоже, что это можно узнать, если не найти фактически значение *N*.

**2) Редукция глобальной пары (*Е*, *В*) по модулю *р*.** Упомянем теперь второй способ нахождения пары, состоящей из эллиптической кривой и точки на ней. Выберем сначала раз и навсегда «глобальную» эллиптическую кривую и точку бесконечного порядка на ней. Итак, пусть *Е* – эллиптическая кривая, определенная над полем рациональных чисел (или, для большей общности, можно было бы использовать эллиптическую кривую, определенную над некоторым числовым полем), и *В* – точка бесконечного порядка на *Е*.

**Пример 18.** Точка *В* = (0, 0) является точкой бесконечного порядка на эллиптической кривой *Е*:  и фактически порождает всю группу рациональных точек на *Е*.

**Пример 19.** Точка *В* = (0, 0) является точкой бесконечного порядка на *Е*:  и порождает всю группу рациональных точек.

Далее, мы выбираем большое простое число *р* (или, если наша эллиптическая кривая определена над расширением 𝕂 поля ℚ, выбираем некоторый простой идеал в 𝕂) и рассматриваем редукцию *Е* и *В* по модулю *р*. Точнее, для всех *р*, за исключением нескольких малых простых чисел, коэффициенты в уравнении для *Е* имеют взаимно простые с *р* знаменатели и, следовательно, могут рассматриваться как коэффициенты в уравнении по модулю *р*. Если сделать замену переменных, приведя полученное уравнение над к виду  то кубический многочлен в главой части не будет иметь кратных корней (за исключением нескольких малых простых *р*) и дает поэтому эллиптическую кривую над (которую мы будем обозначать *Е*(mod *p*)). Координаты точки *В*, будучи также приведенными по модулю *р*, дают точку на эллиптической кривой *Е*(mod *p*), которую мы будем обозначать *В*(mod *p*).

При использовании этого второго способа мы раз и навсегда фиксируем *Е* и *В* и за счет этого получаем много различных возможностей посредством изменения простого *р*.

**Порядок точки *В*.**

С какой вероятностью «случайная» точка *В* на «случайной» эллиптической кривой оказывается порождающим элементом? Или, в случае нашего второго метода выбора (*Е*, *В*), какова вероятность того, что (для случайного *р*) точка *В* при редукции по модулю дает образующий элемент кривой *Е*(mod *p*)? Этот вопрос близок к следующему вопросу о мультипликативных группах конечных полей: пусть целое *b* фиксировано, а простое *р* случайно; какова вероятность того, что *b* – образующий элемент в ? Вопрос изучался как для конечных полей, так и для эллиптических кривых.

Как упоминалось выше, описанные криптосистемы могут быть надежными даже если точка *В* не является порождающим элементом Фактически нужно, чтобы в циклической группе, порождаемой *В*, задача дискретного логарифмирования не была эффективно разрешима. Это будет так (т.е. все известные методы решения задачи дискретного логарифмирования в произвольной абелевой группе оказываются слишком медленными), если порядок *B* делится на очень большое простое число, скажем, имеющее порядок величины, близкий к *N*.

Один из способов гарантировать, что наш выбор *B* является надлежащим (а фактически, что *B* порождает эллиптическую кривую) – это взять такую эллиптическую кривую и такое конечное поле, чтобы число точек *N* было простым чистом. Тогда всякая точка *В*  𝒪 будет порождающим элементом. Если использовать первый из описанных выше методов, то при фиксированном можно продолжать выбор пар (*Е*, *В*), пока не найдется такая, для которой число точек на *Е* есть простое число (что можно определить одним из известных тестов на простоту). Если применять второй метод, то для фиксированной глобальной эллиптической кривой *Е* над ℚ можно продолжать выбирать простые *р*, пока не найдем кривую *Е*(mod *p*), число точек на которой простое. Как долго нам придется ждать? Этот вопрос аналогичен следующему вопросу о группах : является ли (*р* – 1)/2 простым числом, т.е. верно ли, что любой элемент, отличный от ±1, – либо порождающий, либо квадрат порождающего элемента? Ни для эллиптических кривых, ни для конечных полей вопрос пока не получил явного ответа, однако в обоих случаях предполагается, что вероятность выбора *р* с требующимся свойством есть O(1/)

**3амечание**. Для того чтобы *Е*(mod *p*) имела простой порядок *N* при большом *р*, надо выбирать *Е* так, чтобы она имела тривиальное кручение, т.е. чтобы на ней не было точек конечного порядка, кроме 𝒪. В противном случае *N* будет делиться на порядок периодической подгруппы.

**Безопасность криптографии с использованием эллиптических кривых.**

Безопасность, обеспечиваемая криптографическим подходом на основе эллиптических кривых, зависит от того, насколько трудной для решения оказывается задача определения *k* по данным *kP* и *Р*. Наиболее быстрым из известных на сегодня методов логарифмирования на эллиптический кривой является так называемый -метод Полларда (Pollard). В таблице 8 сравнивается эффективность этого метода и метода разложения на простые множители с помощью решета в поле чисел общего вида. Таким образом, по сравнению с RSA в случае применения методов криптографии на основе эллиптических кривых примерно тот же уровень защиты достигается со значительно меньшими значениями длины ключей.

К тому же при равных длинах ключей вычислительные усилия, требуемые при использовании RSA и криптографии на основе эллиптических, кривых, не сильно различаются. Таким образом, в сравнении с RSA при равных уровнях защиты явное вычислительное преимущество принадлежит криптографии на основе эллиптических кривых с более короткой длиной ключа.

**Таблица 8.**

Вычислительные усилия, необходимые для криптоанализа

при использовании эллиптических кривых и RSA

|  |  |
| --- | --- |
| Размер ключа | MIPS-годы |
| 150 |  |
| 205 |  |
| 234 |  |

**а)** Логарифмирование на эллиптической кривой с помощью -метода Полларда (ECC)

|  |  |
| --- | --- |
| Размер ключа | MIPS-годы |
| 512 |  |
| 768 |  |
| 1024 |  |
| 1280 |  |
| 1536 |  |
| 2048 |  |

**б)** Разложение на множители в целых числах

с помощью метода решета в поле чисел общего вида (RSA)

**§ 3. Алгоритм цифровой подписи, основанный**

**на группе точек эллиптической кривой**

**Электронная цифровая подпись (ЭЦП).**

Цифровая подпись для сообщения является числом, зависящим от самого сообщения и от секретного, известного только подписывающему субъекту ключа. При этом подпись должна быть легко проверяемой без знания секретного ключа. При возникновении спорной ситуации, связанной с отказом подписавшего от факта подписи им некоторого сообщения либо с попыткой подделки подписи, третья независимая сторона (арбитр) должна иметь возможность разрешить спор.

Применение ЭЦП позволяет решить следующие задачи:

* осуществить аутентификацию источника сообщения;
* установить целостность сообщения;
* обеспечить невозможность отказа от факта подписи конкретного сообщения.

В настоящее время используются различные схемы ЭЦП. Их можно разделить на три класса:

* схемы на основе симметричных систем шифрования;
* схемы на основе систем шифрования с открытыми ключами;
* схемы со специально разработанными алгоритмами вычисления и проверки подписи.

Замечание. Распространенной практикой является формирование ЭЦП не для самого сообщения, а для его хеш-образа при соответствующем выборе хеш-функции.

**Цифровая подпись на эллиптических кривых.**

В качестве международного стандарта принят американский алгоритм цифровой подписи на эллиптических кривых (ECDSA). В этом стандарте используются эллиптические кривые над полем характеристики 2. Однако криптографически стойких кривых над полем такой характеристики сравнительно мало. Поэтому мы рассмотрим ЭЦП на эллиптических кривых, заданных над полем большей характеристики.

**Замечание.** В России официально принят стандарт ЭЦП на эллиптических кривых над полем большей характеристики – ГОСТ 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (текст стандарта приведен в Приложении 1).

Выбор кривой и точки на ней подразумевает решение ряда вспомогательных задач. Прежде всего, это подсчет количества точек на кривой. Если *N* – количество точек на 𝐸(, то должны выполняться следующие условия:



Таким образом, чтобы отсеять лишние числа из интервала , можно проверять условие (2) для разных точек *G*. Единственное оставшееся число и будет искомым порядком кривой.

**Замечание**. Существует несколько методов оптимизации нахождения порядка кривой, например, метод больших-малых шагов, метод Шуфа. Познакомиться с ними можно по книгам, приведенным в списке литературы.

Для получения криптографически стойкой системы ЭЦП должны выполняться следующие условия:

1. Порядок точки *G*, используемой в системе ЭЦП, должен быть простым числом *n*, .
2.  и , где *N* – порядок кривой.
3.  для всех , где *C* настолько велико, что вычислить дискретный логарифм в за приемлемое время невозможно.

**Замечание.** В настоящее время значение *C* = 20 считается достаточным.

Возможный способ защититься от известных атак и от возможных атак для специальных классов кривых, которые могут быть обнаружены в будущем, – выбирать кривую *E* случайным образом так, чтобы выполнялись указанные условия.

После того, как порядок *N* кривой определен, требуется найти большой простой делитель *n* порядка кривой. Такой делитель может не существовать, и тогда потребуется повторять процедуру выбора кривой до тех пор, пока не будут выполнены все требуемые условия. Поиск числа n может потребовать как разложения на множители числа *N*, так и доказательства простоты числа *n*.

Точку *G* можно выбрать следующим образом. Найдем случайную точку 𝐺′∈𝐸() и вычислим . Если , то требуемая точка найдена, если же , то выбираем другую точку .

Описанные параметры могут быть общими для всех пользователей. Для генерации и проверки подписи требуются еще и индивидуальные параметры пользователя – это секретный и открытый ключи. Ключ подписи (секретный ключ) – это случайное число *d*, . Ключ проверки подписи (открытый ключ) – это точка эллиптической кривой . Алгоритм ЭЦП также использует хеш-функцию, обозначаемую *h*.

**Генерация подписи.**

Входные данные: сообщение *m*, исходные параметры и ключ подписи. Выходные данные: подпись .

Алгоритм:

1. Выбрать случайное число *k* в интервале .
2. Вычислить .
3. Вычислить .
4. Если , то вернуться к шагу 1.
5. Вычислить .
6. Вычислить .
7. Вычислить .
8. Если , то вернуться к шагу 1.
9. Вывести пару  – подпись к *m*.

Замечания.

1. При  результат вычисления *s* не зависит от секретного ключа *d*.

2. При  необходимого для проверки подписи числа  не существует.

3. В качестве хеш-функции *h* на шаге 6 в стандартах ANSI X9F1 и IEEE P1363 используется SHA-1, в российском стандарте ГОСТ Р 34.10-2001 – хеширование по стандарту ГОСТ Р 34.11-94.

**Проверка подписи.**

Входные данные: сообщение *m*, исходные параметры, ключ проверки подписи и подпись к *m*. Выходные данные: заключение о подлинности или фальсификации подписи.

Алгоритм:

1. Если хотя бы одно из условий ,  нарушается, то подпись фальшивая и работа алгоритма закончена.
2. Вычислить .
3. Вычислить .
4. Вычислить .
5. Вычислить .
6. Вычислить .
7. Если , то подпись действительная, иначе подпись фальшивая.

Доказательство корректности алгоритма генерации и алгоритма проверки подписи очень простое и предоставляется в качестве упражнения.

**Пример 20.**

Построение системы цифровой подписи. Используем построенную ранее эллиптическую кривую над конечным полем GF(2184), ее порядок равен 24519928653854221733733552425551231120507846775650841870

и в группе точек этой эллиптической кривой существует циклическая подгруппа простого порядка 2098301128811779764490989552582298324221657814667. Нетрудно убедиться, что число *u* удовлетворяет условию Менезеса-Окамото-Вэнстоуна и поэтому эту кривую можно использовать в криптографических алгоритмах. Легко проверить, что точка 𝐺=(8718530218176903146207227181110236173128144216155151198161,

2618723313241163311561151819363208871622011861361892123221245)

имеет порядок *u*. Возьмем эту точку в качестве порождающей точки циклической подгруппы. Осталось выбрать секретный ключ цифровой подписи 𝑑=639976254049691330438880136087803025472585373106

и вычислить открытый ключ

*Q*=𝑑*P*=(2012355114217111017775249223891566918510915221922014271635084,

67182421615615694798118212159190631191991922031851725515671).

Система цифровой подписи построена. Заметим, что стойкость этой системы эквивалентна стойкости цифровой подписи в простом поле с ключом, размер которого равен 1200 битам.

Примеры вычисления подписи и проверки подписи даны в разделе ``Индивидуальные задания``.

**Литературные указания к Главе 2.**

Основная часть представленного материала содержится в руководствах [1], [2],[3] ,[6]. Для дальнейшего изучения затронутых вопросов можно рекомендовать [7], [8], [9].

**Глава 3**

**Аспекты практической реализации криптографических алгоритмов на эллиптических кривых**

**§1. Эффективная реализация элементарных операций.**

В этом разделе мы рассмотрим основной подход, обычно необходимый для эффективной реализации операций на эллиптической кривой. Как уже говорилось, вычисление кратной точки *kP* (*k* – большое число) осуществляется с помощью тех же методов, которые используются для возведения в степень по модулю (умножение в них заменяет­ся сложением точек). Здесь для конкретности мы все же опишем наиболее простой алгоритм, использующий разложение *k* по степеням числа 2 (то есть его побитовое представление). В литературе описаны более эффективные методы возведения в степень, которые с успехом могут быть применены и для вычисления композиций на эллиптических кривых. Эти методы обычно дают несущественный выигрыш во времени (порядка 25%), и их описание выходит за рамки нашей книги.

Алгоритм 1. Вычисление кратной точки *kP*.

ВХОД: Точка *P*, число (двоичное представление числа *k*).

ВЫХОД:Q = *kР*.

Шаг 1. *Q* ← *O*;

Шаг 2. FOR i = DO

Q ← 2*Q* ;

IF THEN *Q* ← *Q* +*P* END;

END;

Шаг 3. RETURN*Q*.

Данный алгоритм требует не болееtсложений и *t* удвоений точек (в среднемt удвоений и *t*/2 сложений).

**Пример 1**. Проиллюстрируем работу алгоритма на при­мере вычисления точки 29*Р*. Здесь 29 = (11101)2, t= 5. Покажем, что происходит на каждой итерации цикла алгоритма:

[*i* = 5 *m*5 = 1] : *Q* ← *O* , *Q* ← *Q* +*P = P* ;

[*i* = 4*m*4 = 1] : *Q* ← 2*Q =* 2*P* , *Q* ← *Q* +*P =* 3*P* ;

[*i* = 3*m*3 = 1] : *Q* ← 2*Q =* 6*P* , *Q* ← *Q* +*P =* 7*P* ;

[*i* = 2*m*2 = 0] : *Q* ← 2*Q =* 14*P* ;

[*i* = 1*m*1 = 1] : *Q* ← 2*Q =* 28*P*; *Q* ← *Q*+*P =* 29*P*.

Кратная точка вычислена с применением 5 умножений и 4 сложений точек.

Напомним, что в этом алгоритме сумма точек , где вычисляется с помощью формул:

Удвоенная точка вычисляется с помощью формул:

Говорят, что при вычислениях по данным формулам испо­льзуется аффинное представление для точек, т.е. точка P представлена в виде. Точка в бесконечности 𝒪 не имеет такого представления. Фактически в алгоритме 1 она является просто «флажком», показывающим, что нужно пропустить операции удвоения Q ← 2*Q* до первого сложе­ния *Q* ← *Q*+ *P*, которое выполняется как простое присваивание *Q*← *P*.

Обозначим через *М* и *I* стоимость (время) умножения и ин­версии по модулю р. Тогда из приведенных формул сложения и удвоения точки следует, что при аф­финном представлении стоимость сложения точек равна *I* + 3*М*, а стоимость удвоения равна *I* + 4*М* (операции сложения и умно­жения на маленькие коэффициенты заметного влияния на время вычисления не оказывают).

Соотношение стоимости инверсии и умножения может быть раз­личным в зависимости от реализации, но I всегда больше М. Если умножение реализуется за счет сложений и сдвигов, то оно, вероят­нее всего, будет незначительно (в 2-3 раза) опережать инверсию. В этом случае использование аффинного представления для точек на кривой вполне оправдано. Однако, если процессор, на котором выполняются вычисления, имеет встроенный параллельный умно­житель (как большинство современных процессоров общего назначения), то инверсия будет вычисляться существенно медленнее произведения. Можно дать грубую оценку стоимости соответствующих вычислений. Если t – длина чисел в битах, то умножение потребует порядка машинных операций (в данном случае 32 бита – размер машинного слова). С другой стороны, количество итераций в обобщенном алгоритме Евклида, вычисляющем инвер­сию, пропорциональноt по своей природе. Даже если мы сможем на каждой итерации реализовать линейные по t вычисления с помо­щью 32-битовых машинных операций (что возможно), мы получим общую трудоемкость порядка , т.е. одна инверсия бу­дет соответствовать тридцати двум умножениям. В действительно­сти на каждой итерации алгоритма Евклида нужно делать несколь­ко операций, а умножение может быть реализовано более быстрыми методами, так что *I* > 32*М*.

Мы можем избавиться от инверсий на каждом шаге алгоритма 1, если будем работать с координатами в виде рациональных чи­сел, производя вычисления отдельно с числителем и знаменателем. Наиболее выгодной оказывается следующая замена переменных (уже рассмотренная в главе 1 в задаче факторизации чисел с использованием эллиптических кривых):

В этом случае точка на кривой представляется тройкой и говорят о переходе к взвешенному проективному представлению (далее для простоты будем опускать слово «взвешенное»). Переход от аффинной точки к проективной делается очень просто:

После этого все вычисления проводятся в проективных координатах (без вычисления инверсий). Обратный переход от проективного к аффинному представлению осуществляется следующим образом:

и «стоит» оно *I*+4*М* (одно вычисление инверсии , два умножения для получения и и, наконец, два умножения и .

Получим формулы для сложения точек в проективном представ­лении. Вначале в формуле сложения для произведем замену пере­менных. После приведения к общему знаме­нателю и сокращения дроби получим:

Отсюда находим выражения для и , взяв соответственно чис­литель и квадратный корень из знаменателя правой части. Чтобы получить выражение для , прибегнем к хитрости, позво­ляющей в конечном итоге сэкономить одну операцию умножения. Заметим, что и

Произведем замену переменных, причем вместо используем его уже представление из формулы для . После приведения к общему знаменателю, сокращения и приведения подобных членов получаем:

На основании выражений для и запишем следующий алгоритм.

Алгоритм 2.Сложение точек в проективном представлении.

ВХОД:

ВЫХОД:

Все вычисления выполняются по модулю *p*.

Как видно из описания алгоритма, трудоемкость сложения в проективных координатах равна 16*М*. Мы не учитываем простые операции сложения, вычитания, а также умножения и деления на 2 (чтобы пояснить, как вычисляется , заметим, что ес­ли четно, то (сдвиг вправо на один бит); если нечетно, то , четно, поэтому . Если одна из точек, скажем , задана в аффинных координатах, т.е. , то стоимость сложения сни­жается до 11*M*. Это называется смешанным сложением. Алгоритм 1 построен таким образом, что он всегда использует смешанные сложения, т.е. стоимость сложения в нем равна 11*M*.

**Пример 2**. Рассмотрим вычисление суммы (5,1) + (4,6) в проективных координатах для кривой

Все вычисле­ния проводятся по модулю 7.

Для проверки переведем точку в аффинное представление. Для этого вычислим:

В итоге получаем:

что совпадает с результатом вычисления суммы точек в аффинном представлении.

Заметим, что условие эквивалентно , а условие эквивалентно . Если вычисления на кри­вой проводятся, как это предполагалось нами, в подмножестве точек мощности *q*, причем q – простое число, и , то условия для сложения в алгоритме 1 автоматически выполняют­ся (за исключением самого первого сложения, которое заменяется присваиванием).

Для удвоения точки в проективных координатах делаем аналогичную замену переменных в соответствующей формуле:

Что приводит к следующему алгоритму.

Алгоритм 3. Удвоение точки в проективном представлении.

ВХОД:

ВЫХОД:

Мы видим, что стоимость удвоения в проективных координатах в общем случае равна 10*М*. Однако, если параметр кривой ,то , и стоимость удвоения уменьшается до 8М.

Отметим, что в вышеизложенных алгоритмах все вычисления проводятся по модулю *р*. Поэтому многое зависит от эффектив­ной реализации модульной арифметики. Для случайно выбранных модулей наилучший на сегодняшний день подход — использование для чисел представления Монтгомери. В пред­ставлении Монтгомери умножение по модулю *р* эквивалентно двум обычным умножениям.

**§2. Определение количества точек на кривой.**

В этом разделе мы рассмотрим алгоритм Шуфа (Rene Schoof, 1985) для определения , т.е. количества точек, координаты ко­торых удовлетворяют уравнению эллиптической кривой и являются неотри­цательными целыми числами, меньшими *р*. Алгоритм Шуфа был первым полиномиальным алгоритмом подсчета количества точек на эллиптической кривой, его трудоемкость составляет опера­ций по модулю *р*. Этот алгоритм лежит в основе всех современных методов, применяемых для случайных кривых.

Напомним, что согласно теореме Хассе, удовлетворяет неравенствам .

Оказывается удобным представлять в виде

Параметр t здесь может принимать как положительные, так и отрицательные значения или быть равным нулю и называется сле­дом Фробениуса для . В соответствии с теоремой Хассе

До сих пор нас интересовали только точки на кривой с целочис­ленными неотрицательными координатами, меньшими р. Но теперь мы рассмотрим все множество решений уравнения эллиптической кривой в комплексных числах. След Фробениуса замечательным образом свя­зан с модулем р.

Теорема 1. Для всех комплексных чисел х и у, удовле­творяющих уравнению эллиптической кривой с параметрами , справедливо равенство

Чтобы научиться находить общее решение этого уравнения, за­метим, что произведение точки на число вида может быть выражено через координаты точки Р. Например,

Точка может быть получена как путем под­становки найденных выражений для координат точки в фор­мулы вычисления координат суммы точек. Процесс по­лучения выражений для следующих точек кажется довольно слож­ным, тем не менее, он описывается следующей простой рекурсивной схемой.

Для и

Полином называется полиномом деления порядка m. Поскольку точка лежит на кривой, приводимой по модулю *р*, вычисление коэффициентов полиномов достаточно также выпол­нять по модулю *р*. С использованием приведенной выше рекурсив­ной схемы полином деления порядка m может быть вычислен за шагов. Заметим, что при нечетном m полиномы зависят только от одной переменной *х*, так как вторая перемен­ная у входит в них только в четных степенях, а у2 заменяется пра­вой частью уравнения эллиптической кривой. Заметим также, что полиномы «второго слоя» включают в себя произведения четы­рех полиномов «первого слоя» (от до ),поэтому степень полинома растет как .

Комплексная точка *P* на кривой *E* называется торсионной точ­кой порядка m, если mР = 𝒪. Множество торсионных точек по­рядка m будем обозначать как . Вследствие вышеприведенной формулы для mР достаточно очевидно, что точка является торсионной порядка m то­гда и только тогда, когда .

Идея алгоритма Шуфа состоит в нахождении решений уравне­ния из теоремы 1 (относительно t) на множествах торсионных точек малых порядков с последующим вычислением общего решения. Для тор­сионных точек порядка m множители приводятся по модулю m, а полиномы – по модулю , так что уравнение принимает вид

где , ,, кроме того, x и у связаны уравнением кривой . Возьмем в качестве модулей m простые числа вплоть до некоторого mmax, такого, что

Тогда по найденным числам мы однозначно восстановим след Фробениуса *t*, воспользовавшись китайской теоремой об остатках.

Рассмотрим кратко метод решения данного уравнения для случая *m* > 2. Вначале вычисляем полином . Так как *m* нечетно, то (далее все действия с полиномами производятся по модулю , степень у понижается до единицы с помощью уравне­ния кривой, коэффициенты вычисляются по модулю p). Вычисляем полиномы , используя тот же алгоритм возведения в степень, что и для целых чисел. По формуле для вычисления mР вычисляем и, используя формулы сложения на кривой, находим в символическом виде сумму точек . Если , то . В противном случае, чтобы найти , вычисляем абсциссу точки для всех , . Для каждо­го значения нужно проверить равенство и . Вобщем случае разность абсцисс представляется в виде . Берем отсюда , подставляем в уравнение кривой и получаем некоторый полином . Если , то и не равны, и нужно пробовать другое значение . Если же , вычисляем ординату точки *P* и, пользуясь аналогичными приемами, переводим разность в полином . Если , то , иначе .

Когда *m* = 2, и возникает затруднение с вычислением . Однако в этом случае помогает одно простое рассужде­ние. Так как мы исключаем сингулярные кривые, то приведенная по модулю *p* эллиптическая кривая может иметь одно или три пересе­чения с осью х. Все другие точки идут парами ,,и есть одна точка в бесконечности *О*. Таким образом, количество точек на кривой четно или нечетно в зависимости от того, разлагается ли на множители по модулю р или нет. Известен простой критерий неразложимости полинома по модулю *р*.

Теорема 2. Полином третьей степени неразложим на множители по модулю *p* тогда и только тогда, когда

В результате имеем , если , и в противном случае.

Оценим трудоемкость алгоритма Шуфа. Вначале сформулиру­ем следующее известное свойство простых чисел.

Утверждение 1 (о простых числах). Количество про­стых чисел, меньших n, примерно равно .

Из этого утверждения следует, что и количество модулей, для которых ведутся вычисления, равно . Наиболее трудоемкая операция в алгоритме – вычисление и других аналогичных полиномов. При использовании быстрых алгоритмов возведения в степень эти вычисления требуют операций ти­па умножения с полиномами степени . Каждая такая операция требует операций типа умножения по мо­дулю *p*, т.е. всего получается операций по модулю *p*. Одна операция по модулю p выполняется с помощью битовых операций. Таким образом, вычисление требует бито­вых операций. Принимая во внимание число различных модулей, для которых нужно вычислять , получаем общую трудоемкость битовых операций.

**Пример 3.** Определим количество точек на кривой, исполь­зованной в примере 2:

Вначале воспользуемся алгоритмом, у которого время вычисле­ний растет экспоненциально. Будем задавать значения *X* от 0 до 6 и вычислять соответствующие им значения *Y*. Запишем вначале таблицу квадратов по модулю 7:

Используя эту таблицу, найдем множество точек :

Подсчитывая количество полученных точек, и добавляя к ним точку в бесконечности, получаем

Ясно, что этот метод не годится при больших *p*, но мы будем ис­пользовать полученное значение для проверки.

Приступим к выполнению алгоритма Шуфа. Нам достаточно будет трех модулей m = 2, 3, 5, так как (на самом деле двух модулей m = 3, 5 было бы достаточно, но мы используем еще m = 2 для демонстрации алгоритма).

В целях упрощения обозначений договоримся записывать поли­номы в виде десятичных чисел (величина модуля позволяет нам это сделать). Так, например,

Все вычисления с коэффициентами полиномов мы будем проводить по модулю 7. Вначале вычислим необходимые полиномы деления:

Решим уравнение для случая *m* = 3. Вычисляем по модулю :

Левая часть уравнения превращается в:

Значит, .

Теперь решим то же уравнение для *m* = 5. Вычисляем по мо­дулю :

Находим точку . В общем случае это делается по фор­муле:

Видим, что , поэтому будем искать . Найдем точку по обычным формулам сложения точек:

Пробуем , . Проверяем гипотезу :

Пробуем . Вычисляем . Здесь удобно использовать формулы сложения точек, так как мы прибавляем к предыдущей точке *P*. Получаем:

Проверяем гипотезу :

Значит, . Теперь нужно сравнить и . Имеем:

Проверяем гипотезу :

Значит, .

Наконец, определим . Нам нужно найти наибольший общий делитель для и . Сделаем это с помощью алго­ритма Евклида для полиномов. Обратим внимание на то, что при больших *p*, используемых в криптографии, мы не сможем непосред­ственно записать полином . Однако на первом шаге алгоритма Евклида вычисляется остаток , поэтому до­статочно подать на вход алгоритма не сам полином ,а его остаток. Вычисляем с помощью быстрых ме­тодов возведения в степень и вычитаем *х*. После этого используем алгоритм Евклида. В нашем примере:

Значит, .

Теперь используем китайскую теорему об остатках. Имеем:

Решение находится по формуле:

где

Подставляя числа, получаем:

Чтобы получить решение, удовлетворяющее неравенству, из теоремы Хассе, вы­читаем модуль:

Теперь находим:

Как видим, определение числа точек на кривой – не слишком простая задача. Ее решение требует использования мощной вычис­лительной техники. На практике используются улучшенные вариан­ты алгоритма Шуфа, основанные на тонких конструкциях высшей алгебры, главное достоинство которых состоит в снижении степени полиномов деления с до . В результате трудоемкость снижается до и может быть снижена до за счет использования асимптотически более быстрых методов умножения и деления (что обычно не оправдано при тех длинах чисел, которые актуальны для криптосистем на эллиптических кривых).

**§3. Использование стандартных кривых.**

Ввиду того, что формирование случайных кривых, особенно выполнение этапа подсчета количества точек на кривой, может быть слишком трудной задачей (даже с применением описанного выше алгоритма Шуфа), на практике часто бывает достаточным использовать кривые, предлагаемые различны­ми стандартами или другими источниками. Например, в американ­ском стандарте FIPS 186-2 приводятся параметры эллиптических кривых для различных длин модулей. Вообще говоря, нет никаких ограничений на использование всеми одной хорошо выбранной кри­вой. Однако такая кривая, при широком ее использовании, становит­ся слишком притягательной для злоумышленников. Не исключено, что со временем они смогут найти какие-либо эффективные атаки именно на эту кривую, используя ее характерные особенности, не принятые ранее во внимание. Но все это лишь возможность, веро­ятность осуществления которой считается многими специалистами ничтожно малой.

Приведем пример реальной кривой, рекомендуемой в FIPS 186-2 (Curve Р-256). Обратным «слэшем» («\») обозначим продолжение числа на следующей строке. Предполагается, что кривая задана уравнением , число точек на кривой , точка является генератором подмножества мощности q точек, где q – простое число.

(простое число)

Мы видим, что *p* и *q* вряд ли можно назвать случайно выбран­ными числами и вся «случайность» кривой определяется случайным выбором параметра *b* (это считается вполне обоснованным).

Первый вопрос, который возникает, когда мы видим кривую, подобную вышеприведенной, – это нет ли ошибки в записи пара­метров. Три проверки могут быть сделаны для выяснения этого во­проса:

1. Проверяем, является ли число *p* простым.
2. Проверяем, удовлетворяет ли точка уравнению кривой.
3. Удостоверяемся в том, что *n* – это действительно количество точек на кривой. Заметим, что такую проверку целесообразно делать и в том случае, когда мы сами вычисляем *n*, например, с помощью алгоритма Шуфа. В общем случае , где h – небольшое число, a q – простое. Прежде всего, путем последо­вательного деления и проверки на простоту следует убедиться, что *n* соответствует заявленной форме. Затем выбираем слу­чайно точку на кривой *P* (можно взять , где *k* – случайно выбранное число). Число *n* гарантированно являет­ся числом точек на кривой, если одновременно и . При невыполнении этого условия возможны два ва­рианта. Если ,то n – это не число точек. Если же (вероятность этого крайне мала), то нужно взять другую точку *P*.

Второй вопрос, который возникает, когда нам предъявляют «го­товую» кривую, это действительно ли она была сгенерирована слу­чайным образом. Этот вопрос вообще актуален для многих задач криптографии. Возможно, предложенная кривая обладает каким-либо редким свойством, позволяющим «взламывать» криптосисте­му, и человек, изготовивший эту кривую, может в дальнейшем по­лучить доступ, скажем, к информации, зашифрованной при помощи этой кривой. Задача доказательства отсутствия заранее заданных специальных свойств кривой сводится к задаче подобного же дока­зательства для случайно выбираемых параметров. Например, для рекомендованной выше кривой мы должны доказать случайность выбора параметра *b*. Эту задачу можно решить следующим обра­зом. Пусть – криптографически стойкая хеш-функция. Чтобы сгенерировать число *b*, вначале выбираем число *s*, а затем вычис­ляем и предъявляем оба числа: b и s. Если хеш-функция удовлетворяет всем требованиям стойкости, то *b* не может иметь никаких заранее заданных свойств, и мы можем спокойно им поль­зоваться. Число s является «сертификатом», доказывающим «чи­стоту» числа *b*. Приведенная выше эллиптическая кривая имеет по­добный сертификат, основанный на хеш-функции SHA-1, и стандарт оговаривает процедуру использования этого сертификата. Так что мы можем быть уверены в том, что кривая была сформирована действительно случайным образом.

**Индивидуальные задания по теме ``применение эллиптических кривых в криптографии``**

1. **Пример кодирования и декодирования текста.**

Алфавит представляет собой множество символов языка открытых текстов и соответствующих им точек эллиптической кривой над конечным полем.

Для выполнения индивидуальных заданий выбрана кривая , т.е. (mod 751). Предлагается следующий (один из возможных) алфавит, приведенный в таблице 9.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **символ** | **точка** | **№** | **символ** | **точка** | **№** | **символ** | **точка** | **№** | **символ** | **точка** |
| 1 | пробел | (33, 355) | 41 | H | (72, 254) | 81 | p | (109, 200) | 121 | Щ | (218, 601) |
| 2 | ! | (33, 396) | 42 | I | (72, 497) | 82 | q | (109, 551) | 122 | Ъ | (221, 138) |
| 3 | " | (34, 74) | 43 | J | (73, 72) | 83 | r | (110, 129) | 123 | Ы | (221, 613) |
| 4 | # | (34, 677) | 44 | K | (73, 679) | 84 | s | (110, 622) | 124 | Ь | (226, 9) |
| 5 | $ | (36, 87) | 45 | L | (74, 170) | 85 | t | (114, 144) | 125 | Э | (226, 742) |
| 6 | % | (36, 664) | 46 | M | (74, 581) | 86 | u | (114, 607) | 126 | Ю | (227, 299) |
| 7 | & | (39, 171) | 47 | N | (75, 318) | 87 | v | (115, 242) | 127 | Я | (227, 452) |
| 8 | ' | (39, 580) | 48 | O | (75, 433) | 88 | w | (115, 509) | 128 | а | (228, 271) |
| 9 | ( | (43, 224) | 49 | P | (78, 271) | 89 | x | (116, 92) | 129 | б | (228, 480) |
| 10 | ) | (43, 527) | 50 | Q | (78, 480) | 90 | y | (116, 659) | 130 | в | (229, 151) |
| 11 | \* | (44, 366) | 51 | R | (79, 111) | 91 | z | (120, 147) | 131 | г | (229, 600) |
| 12 | + | (44, 385) | 52 | S | (79, 640) | 92 | { | (120, 604) | 132 | д | (234, 164) |
| 13 | , | (45, 31) | 53 | T | (80, 318) | 93 | | | (125, 292) | 133 | е | (234, 587) |
| 14 | - | (45, 720) | 54 | U | (80, 433) | 94 | } | (125, 459) | 134 | ж | (235, 19) |
| 15 | . | (47, 349) | 55 | V | (82, 270) | 95 | ~ | (126, 33) | 135 | з | (235, 732) |
| 16 | / | (47, 402) | 56 | W | (82, 481) | 96 | А | (189, 297) | 136 | и | (236, 39) |
| 17 | 0 | (48, 49) | 57 | X | (83, 373) | 97 | Б | (189, 454) | 137 | й | (236, 712) |
| 18 | 1 | (48, 702) | 58 | Y | (83, 378) | 98 | В | (192, 32) | 138 | к | (237, 297) |
| 19 | 2 | (49, 183) | 59 | Z | (85, 35) | 99 | Г | (192, 719) | 139 | л | (237, 454) |
| 20 | 3 | (49, 568) | 60 | [ | (85, 716) | 100 | Д | (194, 205) | 140 | м | (238, 175) |
| 21 | 4 | (53, 277) | 61 | \ | (86, 25) | 101 | Е | (194, 546) | 141 | н | (238, 576) |
| 22 | 5 | (53, 474) | 62 | ] | (86, 726) | 102 | Ж | (197, 145) | 142 | о | (240, 309) |
| 23 | 6 | (56, 332) | 63 | ^ | (90, 21) | 103 | З | (197, 606) | 143 | п | (240, 442) |
| 24 | 7 | (56, 419) | 64 | \_ | (90, 730) | 104 | И | (198, 224) | 144 | р | (243, 87) |
| 25 | 8 | (58, 139) | 65 | ` | (93, 267) | 105 | Й | (198, 527) | 145 | с | (243, 664) |
| 26 | 9 | (58, 612) | 66 | a | (93, 484) | 106 | К | (200, 30) | 146 | т | (247, 266) |
| 27 | : | (59, 365) | 67 | b | (98, 338) | 107 | Л | (200, 721) | 147 | у | (247, 485) |
| 28 | ; | (59, 386) | 68 | c | (98, 413) | 108 | М | (203, 324) | 148 | ф | (249, 183) |
| 29 | < | (61, 129) | 69 | d | (99, 295) | 109 | Н | (203, 427) | 149 | х | (249, 568) |
| 30 | = | (61, 622) | 70 | e | (99, 456) | 110 | О | (205, 372) | 150 | ц | (250, 14) |
| 31 | > | (62, 372) | 71 | f | (100, 364) | 111 | П | (205, 379) | 151 | ч | (250, 737) |
| 32 | ? | (62, 379) | 72 | g | (100, 387) | 112 | Р | (206, 106) | 152 | ш | (251, 245) |
| 33 | @ | (66, 199) | 73 | h | (102, 267) | 113 | С | (206, 645) | 153 | щ | (251, 506) |
| 34 | A | (66, 552) | 74 | i | (102, 484) | 114 | Т | (209, 82) | 154 | ъ | (253, 211) |
| 35 | B | (67, 84) | 75 | j | (105, 369) | 115 | У | (209, 669) | 155 | ы | (253, 540) |
| 36 | C | (67, 667) | 76 | k | (105,382) | 116 | Ф | (210, 31) | 156 | ь | (256, 121) |
| 37 | D | (69, 241) | 77 | l | (106, 24) | 117 | Х | (210, 720) | 157 | э | (256, 630) |
| 38 | E | (69, 510) | 78 | m | (106, 727) | 118 | Ц | (215, 247) | 158 | ю | (257, 293) |
| 39 | F | (70, 195) | 79 | n | (108, 247) | 119 | Ч | (215, 504) | 159 | я | (257, 458) |
| 40 | G | (70, 556) | 80 | o | (108, 504) | 120 | Ш | (218,150) |

**Таблица 9.** Алфавит точек эллиптической кривой для выполнения индивидуальных заданий.

Заметим, что мощность множества точек на этой кривой *N* = 727, поэтому при необходимости можно точками закодировать и некоторые специальные знаки (например, знак интеграла и т.п.), а также целые слова.

**2) Пример шифрования.**

Пусть выбрана генерирующая точка *G* = (0, 1). Предположим, пользователь А решил отправить пользователю B сообщение: строчную латинскую букву «A». В нашем алфавите эта буква кодируется точкой  = (66, 522). Пусть пользователь А выбрал случайное значение *k* = 3, а открытым ключом B является точка  = (406, 397), при этом секретным ключом B является число .

Шифрованный текст имеет вид  = {*kG*,  + *k*}.

Находим *kG* **=** .

Для нахождения 3*G* используем правила сложения точек эллиптической кривой. Напомним их:







Вычисляем 2G:







Итак, мы нашли 2*G* = (188, 93). Теперь находим 3*G*.







Таким образом, мы нашли точку *kG* **=**  = (56, 419).

Вычисляем  + *k* **=** (66, 552) + (406, 397) = (301, 734).

В результате:  = {(56, 419), (301, 734)}.

Пользователь B для расшифрования сообщения должен провести следующие вычисления:  + *k* – (*kG*) =  + *k* (*G*) – (*kG*) = (301, 734) – (56, 419) = (301, 734) + (175, 559) = (66, 552).

После этого пользователь B по алфавиту определяет открытый буквенный текст: точке (66, 552) соответствует строчная латинская буква «A».

**3) Пример генерации и проверки подписи.**

Пусть используется эллиптическая кривая  и генерирующая точка *G* = (384, 475) порядка *n* = 13 (13 – наибольший из делителей порядка кривой *N* = 728). Предположим, абонент подписывает личным секретным ключом *d* = 12 сообщение, хеш-свертка которого равна *e* = 12.

Пусть абонент, подписывающий сообщение, выбрал случайное *k* = 3. Тогда он вычисляет *kG* =  =  = (596, 318) и затем . Используя расширенный алгоритм Евклида, определяем  (так как ). Наконец, . Таким образом,  – цифровая подпись данного абонента для сообщения.

Пусть теперь необходимо проверить подлинность данной подписи. Открытый ключ абонента, подписавшего сообщение, равен . Проверка подписи начинается с проверки условий ,  – в данном случае они соблюдаются. Затем последовательно вычисляем ,  и . Находим точку  . Наконец, сравниваем значения *r* = 11 и   – они совпадают, следовательно, подпись действительная.

**Варианты заданий**

**Задача 1.** Зашифровать открытый текст, используя алфавит, приведенный в примере (используется кривая  и генерирующая точка *G* = (0, 1)).

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **варианта** | **Открытый текст** | **Открытый ключ *B*** | **Значения случайных чисел *k* для букв открытого текста** |
| 1 | передряга | (489, 468) | 18, 15, 14, 18, 5, 10, 19, 14, 19 |
| 2 | латышский | (179, 275) | 15, 17, 12, 2, 2, 4, 8, 6, 17 |
| 3 | регрессор | (425, 663) | 6, 12, 16, 4, 9, 4, 19 , 9, 18 |
| 4 | симметрия | (179, 275) | 11, 17, 18, 19, 16, 6, 12, 8, 2 |
| 5 | уверовать | (425, 663) | 6, 14, 5, 7, 12, 11, 4, 9, 19 |
| 6 | терновник | (188, 93) | 8, 14, 17, 17, 2, 10, 8, 2, 2 |
| 7 | терпеливо | (725, 195) | 17, 5, 4, 17, 13, 2, 17, 14, 19 |
| 8 | ремонтный | (188, 93) | 2, 2, 4, 18, 15, 19, 11, 2, 15 |
| 9 | ренессанс | (725, 195) | 2, 19, 4, 8, 2, 2, 16, 10, 2 |
| 10 | репарация | (435, 663) | 12, 11, 18, 7, 16, 18, 17, 2, 3 |
| 11 | пролежень | (179, 275) | 9, 5, 17, 2, 2, 2, 3, 17, 15 |
| 12 | прокрутка | (618, 206) | 10, 15, 16, 2, 3, 4, 2, 11, 16 |
| 13 | прокопать | (489, 468) | 3, 16, 17, 5, 16, 18, 3, 7, 15 |
| 14 | отступить | (188, 93) | 7, 9, 3, 8, 18, 18, 8, 11, 16 |
| 15 | отставной | (286, 136) | 5, 3, 3, 2, 4, 19, 2, 4, 10 |
| 16 | отслужить | (16, 416) | 2, 8, 4, 2, 6, 10, 3, 3, 18 |
| 17 | отследить | (188, 93) | 19, 2, 13, 5, 19, 5, 7, 8, 5 |
| 18 | новенький | (425, 663) | 19, 12, 13, 2, 12, 14, 19, 18, 12 |
| 19 | нищенский | (489, 468) | 2, 2, 7, 11, 19, 4, 2, 15, 6 |
| 20 | никелевый | (568, 355) | 9, 9, 2, 3, 8, 19, 6, 18, 9 |
| 21 | низменный | (286, 136) | 12, 5, 7, 17, 18, 2, 12, 10, 11 |
| 22 | неэтичный | (489, 468) | 14, 18, 11, 11, 6, 6, 17, 2, 5 |
| 23 | мысленный | (346, 242) | 6, 17, 18, 11, 18, 2, 4, 2, 12 |
| 24 | муштровка | (618, 206) | 5, 19, 8, 2, 5, 8, 15, 19, 6 |
| 25 | латентный | (725, 195) | 9, 10, 13, 2, 2, 12, 12, 5, 7 |
| 26 | купальщик | (188, 93) | 17, 17, 9, 12, 17, 7, 15, 7, 16 |
| 27 | излечимый | (179, 275) | 10, 14, 2, 2, 10, 10, 14, 3, 7 |
| 28 | звездочка | (725, 195) | 11, 17, 10, 10, 5, 2, 10, 19, 4 |
| 29 | аберрация | (56, 419) | 16, 2, 17, 19, 8, 4, 3, 2, 8 |
| 30 | белиберда | (286, 136) | 2, 9, 18, 2, 19, 4, 5, 11, 9 |

|  |  |  |
| --- | --- | --- |
| **№**  **варианта** | **Секретный ключ** | **Шифртекст** |
| 1 | 29 | {(440, 539), (128, 672)}; {(489, 468), (282, 341)};  {(489, 468), (45, 720)}; {(72, 254), (227, 299)};  {(188, 93), (251, 506)}; {(72, 254), (319, 518)};  {(745, 210), (129, 659)}; {(286, 136), (515, 684)};  {(568, 355), (395, 414)} |
| 2 | 25 | {(72, 254), (397, 184)}; {(188, 93), (526, 412)};  {(188, 93), (328, 290)}; {(135, 82), (433, 47)};  {(179, 275), (711, 341)}; {(568, 355), (546, 670)};  {(16, 416), (734, 170)}; {(568, 355), (371, 14)};  {(596, 433), (604, 610)}; {(16, 416), (734, 170)} |
| 3 | 40 | {(188, 93), (573, 583)}; {(188, 93), (128, 79)};  {(425, 663), (703, 125)}; {(489, 468), (109, 200)};  {(568, 355), (348, 27)}; {(377, 456), (323, 657)};  {(72, 254), (399, 65)}; {(16, 416), (660, 275)};  {(179, 275), (267, 670)}; {(568, 355), (642, 53)} |
| 4 | 34 | {(618, 206), (426, 662)}; {(72, 254), (67, 667)};  {(286, 136), (739, 574)}; {(16, 416), (143, 602)};  {(618, 206), (313, 203)}; {(618, 206), (114, 607)};  {(618, 206), (438, 711)}; {(188, 93), (573, 168)} |
| 5 | 41 | {(283, 493), (314, 127)}; {(425, 663), (561, 140)};  {(568, 355), (75, 433)}; {(440, 539), (602, 627)};  {(188, 93), (395, 414)}; {(179, 275), (25, 604)};  {(72, 254), (47, 349)}; {(72, 254), (417, 137)};  {(188, 93), (298, 225)}; {(56, 419), (79, 111)} |
| 6 | 44 | {(377, 456), (367, 360)}; {(425, 663), (715, 398)};  {(188, 93), (279, 353)}; {(179, 275), (128, 79)};  {(568, 355), (515, 67)}; {(568, 355), (482, 230)};  {(377, 456), (206, 645)}; {(188, 93), (300, 455)};  {(489, 468), (362, 446)}; {(16, 416), (69, 510)};  {(425, 663), (218, 601)} |
| 7 | 12 | {(16, 416), (128, 672)}; {(56, 419), (59, 386)};  {(425, 663), (106, 24)}; {(568, 355), (145, 608)};  {(188, 93), (279, 398)}; {(425, 663), (99, 295)};  {(179, 275), (269, 187)}; {(188, 93), (395, 337)};  {(188, 93), (311, 68)}; {(135, 82), (556, 484)};  {(56, 419), (106, 727)}; {(16, 416), (307, 693)} |
| 8 | 45 | {(745, 210), (259, 401)}; {(568, 355), (606, 147)};  {(188, 93), (407, 82)}; {(56, 419), (739, 574)};  {(286, 136), (329, 447)}; {(425, 663), (520, 749)};  {(72, 254), (374, 315)}; {(188, 93), (149, 97)};  {(745, 210), (13, 134)}; {(440, 539), (235, 19)};  {(425, 663), (128, 79)} |

**Задача 2.** Дан шифртекст. Используя алфавит, приведенный в примере (используется кривая  и генерирующая точка *G* = (–1, 1)), и зная секретный ключ ****, найти открытый текст.

|  |  |  |
| --- | --- | --- |
| 9 | 32 | {(188, 93), (623, 166)}; {(725, 195), (513, 414)};  {(346, 242), (461, 4)}; {(489, 468), (739, 574)};  {(725, 195), (663, 476)}; {(745, 210), (724, 522)};  {(725, 195), (663, 476)}; {(618, 206), (438, 40)};  {(286, 136), (546, 670)}; {(179, 275), (73, 72)} |
| 10 | 18 | {(179, 275), (269, 564)}; {(179, 275), (73, 72)};  {(440, 539), (189, 454)}; {(618, 206), (628, 458)};  {(568, 355), (660, 275)}; {(72, 254), (709, 595)};  {(745, 210), (12, 314)}; {(188, 93), (36, 664)};  {(618, 206), (530, 22)}; {(286, 136), (532, 50)};  {(425, 663), (660, 275)}; {(725, 195), (482, 230)} |
| 11 | 27 | {(745, 210), (185, 105)}; {(188, 93), (681, 385)};  {(377, 456), (576, 465)}; {(440, 539), (138, 298)};  {(745, 210), (520, 2)}; {(188, 93), (681, 385)};  {(286, 136), (282, 410)}; {(72, 254), (200, 721)};  {(72, 254), (643, 94)}; {(745, 210), (476, 315)};  {(440, 539), (724, 229)} |
| 12 | 25 | {(425, 663), (651, 191)}; {(188, 93), (177, 562)};  {(286, 136), (603, 562)}; {(440, 539), (588, 707)};  {(72, 254), (269, 187)}; {(56, 419), (49, 568)};  {(16, 416), (426, 662)}; {(425, 663), (557, 28)};  {(188, 93), (149, 97)}; {(179, 275), (711, 341)} |
| 13 | 48 | {(179, 275), (712, 186)}; {(725, 195), (395, 414)};  {(72, 254), (434, 136)}; {(425, 663), (251, 506)};  {(16, 416), (383, 340)}; {(745, 210), (102, 484)};  {(346, 242), (78, 271)}; {(179, 275), (712, 186)};  {(725, 195), (739, 574)}; {(346, 242), (78, 271)} |
| 14 | 51 | {(425, 663), (273, 481)}; {(188, 93), (85, 716)};  {(16, 416), (422, 162)}; {(283, 493), (36, 87)};  {(179, 275), (100, 364)}; {(188, 93), (298, 225)};  {(56, 419), (555, 303)}; {(745, 210), (100, 387)};  {(377, 456), (526, 412)}; {(286, 136), (316, 228)};  {(745, 210), (49, 183)}; {(179, 275), (428, 247)} |
| 15 | 27 | {(618, 206), (99, 456)}; {(425, 663), (31, 136)};  {(377, 456), (688, 741)}; {(425, 663), (636, 747)};  {(16, 416), (298, 526)}; {(188, 93), (356, 175)};  {(489, 468), (147, 390)}; {(346, 242), (546, 670)};  {(72, 254), (114, 144)}; {(377, 456), (25, 147)} |
| 16 | 48 | {(16, 416), (724, 522)}; {(489, 468), (719, 538)};  {(56, 419), (205, 372)}; {(72, 254), (628, 293)};  {(188, 93), (594, 337)}; {(440, 539), (588, 707)};  {(568, 355), (707, 556)}; {(489, 468), (719, 538)};  {(16, 416), (590, 376)}; {(56, 419), (612, 329)};  {(188, 93), (594, 337)} |

|  |  |  |
| --- | --- | --- |
| 17 | 51 | {(56, 419), (739, 177)}; {(16, 416), (282, 410)};  {(425, 663), (221, 138)}; {(188, 93), (329, 447)};  {(286, 136), (235, 19)}; {(725, 195), (496, 31)};  {(56, 419), (236, 712)}; {(440, 539), (514, 662)};  {(377, 456), (323, 94)}; {(179, 275), (203, 324)};  {(568, 355), (197, 606)} |
| 18 | 16 | {(745, 210), (268, 597)}; {(725, 195), (310, 582)};  {(618, 206), (59, 365)}; {(440, 539), (371, 14)};  {(188, 93), (348, 27)}; {(72, 254), (434, 136)};  {(16, 416), (623, 166)}; {(188, 93), (235, 19)};  {(440, 539), (660, 275)}; {(188, 93), (434, 615)};  {(725, 195), (73, 679)}; {(188, 93), (642, 53)} |
| 19 | 34 | {(725, 195), (538, 325)}; {(725, 195), (176, 413)};  {(425, 663), (689, 670)}; {(346, 242), (652, 315)};  {(283, 493), (463, 736)}; {(16, 416), (744, 133)};  {(179, 275), (542, 351)}; {(56, 419), (298, 225)};  {(286, 136), (719, 538)}; {(568, 355), (319, 518)};  {(16, 416), (704, 46)} |
| 20 | 25 | {(725, 195), (329, 304)}; {(440, 539), (59, 386)};  {(618, 206), (543, 357)}; {(188, 93), (520, 749)};  {(489, 468), (585, 211)}; {(179, 275), (707, 556)};  {(596, 433), (419, 38)}; {(377, 456), (643, 94)};  {(188, 93), (385, 749)}; {(725, 195), (150, 355)};  {(725, 195), (197, 606)} |
| 21 | 58 | {(16, 416), (93, 484)}; {(489, 468), (531, 397)};  {(188, 93), (654, 102)}; {(489, 468), (218, 150)};  {(16, 416), (530, 729)}; {(425, 663), (295, 219)};  {(725, 195), (742, 299)}; {(188, 93), (367, 360)};  {(188, 93), (235, 732)}; {(618, 206), (251, 245)};  {(425, 663), (688, 10)} |
| 22 | 50 | {(179, 275), (326, 675)}; {(725, 195), (83, 378)};  {(440, 539), (340, 78)}; {(425, 663), (67, 84)};  {(425, 663), (620, 71)}; {(72, 254), (251, 245)};  {(568, 355), (75, 318)}; {(725, 195), (228, 271)};  {(188, 93), (734, 170)}; {(188, 93), (704, 705)};  {(286, 136), (235, 732)} |
| 23 | 19 | {(618, 206), (294, 595)}; {(188, 93), (13, 617)};  {(188, 93), (206, 106)}; {(188, 93), (67, 667)};  {(56, 419), (350, 184)}; {(440, 539), (275, 456)};  {(745, 210), (301, 17)}; {(346, 242), (588, 707)};  {(188, 93), (256, 121)}; {(425, 663), (209, 82)};  {(16, 416), (687, 660)} |

|  |  |  |
| --- | --- | --- |
| 24 | 54 | {(188, 93), (295, 219)}; {(618, 206), (646, 706)};  {(440, 539), (573, 583)}; {(16, 416), (694, 581)};  {(179, 275), (585, 540)}; {(377, 456), (701, 570)};  {(618, 206), (67, 667)}; {(286, 136), (36, 664)};  {(72, 254), (727, 65)}; {(568, 355), (438, 40)} |
| 25 | 55 | {(725, 195), (9, 150)}; {(745, 210), (138, 453)};  {(56, 419), (36, 87)}; {(283, 493), (39, 580)};  {(377, 456), (515, 684)}; {(346, 242), (458, 261)};  {(283, 493), (105, 369)}; {(568, 355), (326, 675)};  {(425, 663), (529, 358)}; {(283, 493), (668, 409)} |
| 26 | 24 | {(16, 416), (150, 355)}; {(188, 93), (394, 20)};  {(725, 195), (13, 134)}; {(377, 456), (209, 669)};  {(56, 419), (514, 662)}; {(56, 419), (243, 87)};  {(618, 206), (719, 538)}; {(618, 206), (159, 13)};  {(618, 206), (326, 76)}; {(188, 93), (557, 28)} |
| 27 | 43 | {(440, 539), (279, 398)}; {(568, 355), (295, 219)};  {(16, 416), (724, 229)}; {(346, 242), (730, 240)};  {(72, 254), (334, 226)}; {(188, 93), (310, 169)};  {(72, 254), (36, 664)}; {(179, 275), (481, 369)};  {(188, 93), (236, 39)}; {(377, 456), (438, 711)};  {(377, 456), (307, 58)} |
| 28 | 20 | {(16, 416), (675, 505)}; {(72, 254), (611, 579)};  {(72, 254), (727, 686)}; {(489, 468), (39, 171)};  {(72, 254), (531, 354)}; {(568, 355), (36, 87)};  {(188, 93), (588, 44)}; {(618, 206), (70, 195)};  {(568, 355), (267, 81)}; {(56, 419), (525, 674)} |
| 29 | 47 | {(725, 195), (651, 560)}; {(425, 663), (147, 361)};  {(286, 136), (109, 551)}; {(440, 539), (90, 730)};  {(618, 206), (668, 342)}; {(745, 210), (109, 200)};  {(425, 663), (147, 361)}; {(72, 254), (228, 480)};  {(346, 242), (530, 22)} |
| 30 | 50 | {(16, 416), (726, 608)}; {(188, 93), (395, 337)};  {(440, 539), (163, 513)}; {(188, 93), (269, 187)};  {(725, 195), (177, 562)}; {(188, 93), (115, 509)};  {(188, 93), (734, 170)}; {(745, 210), (110, 622)};  {(179, 275), (576, 286)}; {(188, 93), (325, 297)} |

**Задача 3.** Даны точки *P*, *Q*, *R* на кривой . Найти точку 2*P* + 3*Q* – *R*.

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **варианта** | **Координаты точек** | | |
| ***P*** | ***Q*** | ***R*** |
| 1 | (58, 139) | (67, 667) | (82, 481) |
| 2 | (61, 129) | (59, 365) | (105, 369) |
| 3 | (62, 372) | (70, 195) | (67, 84) |
| 4 | (56, 332) | (69, 241) | (83, 373) |
| 5 | (59, 386) | (70, 195) | (72, 254) |
| 6 | (72, 497) | (61, 622) | (70, 556) |
| 7 | (74, 170) | (53, 277) | (86, 25) |
| 8 | (48, 702) | (69, 241) | (98, 338) |
| 9 | (59, 386) | (61, 129) | (100, 364) |
| 10 | (72, 497) | (53, 474) | (90, 730) |
| 11 | (59, 365) | (59, 386) | (105, 382) |
| 12 | (61, 622) | (61, 622) | (90, 730) |
| 13 | (61, 129) | (69, 510) | (72, 497) |
| 14 | (70, 556) | (56, 419) | (86, 726) |
| 15 | (67, 84) | (69, 241) | (66, 199) |
| 16 | (73, 72) | (56, 332) | (85, 35) |
| 17 | (69, 241) | (53, 277) | (106, 24) |
| 18 | (74, 581) | (53, 277) | (85, 35) |
| 19 | (56, 419) | (69, 510) | (79, 640) |
| 20 | (58, 612) | (67, 84) | (83, 373) |
| 21 | (62, 379) | (53, 474) | (110, 622) |
| 22 | (53, 277) | (66, 552) | (99, 456) |
| 23 | (67, 667) | (53, 474) | (105, 382) |
| 24 | (69, 241) | (66, 552) | (69, 510) |
| 25 | (69, 510) | (53, 277) | (105, 369) |
| 26 | (72, 497) | (62, 372) | (69, 241) |
| 27 | (61, 129) | (59, 365) | (105, 369) |
| 28 | (61, 622) | (59, 365) | (102, 267) |
| 29 | (58, 139) | (67, 84) | (85, 35) |
| 30 | (69, 510) | (62, 372) | (74, 170) |

**Задача 4.** Дана точка *P* на кривой  и натуральное число *n*. Найти точку *nP*.

|  |  |  |
| --- | --- | --- |
| **№**  **варианта** | ***P*** | ***n*** |
| 1 | (62, 372) | 128 |
| 2 | (43, 527) | 116 |
| 3 | (39, 171) | 110 |
| 4 | (43, 527) | 107 |
| 5 | (36, 87) | 111 |
| 6 | (49, 568) | 122 |
| 7 | (39, 580) | 109 |
| 8 | (75, 318) | 142 |
| 9 | (45, 720) | 111 |
| 10 | (78, 480) | 147 |
| 11 | (53, 474) | 120 |
| 12 | (43, 527) | 109 |
| 13 | (49, 568) | 124 |
| 14 | (39, 171) | 108 |
| 15 | (49, 183) | 126 |
| 16 | (58, 139) | 121 |
| 17 | (33, 355) | 111 |
| 18 | (39, 580) | 101 |
| 19 | (44, 366) | 113 |
| 20 | (73, 72) | 103 |
| 21 | (85, 716) | 159 |
| 22 | (66, 199) | 103 |
| 23 | (44, 385) | 113 |
| 24 | (45, 720) | 111 |
| 25 | (39, 171) | 107 |
| 26 | (34, 677) | 106 |
| 27 | (34, 74) | 107 |
| 28 | (34, 677) | 105 |
| 29 | (79, 640) | 149 |
| 30 | (58, 139) | 124 |

**Задача 5.** Сгенерировать ЭЦП для сообщения с известным значением хэш-свертки *e*, зная секретный ключ подписи *d* при данном значении выбираемого случайным образом числа *k*. Используется кривая  и генерирующая точка *G* = (416, 55) порядка *n* = 13.

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **варианта** | ***e*** | ***d*** | ***k*** |
| 1 | 9 | 3 | 5 |
| 2 | 3 | 9 | 6 |
| 3 | 12 | 9 | 2 |
| 4 | 3 | 4 | 7 |
| 5 | 5 | 12 | 6 |
| 6 | 6 | 12 | 7 |
| 7 | 8 | 5 | 5 |
| 8 | 8 | 2 | 5 |
| 9 | 11 | 5 | 6 |
| 10 | 3 | 3 | 11 |
| 11 | 10 | 9 | 2 |
| 12 | 11 | 2 | 8 |
| 13 | 8 | 6 | 3 |
| 14 | 3 | 10 | 6 |
| 15 | 4 | 6 | 11 |
| 16 | 6 | 12 | 11 |
| 17 | 2 | 11 | 5 |
| 18 | 10 | 5 | 11 |
| 19 | 11 | 5 | 7 |
| 20 | 6 | 10 | 7 |
| 21 | 10 | 9 | 11 |
| 22 | 6 | 10 | 2 |
| 23 | 9 | 6 | 6 |
| 24 | 8 | 12 | 8 |
| 25 | 3 | 2 | 8 |
| 26 | 6 | 5 | 6 |
| 27 | 6 | 7 | 11 |
| 28 | 7 | 3 | 7 |
| 29 | 9 | 11 | 2 |
| 30 | 5 | 12 | 8 |

**Задача 6.** Проверить подлинность ЭЦП  для сообщения с известным значением хэш-свертки *e*, зная открытый ключ проверки подписи *Q*. Используется кривая  и генерирующая точка *G* = (562, 89) порядка *n* = 13.

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **варианта** | ***e*** | ***Q*** | **(*r*, *s*)** |
| 1 | 4 | (596, 318) | (11, 4) |
| 2 | 5 | (455, 368) | (3, 7) |
| 3 | 6 | (135, 669) | (5, 7) |
| 4 | 6 | (562, 662) | (5, 7) |
| 5 | 2 | (135, 669) | (7, 6) |
| 6 | 8 | (135, 82) | (11, 10) |
| 7 | 4 | (384, 475) | (11, 9) |
| 8 | 7 | (596, 433) | (11, 1) |
| 9 | 7 | (455, 368) | (11, 11) |
| 10 | 7 | (384, 475) | (5, 5) |
| 11 | 5 | (384, 475) | (11, 1) |
| 12 | 10 | (455, 383) | (11, 10) |
| 13 | 8 | (384, 276) | (3, 1) |
| 14 | 3 | (135, 669) | (11, 10) |
| 15 | 6 | (455, 383) | (3, 1) |
| 16 | 2 | (596, 433) | (3, 10) |
| 17 | 10 | (455, 368) | (11, 6) |
| 18 | 5 | (596, 433) | (11, 12) |
| 19 | 9 | (135, 82) | (7, 7) |
| 20 | 2 | (596, 433) | (11, 4) |
| 21 | 6 | (596, 318) | (7, 5) |
| 22 | 5 | (596, 318) | (7, 4) |
| 23 | 12 | (135, 669) | (5, 11) |
| 24 | 12 | (562, 89) | (3, 2) |
| 25 | 6 | (562, 662) | (7, 10) |
| 26 | 12 | (135, 82) | (7, 8) |
| 27 | 7 | (384, 276) | (5, 2) |
| 28 | 8 | (596, 318) | (11, 6) |
| 29 | 10 | (384, 276) | (7, 6) |
| 30 | 9 | (416, 696) | (11, 11) |

**Темы лабораторных работ**

В лабораторных работах рекомендуется использовать эллип­тическую кривую со следующими параметрами:

Количество точек на этой кривой

В качестве генератора можно взять точку

Точку в бесконечности О удобно представлять как точку с координатами (0,0).

**Лабораторная работа 1.** Написать набор подпрограмм для вычисления суммы точек на эллиптической кривой и произведения точки на число. При­ведем несколько тождеств для тестирования разработанных подпрограмм:

(51, 7858) + (91, 5500) = (7252,18353),

(7777,10935) + (16000,20400) = (12395, 26268),

(12405,28624) + (2963,16300) = (14905,2313),

(8020,1740) + (8020, 30251) = *О*,

2 · (0,5585) = (8,19435),

2 · (23161,17992) = (26775,10831),

2 · (110,13171) = (26948,16087),

10000 · (31122,9) = (31180,29596),

12345 · (13140,5033) = (9362,27046),

11111 · (11007,23704) = (850,6718).

**Лабораторная работа 2.** Выполнить программную реализацию шифра Эль-Гамаля на эллиптической кривой. При отладке и тестировании програм­мы можно воспользоваться следующим примером построения шифра:

Полученный шифртекст должен расшиф­роваться в сообщение 10000 при использовании секретного ключа 5103.

**Лабораторная работа 3.** Выполнить программную реализацию алгоритмов генерации и проверки цифровой подписи на эллиптической кривой по стандарту ГОСТ 34.10-2001 (как обычно, полагаем ). В качестве q берем n = 32089 (число точек на кривой). Подпись (4615, 5944) для сообщения 1000 должна признаваться подлинной для пользователя, имеюще­го открытый ключ .

**Библиографический список**

1. Н.Коблиц. Курс теории чисел и криптографии. М., Научное издательство ТВП, 2001,254 с.
2. В. Столлингс. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001.
3. А.А.Болотов, С.Б.Гашков, А.Б.Фролов, А.А.Часовских Элементарное введение в эллиптическую криптографию. М., Комкнига, 2006. 328с.
4. Э. Кнэпп. Эллиптические кривые. Пер. с англ. Ф. Ю. Попеленского. -М.: Изд-во «Факториал Пресс», 2004. – 488с.
5. Соловьев, Шавгулидзе, Садовничий. Эллиптические кривые и современные алгоритмы теории чисел. Ижевск, 2003.
6. Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. «Математические и компьютерные основы криптологии».- Мн.: Новое знание, 2003.-382с.
7. Diffie W., Hellman M. New Directions in Cryptography// IEEE Transactions on Information Theory, − 22.  
   − 1976. − p. 644 − 654.
8. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems// Communications of the ACM. − 21. − 1978. − p. 120 − 126.
9. Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms// IEEE Transactions on Information Theory. − 31. − 1985. − p. 469 − 472.
10. Schnorr C.P. Efficient Identification and Signatures for Smart Cards// Advances in Cryptology − Crypto’89.   
     − LNCS 435, − 1990. − p. 239 − 252.
11. Lenstra A.K., Lenstra H.W. The Development of the Number Field Sieve. − Berlin: Springer, 1993. − p. 131.
12. С.С.Степанов. Арифметика алгебраических кривых. М., Наука, 1991. 365с.
13. О.Н.Василенко.Теоретико-числовые алгоритмы в криптографии. М., 2001, 265 с.
14. Miller V.S. Use of Elliptic Curves in Cryptography// Advances in Cryptology − Crypto’85. − LNCS 218.   
    − 1986. − p. 417 − 426.
15. Schoof R. Elliptic Curves over Finite Fields and the Computation of Square Roots mod *p*// Mathematics of Computation. − 44. − 1985. − p. 483 − 494.
16. Menezes A., Okamoto T., Vanstone S. Reducing Elliptic Curve Logarithms to a Finite Field// IEEE Trans. Info. Theory. − 39. −1993. − p. 1639 − 1646.
17. Balasubramanian R., Koblitz N. The Improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm// J. of Cryptology, − №2. −11. −1998.   
    −p.141− 145.
18. Smart N.P. The Discrete Logarithm Problem on Elliptic Curves of Trace 1//J.of Cryptology.−№3. − 12.   
    − 1999. −p. 193 − 196.

1. Silverman J. Advanced Topics in the Arithmetic of Elliptic Curves. −New York: Springer, 1994. −p. 525.
2. Menezes A. Elliptic Curve Public Key Cryptosystems. − Boston: Kluwer Academic Publishers, 1993. −p. 126.

21.Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информации.СибГАУ,Красноярск,2008, 253с.

**ПРИЛОЖЕНИЕ 1**

**Выдержки из Стандарта**

**ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита**

**информации. Процессы формирования и проверки электронной цифровой подписи**

Предисловие

1. РАЗРАБОТАН Главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации с участием Всероссийского научно-исследовательского института стандартизации (ВНИИстандарт).

ВНЕСЕН Федеральным агентством правительственной связи и информации при Президенте Российской Федерации.

1. ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 12 сентября 2001 г. № 380-ст….

Введение

Настоящий стандарт содержит описание процессов формирования и проверки электронной цифровой подписи (ЭЦП), реализуемой с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем….

1. Область применения

Настоящий стандарт определяет схему электронной цифровой подписи (ЭЦП) (далее по тексту – цифровая подпись), процессы формирования и проверки цифровой подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения.

Внедрение цифровой подписи на базе настоящего стандарта повышает, по сравнению с действующей схемой цифровой подписи, уровень защищенности передаваемых сообщений от подделок и искажений.

Стандарт рекомендуется использовать в новых системах обработки информации различного назначения, а также при модернизации действующих систем.

2. Нормативные ссылки

В настоящем стандарте использованы следующие термины:

3.1.1. Дополнение (appendix): Строка бит, формируемая из цифровой подписи и произвольного текстового поля (ИСО/МЭК 148881-1).

3.1.2. Ключ подписи (signature key): Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи (ИСО/МЭК 14888-1).

3.1.3. Ключ проверки (verification key): Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи (ИСО/МЭК 14888-1).

3.1.4. Параметр схемы ЭЦП (domain parameter): Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам (ИСО/МЭК 14888-1).

3.1.5. Подписанное сообщение (signed message): Набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения.

3.1.6. Последовательность псевдослучайных чисел (pseudo-random number sequence): Последовательность чисел, полученная в результате выполнения некоторого арифметического (вычислительного) процесса, используемая в конкретном случае вместо последовательности случайных чисел (ИСО 2382-2).

3.1.7. Последовательность случайных чисел (random number sequence): Последовательность чисел, каждое из которых не может быть предсказано (вычислено) только на основе знания предшествующих ему чисел данной последовательности (ИСО 2382-2).

3.1.8. Процесс проверки подписи (verification process): Процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки и параметры схемы ЭЦП и результатом которого является заключение о правильности или ошибочности цифровой подписи (ИСО/МЭК 14888-1).

3.1.9. Процесс формирования подписи (signature process): Процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП, а в результате формируется цифровая подпись (ИСО/МЭК 14888-1).

3.1.10. Свидетельство (witness): Элемент данных, представляющий соответствующее доказательство достоверности (недостоверности) подписи проверяющей стороне (ИСО/МЭК 14888-1).

3.1.11. Случайное число (random number): Число, выбранное из определенного набора чисел таким образом, что каждое число из данного набора может быть выбрано с одинаковой вероятностью (ИСО 2382-2).

3.1.12. Сообщение (message): Строка бит ограниченной длины (ИСО/МЭК 9796).

3.1.13. Хэш-код (hash-code): Строка бит, являющаяся выходным результатом хэш-функции (ИСО/МЭК 148881-1).

3.1.14. Хэш-функция (hash-function): Функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

1) по данному значению функции сложно вычислить исходные данные, отображенные в это значение;

2) для заданных исходных данных трудно найти другие исходные данные, отображаемые с тем же результатом;

3) трудно найти какую-либо пару исходных данных с одинаковым значением хэш-функции.

Примечание. Применительно к области ЭЦП свойство 1 подразумевает, что по известной ЭЦП невозможно восстановить исходное сообщение; свойство 2 подразумевает, что для заданного подписанного сообщения трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же ЭЦП, свойство 3 подразумевает, что трудно подобрать какую-либо пару сообщений, имеющих одну и ту же подпись.

3.1.15. [Электронная] цифровая подпись (digital signature): Строка бит, полученная в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

Примечание. В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями, установлено, что термины «цифровая подпись» и «электронная цифровая подпись (ЭЦП)» являются синонимами.

3.2. Обозначения.

В настоящем стандарте использованы следующие обозначения:

 – множество всех двоичных векторов длиной 256 бит;

 – множество всех двоичных векторов произвольной конечной длины;

Z – множество всех целых чисел;

*р* – простое число, *р* > 3;

 – конечное простое поле, представляемое как множество из *р* целых чисел ;

*b* (mod *р) –* минимальное неотрицательное число, сравнимое с *b* по модулю *р*;

*М* – сообщение пользователя, ;

 – конкатенация (объединение) двух двоичных векторов;

*а*, *b* – коэффициенты эллиптической кривой;

*т* – порядок группы точек эллиптической кривой;

*q* – порядок подгруппы группы точек эллиптической кривой;

*О* – нулевая точка эллиптической кривой;

*Р* – точка эллиптической кривой порядка *q*;

*d* – целое число – ключ подписи;

*Q* – точка эллиптической кривой – ключ проверки;

 – цифровая подпись под сообщением *М*.

4. Общие положения

Общепризнанная схема (модель) цифровой подписи (см. 6 ИСО/МЭК 14888-1) охватывает три процесса:

- генерация ключей (подписи и проверки);

- формирование подписи;

- проверка подписи.

В настоящем стандарте процесс генерации ключей (подписи и проверки) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию.

Механизм цифровой подписи определяется посредством реализации двух основных процессов (см. раздел 6):

- формирование подписи (см. 6.1);

- проверка подписи (см. 6.2).

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществить контроль целостности передаваемого подписанного сообщения,

- доказательно подтвердить авторство лица, подписавшего сообщение,

- защитить сообщение от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 1.



Рисунок 1 – Схема подписанного сообщения

Поле «текст», показанное на данном рисунке и дополняющее поле «цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем, а также хэш-функции….

Цифровая подпись, представленная в виде двоичного вектора длиной 512 бит, должна вычисляться с помощью определенного набора правил, изложенных в 6.1…

5. Математические соглашения

Для определения схемы цифровой подписи необходимо описать базовые математические объекты, используемые в процессах ее формирования и проверки. В данном разделе установлены основные математические определения и требования, накладываемые на параметры схемы цифровой подписи.

5.1. Математические определения.

Пусть задано простое число *р* > 3. Тогда эллиптической кривой *Е*, определенной над конечным простым полем , называется множество пар чисел , , удовлетворяющих тождеству



где  и  не сравнимо с нулем по модулю *р*.

Инвариантом эллиптической кривой называется величина , удовлетворяющая тождеству



Коэффициенты  эллиптической кривой *Е*, по известному инварианту , определяются следующим образом:



где ,  или 1728.

Пары , удовлетворяющие тождеству (1), называются точками эллиптической кривой *Е*; *х* и *у* – соответственно *x*- и *y*-координатами точки.

Точки эллиптической кривой будем обозначать  или просто *Q*. Две точки эллиптической кривой равны, если равны их соответствующие *x*- и *y*-координаты.

На множестве всех точек эллиптической кривой *Е* введем операцию сложения, которую будем обозначать знаком «+». Для двух произвольных точек  и  эллиптической кривой *Е* рассмотрим несколько вариантов.

Пусть координаты точек  и  удовлетворяют условию . В этом случае их суммой будем называть точку , координаты которой определяются сравнениями



где .

Если выполнены равенства  и , то определим координаты точки  следующим образом:



где .

В случае, когда выполнено условие  и , сумму точек  и  будем называть нулевой точкой *O*, не определяя ее *x*- и *y*-координаты. В этом случае точка  называется отрицанием точки . Для нулевой точки *O* выполнены равенства



где  – произвольная точка эллиптической кривой *Е*.

Относительно введенной операции сложения множество всех точек эллиптической кривой *Е*, вместе с нулевой точкой, образуют конечную абелеву (коммутативную) группу порядка *m*, для которого выполнено неравенство



Точка *Q* называется точкой кратности *k*, или просто кратной точкой эллиптической кривой *Е*, если для некоторой точки *Р* выполнено равенство



5.2. Параметры цифровой подписи.

Параметрами схемы цифровой подписи являются:

- простое число *р* – модуль эллиптической кривой, удовлетворяющее неравенству . Верхняя граница данного числа должна определяться при конкретной реализации схемы цифровой подписи;

- эллиптическая кривая *Е*, задаваемая своим инвариантом  или коэффициентами ;

- целое число *m* – порядок группы точек эллиптической кривой *Е*;

- простое число *q* – порядок циклической подгруппы группы точек эллиптической кривой *Е*, для которого выполнены следующие условия:



- точка  эллиптической кривой *Е*, с координатами , удовлетворяющая равенству ;

-хэш-функция , отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные вектора длины 256 бит. Хэш-функция определена в ГОСТ Р 34.11-94.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

- ключом подписи – целым числом *d*, удовлетворяющим неравенству 0 < *d* < *q*;

- ключом проверки – точкой эллиптической кривой *Q* с координатами , удовлетворяющей равенству .

На приведенные выше параметры схемы цифровой подписи накладываются следующие требования:

- должно быть выполнено условие , для всех целых , где *B* удовлетворяет неравенству ;

- должно быть выполнено неравенство ;

- инвариант кривой должен удовлетворять условию  или 1728.

5.3. Двоичные векторы.

Для определения процессов формирования и проверки цифровой подписи необходимо установить соответствие между целыми числами и двоичными векторами длины 256 бит.

Рассмотрим следующий двоичный вектор длиной 256 бит, в котором младшие биты расположены справа, а старшие – слева:



где  равно либо 1, либо 0. Будем считать, что число  соответствует двоичному вектору , если выполнено равенство



Для двух двоичных векторов  и , соответствующих целым числам  и , определим операцию конкатенации (объединения) следующим образом. Пусть



тогда их объединение имеет вид



и представляет собой двоичный вектор длиной 512 бит, составленный из коэффициентов векторов  и .

С другой стороны, приведенные формулы определяют способ разбиения двоичного вектора  длиной 512 бит на два двоичных вектора длиной 256 бит, конкатенацией которых он является.

6. Основные процессы

…6.1. Формирование цифровой подписи.

Для получения цифровой подписи под сообщением  необходимо выполнить следующие действия (шаги) по алгоритму I.

Шаг 1 – вычислить хэш-код сообщения *M*: . (14)

Шаг 2 – вычислить целое число , двоичным представлением которого является вектор , и определить



Если *e* = 0, то определить *e* = 1.

Шаг 3 – сгенерировать случайное (псевдослучайное) целое число *k*, удовлетворяющее неравенству



Шаг 4 – вычислить точку эллиптической кривой *С* = *kP* и определить



где  – *x*-координата точки *С*. Если *r* = 0, то вернуться к шагу 3.

Шаг 5 – вычислить значение



Если *s* = 0, то вернуться к шагу 3.

Шаг 6 – вычислить двоичные векторы  и , соответствующие *r* и *s*, и определить цифровую подпись  как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи *d* и подписываемое сообщение *М*, а выходным результатом — цифровая подпись .

Схематическое представление процесса формирования цифровой подписи приведено на рисунке 2.



Рисунок 2 – Схема процесса формирования цифровой подписи

6.2. Проверка цифровой подписи.

Для проверки цифровой подписи  под полученным сообщением *М* необходимо выполнить следующие действия (шаги) по алгоритму II.

Шаг 1 – по полученной подписи  вычислить целые числа *r* и *s*. Если выполнены неравенства , , то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2 – вычислить хэш-код полученного сообщения *М*:



Шаг 3 – вычислить целое число , двоичным представлением которого является вектор , и определить



Если *е* = 0, то определить *е* = 1.

Шаг 4 – вычислить значение . (21)

Шаг 5 – вычислить значения



Шаг 6 – вычислить точку эллиптической кривой  и определить



где  – *x*-координата точки *С*.

Шаг 7 – если выполнено равенство *R* = *r*, то подпись принимается, в противном случае, подпись неверна.

Исходными данными этого процесса являются подписанное сообщение *М*, цифровая подпись  и ключ проверки *Q*, а выходным результатом — свидетельство о достоверности или ошибочности данной подписи.

Схематическое представление процесса проверки цифровой подписи приведено на рисунке 3.



Рисунок 3 – Схема процесса проверки цифровой подписи

Приложение А (справочное)

Дополнительные термины в области ЭЦП

В настоящем приложении приведены дополнительные международные термины, применяемые в рассматриваемой и смежных областях.

А.1. Заполнение (padding): Дополнение строки данных лишними битами (ИСО/МЭК 10118-1).

А.2. Идентификационные данные (identification data): Последовательность элементов данных, включая отличительный идентификатор объекта, принадлежащая объекту и используемая для его обозначения (ИСО/МЭК 148881-1).

А.З. Уравнение цифровой подписи (signature equation): Уравнение, определяемое функцией цифровой подписи (ИСО/МЭК 148881-1).

А.4. Функция проверки (verification function): Функция процесса проверки, определяемая ключом проверки, выдающая в качестве результата вычисленное значение свидетельства о достоверности подписи (ИСО/МЭК 148881-1).

А.5. Функция цифровой подписи (signature function): Функция в процессе формирования подписи, определяемая ключом подписи и параметрами схемы ЭЦП. Эта функция в качестве исходных данных получает часть исходных данных и, возможно, формирователь последовательности псевдослучайных чисел (рандомизатор), а в результате выдает вторую часть цифровой подписи.

Приложение Б (справочное)

Контрольный пример

Данное приложение носит справочный характер и не является частью стандарта. Приводимые ниже значения параметров *р*, *a*, *b*, *m*, *q*, *Р*, а также значения ключей подписи и проверки *d* и *Q* рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящем стандарте.

Все числовые значения приведены в десятичной и шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления. Символ "\\" обозначает перенос числа на новую строку. Например, запись

12345\\

6789010

499602D216

представляет целое число 1234567890, соответственно, в десятичной и шестнадцатеричной системах счисления.

Б.1. Параметры схемы цифровой подписи.

Для формирования и проверки цифровой подписи должны быть использованы следующие параметры (см. 5.2).

Б.1.1. Модуль эллиптической кривой.

В данном примере параметру *р* присвоено следующее значение:

*р* = 57896044618658097711785492504343953926\\

63499233282028201972879200395656482104110

*р* = 800000000000000000000000000000000000000000000000000000000000043116

Б.1.2 Коэффициенты эллиптической кривой.

В данном примере параметры *а* и *b* принимают следующие значения:

*а* = 710

*а* = 716

*b* = 43308876546767276905765904595650931995\\ 94211179445103958325296884203384958041410

*b* = 5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514C0CE9DAE23B7E16

Б.1.3. Порядок группы точек эллиптической кривой.

В данном примере параметр *m* принимает следующее значение:

*m* = 5789604461865809771178549250434395392\\

708293458372545062238097359213763106961910

*m* = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B316

Б.1.4. Порядок циклической подгруппы группы точек эллиптической кривой.

В данном примере параметр *q* принимает следующее значение:

*q* = 5789604461865809771178549250434395392\\

708293458372545062238097359213763106961910

*q* = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B316

Б.1.5. Коэффициенты точки эллиптической кривой.

В данном примере координаты точки *Р* принимают следующие значения:

*хр* = 210

*хр* = 216

*ур* = 40189740565390375033354494229370597\\

7563573938990554508069097936521343156628010

*ур* = 8E2A8A0E65147D4BD6316030E16D19\\ C85C97F0A9CA267122B96ABBCEA7E8FC816

Б.1.6. Ключ подписи.

В данном примере считается, что пользователь обладает следующим ключом подписи *d*:

*d* = 554411960653632461263556241303241831\\

9657670922234001657210809775000609752554410

*d* = 7A929ADE789BB9BE10ED359DD39A72C\\

11B60961F49397EEE1D19CE9891EC3B2816

Б.1.7. Ключ проверки.

В данном примере считается, что пользователь обладает ключом проверки *Q*, координаты которого имеют следующие значения:

*xq* = 57520216126176808443631405023338071\\ 17663010490631363218289674134220660485940310

*xq* = 7F2B49E270DB6D90D8595BEC458B5\\

0C58585BA1D4E9B788F6689DBD8E56FD80B16

*yq* = 17614944419213781543809391949654080\\

03194266204536363926070984785943828676399410

*yq* = 26F1B489D6701DD185C8413A977B3\\ CBBAF64D1C593D26627DFFB101A87FF77DA16

Б.2. Процесс формирования цифровой подписи (алгоритм I).

Пусть после выполнения шагов 1 – 3 по алгоритму I (6.1) были получены следующие числовые значения:

*е* = 2079889367447645201713406156150827013\\ 063714251537965328995261725266146887242110

*е* = 2DFBC1B372D89A1188C09C52E0EE\\

C61FCE52032AB1022E8E67ECE6672B043EE516

*k* = 538541376773484637314038411479966192\\ 4150400343430202071296083852889319623339510

*k* = 77105C9B20BCD3122823C8CF6FCC\\

7B956DE33814E95B7FE64FED924594DCEAB316

При этом кратная точка *С* = *kP* имеет координаты:

*хC* = 297009809158179528743712049839382569\\ 9042275210799431965163268798205921093339510

*хC* = 41AA28D2F1AB148280CD9ED56FED\\ A41974053554A42767B83AD043FD39DC049316

*уC* = 328425352786846634770946653225170845\\ 0680472103245454326813285455653927406091010

*уC* = 489C375A9941A3049E33B34361DD\\

204172AD98C3E5916DE27695D22A61FAE46E16

Параметр  принимает значение:

*r* = 297009809158179528743712049839382569\\

9042275210799431965163268798205921093339510

*r* = 41AA28D2F1AB148280CD9ED56FED\\

A41974053554A42767B83AD043FD39DC049316

Параметр  принимает значение:

*s* = 57497340027008465417892531001914703\\ 845522704264909856393371899917551583955210

*s* = 1456C64BA4642A1653C235A98A60249BCD6D3F746B631DF928014F6C5BF9C4016

Б.3. Процесс проверки цифровой подписи (алгоритм II).

Пусть после выполнения шагов 1 – 3 по алгоритму II (6.2) было получено следующее числовое значение:

*е* = 2079889367447645201713406156150827013\\ 063714251537965328995261725266146887242110

*е* = 2DFBC1B372D89A1188C09C52E0EE\\

C61FCE52032AB1022E8E67ECE6672B043EE516

При этом параметр  принимает значение:

*v* = 176866836059344686773017138249002685\\

6274688308067549671528803657243114571897810

*v* = 271A4EE429F84EBC423E388964555BB\\

29D3BA53C7BF945E5FAC8F381706354C216

Параметры  и  принимают значения:

*z*1 = 376991675009019385568410572935126561\\

0884134519049194261930453241274372099975910

*z*1 = 5358F8FFB38F7C09ABC782A2DF2A\\

3927DA4077D07205F763682F3A76C9019B4F16

*z*2 = 141719984273434721125159179695007657\\

692466558389728621144999326533336710922110

*z*2 = 3221B4FBBF6D101074EC14AFAC2D4F7\\ EFAC4CF9FEC1ED11BAE336D27D52766516

Точка  имеет координаты:

*xC* = 2970098091581795287437120498393825699\\ 042275210799431965163268798205921093339510

*xC* = 41AA28D2F1AB148280CD9ED56FED\\ A41974053554A42767B83AD043FD39DC049316

*уC* = 3284253527868466347709466532251708450\\ 680472103245454326813285455653927406091010

*уC* = 489C375A9941A3049E33B34361DD\\

204172AD98C3E5916DE27695D22A61FAE46E16

Тогда параметр  принимает значение:

*R* = 2970098091581795287437120498393825699\\ 042275210799431965163268798205921093339510

*R* = 41AA28D2F1AB148280CD9ED56FED\\ A41974053554A42767B83AD043FD39DC049316

Поскольку выполнено равенство *R* = *r*, то цифровая подпись принимается.

**ПРИЛОЖЕНИЕ 2**

**Выдержки из Федерального Закона** 6 апреля 2011 года N 63-ФЗ

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

3) квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

4) владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

9) средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

10) средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

12) корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Статья 3. Правовое регулирование отношений в области использования электронных подписей

1. Отношения в области использования электронных подписей регулируются настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между участниками электронного взаимодействия. ….

Статья 5. Виды электронных подписей

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

2. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

3. Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

5. При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Статья 6. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью….

Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). …

Статья 9. Использование простой электронной подписи

1. Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

1) простая электронная подпись содержится в самом электронном документе;

2) ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

2. Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

1) правила определения лица, подписывающего электронный документ, по его простой электронной подписи;

2) обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность….

Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Статья 11. Признание квалифицированной электронной подписи

Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;

4) квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены).

Статья 12. Средства электронной подписи

1. Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:

1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

2. При создании электронной подписи средства электронной подписи должны:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

3) однозначно показывать, что электронная подпись создана.

3. При проверке электронной подписи средства электронной подписи должны:

1) показывать содержание электронного документа, подписанного электронной подписью;

2) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

3) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

4. Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих сведения, составляющие государственную тайну, или предназначенные для использования в информационной системе, содержащей сведения, составляющие государственную тайну, подлежат подтверждению соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации. Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

5. Требования [частей 2](consultantplus://offline/main?base=LAW;n=112701;fld=134;dst=100098) и [3](consultantplus://offline/main?base=LAW;n=112701;fld=134;dst=100102) настоящей статьи не применяются к средствам электронной подписи, используемым для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Статья 13. Удостоверяющий центр

1. Удостоверяющий центр:

1) создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям);

2) устанавливает сроки действия сертификатов ключей проверки электронных подписей;

3) аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

4) выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5) ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

7) создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

10) осуществляет иную связанную с использованием электронной подписи деятельность….

Статья 14. Сертификат ключа проверки электронной подписи

1. Удостоверяющий центр осуществляет создание и выдачу сертификата ключа проверки электронной подписи на основании соглашения между удостоверяющим центром и заявителем….