Федеральное агентство по образованию

Сибирский государственный аэрокосмический университет

имени академика М. Ф. Решетнева

ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОГРАФИИ

Жданов О. Н .

Чалкин Т. А.

Содержание

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

В последние два десятилетия все большее применение в криптографии находит одна из областей теории чисел и алгебраической геометрии – теория эллиптических кривых над конечными полями. Основная причина этого состоит в том, что эллиптические кривые над конечными полями доставляют неисчерпаемый источник конечных абелевых групп, которые (даже если они велики) удобны для вычислений и обладают богатой структурой. 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.

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. Основные факты

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 E_q из $q = p^r$ элементов. Напомним, что характеристикой поля K называется такое натуральное число $p = \mathrm{char}\, K$, что $p \cdot 1 = 0$, где 1 и 0 – единичный и нулевой элементы K соответственно.

Определение. Пусть K – поле характеристики, отличной от 2 и 3, и $x^3 + ax + b$ (где $a, b \in K$) – кубический многочлен без кратных корней. *Эллиптическая кривая над K* – это множество точек (x, y) (где $x, y \in K$), удовлетворявших уравнению

$$y^2 = x^3 + ax + b, \quad (1)$$

вместе с единственным элементом, обозначаемым O и называемым «точка в бесконечности» (о ней подробнее будет сказано ниже).

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

$$y^2 + cy = x^3 + ax + b, \quad (2а)$$

либо типа

$$y^2 + xy = x^3 + ax^2 + b \quad (2б)$$

(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

$$y^2 = x^3 + ax^2 + bx + c \quad (3)$$

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

Замечания.

1. Имеется общая форма уравнения эллиптической кривой, которая применима для поля любой характеристики: $y^2 + a_1xy + a_3y = x^2 + a_2x^2 + a_4x + a_6$: в случае, когда $\mathrm{char}\, K \neq 2$, ее можно привести к виду $y^2 = x^3 + ax^2 + bx + c$ (или к виду $y^2 = x^3 + bx + c$, если $\mathrm{char}\, K > 3$). В случае, когда поле K имеет характеристику 2, это уравнение преобразуется либо к виду (2а), либо к виду (2б).

2. Если $F(x, y) = 0$ – неявное уравнение, выражающее y как функцию x в (1) (или в (2), (3)), т. е.

$$F(x, y) = y^2 - x^3 - ax - b$$

(или $F(x, y) = y^2 + cy + x^3 - ax + b$, $y^2 + xy + x^3 + ax + b$, $y^2 - x^3 - ax^2 - bx - c$),

то точка (x, y) этой кривой называется *неособенной* (или *гладкой*) точкой, если, по крайней мере, одна из частных производных $\partial F / \partial x, \partial F / \partial y$ в этой точке не равна нулю (производные многочленов можно определить обычными формулами над любым полем).

Нетрудно показать, что условие отсутствия кратных корней у кубических многочленов в правой части в (1) и (3) эквивалентно требованию, чтобы все точки кривой были неособенными.

Эллиптические кривые над полем вещественных чисел.

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 E – эллиптическая кривая над вещественными числами, и пусть P и Q – две точки на E. 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 x-координаты, а их y-координаты различаются только знаком, т.е. $-(x, y) = (x, -y)$. Из (1) сразу следует, что $(x, -y)$ – также точка на E.

3. Если P и Q имеют различные x-координаты, то прямая $l = \overline{PQ}$ имеет с E еще в точности одну точку пересечения R (за исключением двух случаев: когда она оказывается касательной в P, 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 1.

4. Если $Q = -P$ (т. е. x-координата Q та же, что и у 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 E. 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 1. На рис. 1 слева изображена эллиптическая кривая $y^2 = x^3 - x$ в плоскости xOy и приведен типичный случай сложения точек P и Q. Чтобы найти $P + Q$, проводим прямую $\overline{PQ}$ и в качестве $P + Q$ берем точку, симметричную относительно оси x третьей точке, определяемой пересечением прямой $\overline{PQ}$ и кривой. Если бы P совпадала 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.

На рис. 1 справа аналогичным образом проиллюстрировано сложение точек R и Q на кривой $y^2 = x^3 + x + 1$.

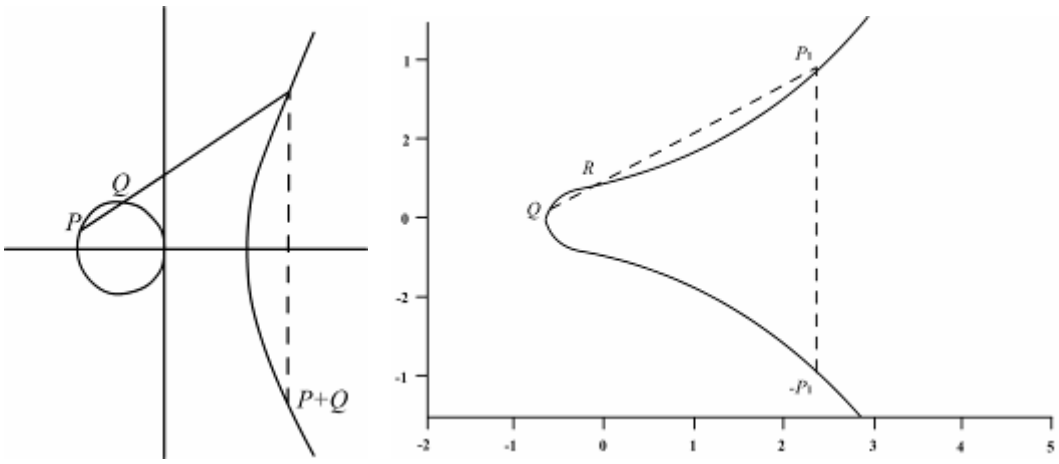

Рис. 1. Примеры геометрического построения суммы точек эллиптической кривой

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 (x_1, y_1), (x_2, y_2) и (x_3, y_3) – координаты точек *P*, *Q* и *P*+*Q* соответственно. Мы хотим выразить x_3 и y_3 через x_1, y_1, x_2 и y_2.

Предположим, что мы находимся в ситуации п. 3 определения операции сложения точек, и пусть $y = \alpha x + \beta$ есть уравнение прямой, проходящей через *P* и *Q* (в этой ситуации она не вертикальна). Тогда $\alpha = (y_2 - y_1)/(x_2 - x_1)$ и $\beta = y_1 - \alpha x_1$. Точка на *l*, т. е. точка $(x, \alpha x + \beta)$, лежит на эллиптической кривой тогда и только тогда, когда

$$(\alpha x + \beta)^2 = x^3 + ax + b.$$

Таким образом, каждому корню кубического многочлена $x^3 - (\alpha x + \beta)^2 + ax + b$ соответствует точка пересечения. Мы уже знаем, что имеется два корня x_1 и x_2, так как $(x_1, \alpha x_1 + \beta)$ и $(x_2, \alpha x_2 + \beta)$ – точки *P* 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 $x_3 = \alpha^2 - x_1 - x_2$. Тем самым получаем выражение для x_3, и, следовательно, $P + Q = (x_3, (ax_3 + \beta))$, или, в терминах x_1, y_1, x_2, y_2:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad (4)$$

$$y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3).$$

Ситуация в п. 5 аналогична рассмотренной, только теперь α – производная dy/dx в точке *P*. Дифференцирование неявной функции, заданной уравнением (1), приводит к формуле $\alpha = (3x_1^2 + a)/2y_1$, и мы получаем следующие формулы для координат удвоенной точки:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \quad (5)$$

$$y_3 = -y_1 + \frac{3x_1^2 + a}{2y_1}(x_1 - x_3).$$

Пример 2. Пусть *P* = (-3, 9) и *Q* = (-2, 8) – точки на эллиптической кривой $y^2 = x^3 - 36x$. Найти *P* + *Q* и 2*P*.

Решение. Подстановка $x_1 = -3, y_1 = 9, x_2 = -2, y_2 = 8$ в первое из уравнений (4) дает $x_3 = 6$; тогда второе из уравнений (4) дает $y_3 = 0$. Непосредственной подстановкой координат точки $P + Q = (6, 0)$ в уравнение кривой можно убедиться в том, что она также лежит на ней. Далее, подставляя $x_1 = -3$, $y_1 = 9$, $a = -36$ в первое из уравнений (5), получаем для x-координаты точки $2P$ значение 25/4, а второе из уравнений (5) дает для y-координаты значение -35/8. Точка $2P = (25/4, -35/8)$ 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, nP обозначает сумму n точек P при $n > 0$ и сумму $|n|$ точек $-P$, если $n \le 0$.

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 (x_1, y_1), $(x_1, -y_1)$ 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. (λX, λY, λZ) ~ (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 (x, y, 1): просто полагаем $x = X/Z$, $y = Y/Z$. Тем самым проективную плоскость можно представить как объединение всех точек (x, y) 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 $\tilde{F}(X, Y, Z) = 0$, которому удовлетворяют соответствующие проективные точки: нужно заменить x 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» $Y^2Z = X^3 + aXZ^2 + bZ^3$. Этому уравнению удовлетворяют все проективные точки (X, Y, Z) с $Z \neq 0$, для которых соответствующие аффинные точки (x, y), где $x = X/Z$, $y = Y/Z$, удовлетворяют (1). Помимо них, какие еще точки бесконечно удаленной прямой удовлетворяют последнему уравнению? Если положить в уравнении $Z = 0$, то уравнение примет вид $X^3 = 0$, 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 y с бесконечно удаленной прямой.

Эллиптические кривые над полем комплексных чисел.

Алгебраические формулы (4)-(5) 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, исходя из уравнений (2) или (3). Можно показать, что точки эллиптической кривой над любым полем образуют абелеву группу по сложению, определенную по этим формулам.

В частности, пусть E – эллиптическая кривая, определенная над полем C комплексных чисел, т. е. E – множество пар (x, y) комплексных чисел, удовлетворяющих уравнению (1), вместе с точкой в бесконечности O. Мы называем E «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 E 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 ω_1 и ω_2 (где ω_1 и ω_2 «заметают» плоскость, т.е. не лежат на одной прямой, проходящей через начало координат): $L = Z\omega_1 + Z\omega_2$ (здесь Z – множество целых чисел). Например, если $\omega_1 = 1$, $\omega_2 = i$, 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 «$\wp$-функцией Вейерштрасса» и обозначаемая $\wp_L(z)$, со следующими свойствами:

1. $\wp(z)$ аналитична всюду, кроме точек L, в каждой из которых имеет полюс второго порядка.

2. $\wp(z)$ удовлетворяет дифференциальному уравнению $\wp'^2 = \wp^3 + a\wp + b$ и, следовательно, при любом $z \notin L$ точка $(\wp(z), \wp'(z))$ лежит на эллиптической кривой E.

3. Два комплексных числа z_1 и z_2 дают одну и ту же точку $(\wp(z), \wp'(z))$ на E тогда и только тогда, когда $z_1 - z_2 \in L$.

4. Отображение, которое любой точке $z \notin L$ ставит в соответствие точку $(\wp(z), \wp'(z))$ на E, а любой точке $z \in L$ – точку в бесконечности O, дает взаимно однозначное соответствие между E и факторгруппой C/L комплексной плоскости по подгруппе L.

5. Это взаимно однозначное соответствие есть изоморфизм абелевых групп, иными словами, если z_1 соответствует точке $P \in E$ а z_2 – точке $Q \in E$, то $z_1 + z_2$ соответствует точке $P + Q$.

Таким образом, можно представлять себе абелеву группу E как комплексную плоскость «по модулю» некоторой решетки. Чтобы эту последнюю группу изобразить наглядно, заметим, что у каждого класса эквивалентности $z + L$ существует один и только один представитель в «фундаментальном параллелограмме», состоящем из комплексных чисел вида $a\omega_1 + b\omega_2$, $0 \le a, b < 1$ (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. 2.

Как группа, тор есть произведение двух экземпляров группы окружности, т.е. его точки можно параметризовать парой углов (α, β). Точнее, если тор получен из решетки $L = Z\omega_1 + Z\omega_2$, то следует представить элемент из C/L в виде $a\omega_1 + b\omega_2$, полагая $a = 2\pi\alpha$, $b = 2\pi\beta$. Таким образом, можно рассматривать эллиптическую кривую над комплексными числами как двумерное обобщение окружности в вещественной плоскости.

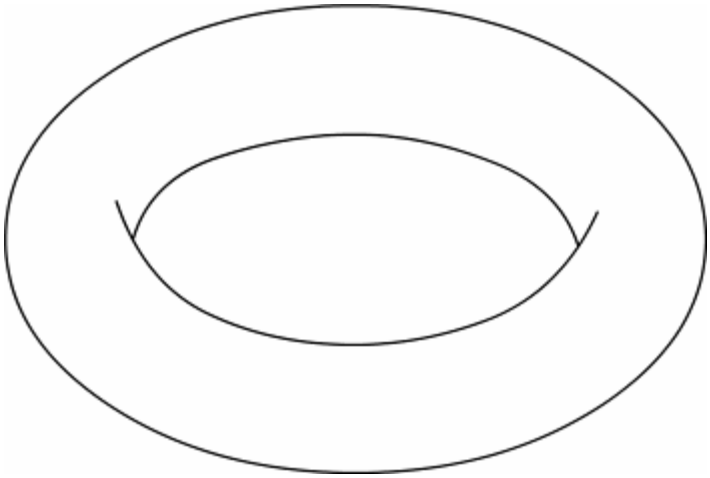

Рис. 2. Геометрическая интерпретация эллиптической кривой
над полем комплексных чисел

Фактически эта аналогия идет значительно дальше, чем может показаться. «Эллиптические функции» (которые показывают, как по точке $(x, y) \in E$ найти то комплексное число z, для которого $(x, y) = (\wp(z)', \wp(z))$), 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 $nP = O$) и точками, делящими на n частей единичную окружность (которые соответствуют корням степени n из единицы в комплексной плоскости).

Точки конечного порядка.

Порядком n точки P на эллиптической кривой называется такое наименьшее натуральное число, что $nP = 0$; 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 3. Найти порядок точки $P = (2, 3)$ на $y^2 = x^3 + 1$.

Решение. Применяя (5), находим, что $2P = (0, 1)$, и вновь, с помощью (5), что $4P = 2(2P) = (0, -1)$. Поэтому $4P = -2P$ и, следовательно, $6P = O$. Тем самым порядок P может быть равен 2, 3 или 6. Но $2P = (0,1) \neq O$, а если бы P имела порядок 3, то было бы $4P = P$, что неверно. Итак, P 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. Теория эллиптических кривых над полем рациональных чисел очень обширна. Было доказано, что соответствующие абелевы группы являются конечнопорожденными (теорема Морделла). Это означает, что каждая из таких групп есть сумма конечной «подгруппы кручения» Tors$E(Q)$ (точек конечного порядка) и подгруппы, порожденной конечным числом точек бесконечного порядка: $E(Q) \cong Z^r \oplus \mathrm{Tors}\, E(Q)$. 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 $y^2 = x^3 - n^2 x$ больше нуля?» Случай n = 6 и прямоугольного треугольника со сторонами 3, 4 и 5 соответствует точке P = (-3, 9) из примера 2, которая является точкой бесконечного порядка на эллиптической кривой $y^2 = x^3 - 36x$.

Эллиптические кривые над конечным полем.

Будем предполагать, что K – конечное поле F_q, с $q = p^r$ элементами. Пусть E – эллиптическая кривая, определенная над F_q. Если p = 2 или 3, то E задается уравнением вида (2) или (3) соответственно.

Легко усмотреть, что эллиптическая кривая может иметь не более $2q + 1$ различных F_q-точек, т.е. точку в бесконечности и не более чем $2q$ пар (x, y), $x, y \in F_q$, удовлетворяющих (1) (или (2) или (3), если p = 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 F_q^* имеются квадратные корни, естественно ожидать (если бы $x^3 + ax + b$ были случайными элементами поля), что количество F_q-точек примерно вдвое меньше этого числа. Точнее, пусть χ – квадратичный характер F_q. Это – отображение, переводящее $x \in F_q^*$ в 1 или -1 в зависимости от того, является или нет элемент x квадратом элемента из F_q (полагаем также $\chi(0) = 0$). Например, если q – это простое число p, то $\chi(x) = \left(\frac{x}{p}\right)$ называется символом Лежандра. В любом случае число решений $y \in F_q$ уравнения $y^2 = u$ равно $1 + \chi(u)$ и, значит, число решений (1) (с учетом точки в бесконечности) равно

$$1 + \sum_{x \in F_q} (1 + \chi(x^3 + ax + b)) = q + 1 + \sum_{x \in F_q} \chi(x^3 + ax + b) \quad (6)$$

Следует ожидать, что $\chi(x^3 + ax + b)$ 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 $\sqrt{q}$ от исходного положения. Сумма $\sum \chi(x^3 + ax + b)$ ведет себя в чем-то аналогично случайному блужданию. Точнее, удалось доказать, что она ограничена величиной $2\sqrt{q}$. Этот результат – теорема Хассе.

Теорема Хассе. Пусть N – число F_q-точек на эллиптической кривой, определенной над F_q. Тогда

$$\left|N - (q+1)\right| \le 2\sqrt{q}\,.$$

В дополнение к числу N элементов на эллиптической кривой над F_q 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 p-примарных групп вида $Z / p^\alpha Z \times Z / p^\beta Z$, где произведение берется по всем простым делителям N (здесь $\alpha \ge 1, \beta \ge 0$). Под типом абелевой группы F_q-точек на E мы понимаем список $\left(\ldots, p^\alpha, p^\beta, \ldots\right)_{p|N}$ – порядков циклических p-примарных сомножителей в упомянутом представлении в виде произведения (если $\beta = 0$, то p^β опускаем). Найти тип не всегда легко.

Пример 4. Найти тип для кривой $y^2 = x^3 - x$ над F_{71}.

Решение. Находим сначала число точек *N*. Из свойств квадратичного характера $\chi(a)\chi(b) = \chi(ab)$ и χ (-1) = -1 следует, что в сумме (6) члены для *x* и для -*x* взаимно уничтожаются: $\chi((-x)^3 - (-x)) = \chi(-1)\chi(x^3 - x) = -\chi(x^3 - x)$. Следовательно, *N* = *q* + 1 = 72. Далее, имеется в точности четыре точки порядка 2 (включая «бесконечную» точку *O*): они соответствуют корням многочлена $x^2 - x = x(x+1)(x-1)$ (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 $3P = O$ при $P \neq O$ эквивалентно условию $2P = \pm P$, т.е. тому, что *x*-координаты точек 2*P* и *P* одинаковы. Согласно (5) это означает, что $((3x^2 - 1)/(2y))^2 - 2x = x$, т.е. $(3x^2 - 1)^2 = 12xy^2 = 12x^4 - 12x^2$. Упрощая, получаем $3x^4 - 6x^2 - 1 = 0$ Это уравнение имеет, самое большее, 4 корня в F_{71}. Каждый корень может давать не более двух точек (при $y = \sqrt{x^3 - x}$, если $x^3 - x$ 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 $x^3 - x$ есть квадрат по модулю 71, то для другого его корня -*x* получаем, что $(-x)^3 - (-x) = -(-x^3 - x)$ 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 F_q, то она определена также над F_{q^r}, *r* = 1,2,… и имеет смысл рассматривать F_{q^r}-точки, т.е. решения (1) над расширениями поля. Отправляясь от поля F_q как поля, над которым задана *E*, определяем число N_r как число F_{q^r}-точек на *E* (таким образом, $N_1 = N$ есть число точек с координатами в нашем «основном поле» F_q).

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

$$Z(T; E/F_q) = e^{\sum N_r T^r / r}, \quad (7)$$

где *T* – неизвестная; обозначение E/F_q 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 $e^{\sum N_r T^r / r}$) имеет положительные целые коэффициенты. Этот степенной ряд называется *дзета-функцией* эллиптической кривой (над F_q) и представляет собой весьма важный объект, связанный с *E*.

«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/F_q Вейль (A. Weil) доказал следующее утверждение:

Гипотеза (теорема) Вейля для эллиптической кривой. Дзета-функция есть рациональная функция от *T* вида

$$Z(T; E/F_q) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}, \quad (8)$$

где от эллиптической кривой E зависит лишь целое число a. Значение a связано с числом $N = N_1$ соотношением $N = q + 1 - a$. Кроме того, дискриминант квадратного трехчлена в числителе отрицателен (т.е. $a^2 \le 4q$ – теорема Хассе), таким образом, этот трехчлен имеет два комплексно сопряженных корня α и β, оба по модулю равные $\sqrt{q}$ (точнее, корнями являются $1/\alpha$ и $1/\beta$, а α, β — корни «возвратного» уравнения).

Замечание. Если записать числитель (8) в виде $(1-\alpha T)(1-\beta T)$ и затем взять производную от логарифмов обеих частей (заменяя левую часть по формуле (7), определяющей дзета-функцию), то нетрудно убедиться, что формула (8) эквивалентна последовательности соотношений

$$N_r = q^r + 1 - \alpha^r - \beta^r,\ r = 1,2,...$$

Так как α и β, наряду с a, определяются значением $N = N_i$, то число точек над полем F_q 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.

Пример 5. Легко вычисляется дзета-функция эллиптической кривой $y^2 + y = x^3$ над F_2, так как имеется всего три F_2-точки. Она равна $(1+2T^2)/((1-T)(1-2T))$. Таким образом, обратные корни числителя – это $\pm i\sqrt{2}$. Отсюда следует формула

$$N_r = \begin{cases} 2^r + 1, \text{ если } r \text{ нечетно}, \\ 2^r + 1 - 2(-2)^{r/2}, \text{ если } r \text{ четно}. \end{cases} \quad (9)$$

В заключение этого параграфа заметим, что существует много аналогий между группой F_q-точек на эллиптической кривой и мультипликативной группой F_q^*. 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

1. Пусть E – эллиптическая кривая, определенная над C, уравнение (1) которой имеет коэффициенты $a, b \in R$; 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). Приведите пример для каждой из них.

2. Сколько точек P порядка n (т.е. таких, что $nP = O$) 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 P – точка на эллиптической кривой над R. Предположим, что P не есть точка в бесконечности. Найти геометрическое условие, эквивалентное тому, что P – 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.

а) $P = (0, 16)$ на $y^2 = x^3 + 256$.

б) $P = \left(\frac{1}{2}, \frac{1}{2}\right)$ на $y^2 = x^3 + \frac{1}{4}x$.

в) $P = (3, 8)$ на $y^2 = x^3 - 43x + 166$.

г) $P = (0, 0)$ на $y^2 + y = x^3 - x^2$ (уравнение можно привести к виду (1) заменой переменных $y \to y - \frac{1}{2}$, $x \to x + \frac{1}{3}$).

6. Вывести формулы сложения, аналогичные (4)-(5), для эллиптических кривых над полем характеристики 2, 3 (см. уравнение (2)-(3)).

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

а) $y^2 = x^3 - x$, когда $q \equiv 3 \pmod 4$;

в) $y^2 = x^3 - 1$, когда $q \equiv 2 \pmod 3$ (q нечетно);

г) $y^2 + y = x^3$, когда $q \equiv 2 \pmod 3$ (здесь q может быть четным).

8. Для всех степеней нечетных простых чисел $q = p^r$ до 27 включительно найти порядок и тип группы F_q-точек на эллиптических кривых $y^2 = x^3 - x$ и $y^2 = x^3 - 1$ (в последнем случае – при $p \neq 3$). В некоторых случаях Вам нужно будет проверить, сколько точек имеют порядок 3 или 4.

9. Пусть $q = p^r$ и пусть эллиптическая кривая E над F_q имеет уравнение $y^2 + y = x^3$:

а) Выразить координаты $-P$ и $2P$ в терминах координат P.

б) Показать, что при $q = 16$ каждая $P \in E$ есть точка порядка 3.

в) Показать, что любая точка E с координатами в F_{16} фактически есть точка с координатами в F_4. Далее с помощью теоремы Хассе при $q = 4$ и 16 определить число точек на кривой.

10. Вычислить дзета-функцию упражнения 8 над F_q для p=5, 7, 11, 13.

11. Вычислить дзета-функцию кривой $y^2 + y = x^3 - x + 1$ над F_p для $p = 2$ и 3 (сначала покажите, что в обоих случаях $N_1 = 1$) Пусть $N(x) = x \cdot \bar{x}$ обозначает норму комплексного числа. В терминах нормы найти простую формулу для N_r.

§ 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, хотя теория криптографии с использованием эллиптических кривых у всех на слуху уже в течение достаточно долгого времени, только недавно начали появляться продукты, представляющие интерес для криптоанализа на предмет наличия соответствующих слабых мест. Таким образом, 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 повтор-

ное сложение – **аналогом возведения в 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 F_q. Прежде чем описывать криптосистемы, нужно обсудить некоторые вспомогательные понятия.

Пример эллиптической кривой над конечным полем.

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, *a* и *b*, которые меньше *p* и удовлетворяют условию

$$4a^2 + 27b^2 (\mathrm{mod}\, p) \neq 0$$

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

$$y^2 = x^3 + ax + b (\mathrm{mod}\, p)$$

вместе с «точкой в бесконечности» *O*.

Например, пусть *p* = 23. Рассмотрим эллиптическую кривую $y^2 = x^3 + x + 1$. В этом случае *a* = *b* = 1 и мы имеем $4 \times 1^2 + 27 \times 1^2 (\mathrm{mod}\, 23) = 8 \neq 0$, 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 1 представлены точки (отличные от *O*), являющиеся элементами $E_{23}(1,1)$. В нашем случае такой список можно создать по следующим правилам.

1. Вычисляем значения $y^2 (\mathrm{mod}\, 23)$ (см. таблицу 1).

Таблица 1. Значения $y^2 (\mathrm{mod}\, 23)$ для *y* от 0 до 22

y	$y^2 (\mathrm{mod}\, 23)$
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

2.Вычисляем значения $y^2 = x^3 + x + 1 (\mathrm{mod}\, 23)$ (см. таблицу 2).

Таблица 2. Значения $x^3 + x + 1 (\mathrm{mod}\, 23)$ для *x* от 0 до 22

x	$x^3 + x + 1 (\mathrm{mod}\, 23)$
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

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 1, и в правом столбце таблицы 2. 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 3.. Пара чисел (x, y), для которой $y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p)$, включается в нашу таблицу соответствий: эта пара чисел, т.е. точка кривой, кодирует некоторый символ языка открытых текстов.

Таблица 3. Точки группы $E_{23}(1,1)$

(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)

Далее устанавливаем соответствие символов языка и точек кривой, например, $a \to (0,1)$; $б \to (0,22)$ и т.д.

Кратные точки.

Для эллиптических кривых аналогом умножения двух элементов группы F_q^* служит сложение двух точек эллиптической кривой E, определенной над F_q. Таким образом, аналог возведения в степень к элемента из F_q^* – это умножение точки $P \in E$ на целое число k. Возведение в k-ю степень в F_q^* методом повторного возведения в квадрат можно осуществить за $O(\log k \ \log^3 q)$ двоичных операций. Аналогично мы покажем, что кратное $kP \in E$ можно найти за $O(\log k \ \log^3 q)$ двоичных операций методом повторного удвоения.

Пример 1. Чтобы найти 100P, записываем 100P = 2(2(P + 2(2(2(P + 2P))))) и приходим к цели, производя 6 удвоений и 2 сложения точек на кривой.

Предложение 1. Пусть эллиптическая кривая E определена уравнением Вейерштрасса (уравнением (1), (2) или (3) из предыдущего параграфа) над конечным полем F_q. Если задана точка P на E, то координаты kP можно вычислить за O($\log k \ \log^3 q$) двоичных операций.

Замечания.

1. Оценки времени работы в предложении 2.1 не являются наилучшими, особенно для конечных полей характеристики $p = 2$. Нам, однако, достаточно этих оценок, которые следуют из наиболее очевидных алгоритмов арифметики в конечных полях.

2. Если известно число N точек на эллиптической кривой E и если $k > N$, то в силу равенства $NP = O$ мы можем заменить k его наименьшим неотрицательным вычетом по модулю N ($k \bmod N$); в этом случае временная оценка заменяется на $O(\log^4 q)$ (напомним, что $N \le q + 1 + 2\sqrt{q} = O(q)$). Рене Шуф (R. Schoof) предложил алгоритм, вычисляющий N за $O(log^8 q)$ двоичных операций.

Представление открытого текста.

Мы намереваемся кодировать наши открытые тексты точками некоторой заданной эллиптической кривой E, определенной над конечным полем F_q 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 P_m. Заметим, что это «кодирование» – не то же самое, что засекречивание. Позднее мы будем рассматривать способы шифрования точек P_m 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 F_q.В приведенном примере 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 приформировании цифровой подписи. Однако, как мы увидим далее, существуют вероятностные алгоритмы с малой вероятностью неудачи. Во-вторых, порождать случайные точки на E 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 E, определенной над F_q, где $q = p^r$ предполагается большим (и нечетным – см. упражнение 8 при $q = p^r$). Пусть κ – 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 2^κ; практически достаточно $\kappa = 30$ или, на худой конец, $\kappa = 50$. Пусть элементы нашего сообщения m – целые числа, $0 \le m \le M$. Предположим также, что выбранное нами конечное поле имеет q элементов, $q > M\kappa$. Записываем целые числа от 1 до $M\kappa$ в виде $m\kappa + j$, где $1 \le j \le \kappa$ и устанавливаем взаимно однозначное соответствие между такими числами и некоторым множеством элементов из F_q. Например, можно записать такое число как r-значное числе в p-ичной системе счисления и, отождествляя цифры в этой записи с элементами $F_p \cong Z / pZ$, рассматривать их как коэффициенты многочлена степени не выше r - 1 над F_p, соответствующего элементу поля F_q. Таким образом, числу $(a_{r-1}a_{r-2}...a_1a_0)$ (здесь $0 \le a_i < P$) ставится в соответствие многочлен $\sum_{i=0}^{r-1} a_i X^i$ который, будучи рассмотрен по модулю некоторого фиксированного неприводимого многочлена степени r над F_p, дает элемент F_q.

Итак, при данном m для каждого $j = 1,2,\ldots,\kappa$ мы получаем элемент x из F_q, соответствующий $m\kappa + j$. Для такого x вычисляем правую часть уравнения

$$y^2 = f(x) = x^3 + ax + b$$

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

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

Дискретный логарифм на *E*.

Определение. Пусть E – эллиптическая кривая над F_q, и B – точка на E. Задачей дискретного логарифмирования на E (с основанием B) называется задача нахождения для данной точки $P \in E$ такого целого числа $x \in Z$ (если оно существует), что $xB = P$.

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 F_{2^r} позволяют сравнительно легко вычислять дискретные логарифмы и, следовательно, вскрывать соответствующие криптосистемы, если r не выбрано очень большим. Аналогичные системы, использующие эллиптические кривые над F_q (см. ниже), судя по всему, **являются столь же надежными при значительно меньших значениях *r***. Так как имеются практические причины (связанные с устройством ЭВМ и программированием) предпочтительности арифметических операций над полями F_{2^r}, криптосистемы с открытым ключом, рассматриваемые ниже, могут оказаться более удобными для практического применения, чем системы, основанные на задаче дискретного логарифмирования в F_q^*

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 впоследствии Менезес (Menezes), Окамото (Okanoto) и Вэнстон (Vanstone) предложили новый подход к задаче дискретного логарифмирования на эллиптической кривой E, определенной над F_q. А именно, они использовали спаривание Вейля для вложения группы E в мультипликативную группу некоторого расширения F_{q^k} поля F_q. Это вложение сводит задачу дискретного логарифмирования на E к соответствующей задаче для $F_{q^k}^*$.

Однако такое сведение полезно, лишь если степень k расширения мала. Фактически единственный вид эллиптических кривых, для которых k мало, – это так называемые «суперсингулярные» эллиптические кривые, наиболее известными примерами которых являются кривые вида $y^2 = x^3 + az$ над полем F_q, характеристики $p \equiv -1 (\mathrm{mod}\, 4)$ и кривые вида $y^2 = x^3 + b$ над полем F_q, когда $p \equiv -1 (\mathrm{mod}\, 3)$. Как правило, эллиптические кривые не являются суперсингулярными. Для них такое сведение почти никогда не приводит к субэкспоненциальным алгоритмам.

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.

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

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 F_q и какую-либо эллиптическую кривую E над ним. Их ключ строится по случайной точке P на этой эллиптической кривой. Если у них есть случайная точка P, то, например, ее x-координата дает случайный элемент F_q, который можно затем преобразовать в r-разрядное целое число в p-ичной системе счисления (где $q = p^r$), и это число может служить ключом в их классической криптосистеме (здесь мы пользуемся словом «случайный» в неточном смысле; мы лишь хотим сказать, что выбор из некоторого большого множества допустимых ключей произволен и непредсказуем). Они должны выбрать точку P так, чтобы все их сообщения друг другу были открытыми и все же никто, кроме них двоих, ничего бы не знал о P.

Абоненты (пользователи) А и Б первым делом открыто выбирают точку $B \in E$ 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, мы не хотим тратить время на проверку того, что B – образующий элемент (или даже на нахождение общего числа N точек, которое нам не понадобится в последующем). Нам хотелось бы, чтобы порожденная B подгруппа была большой, предпочтительно того же порядка величины, что и сама E. Позже мы обсудим этот вопрос. Пока что предположим, что B – взятая открыто точка на E 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 $aB \in E$ и передает эту точку открыто. Абонент Б делает то же самое: он выбирает случайно b и открыто передает $bB \in E$. Тогда используемый ими секретный ключ – это $P = abB \in E$. 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 B и bB) по-видимому, нет способа найти abB, зная лишь aB и bB.

Пример 2. Возьмем $p = 211$, $E_p(0,-4)$ (что соответствует кривой $y^2 = x^3 - 4$) и $B = (2, 2)$. Можно подсчитать, что $241B = O$. Личным ключом пользователя А является $a = 121$, поэтому открытым ключом А будет $aB = 121(2, 2) = (115, 48)$. Личным ключом поль-

зователя Б является b = 203, поэтому его открытым ключом будет 203(2, 2) = (130, 203). Общим секретным ключом является 121(130, 203) = 203(115, 48) = (161,169).

Обратите еще раз внимание на то, что 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 P_m фиксированной (и не скрываемой) эллиптической кривой E над F_q (q берется большим). Предполагается также, что общее число N точек на E вычислено и не составляет секрета. Каждый пользователь системы секретно выбирает такое целое случайное число e между 1 и N, что НОД(e, N) = 1. Используя алгоритм Евклида, он находит затем обратное e^{-1} к числу e по модулю N, т.е. такое целое число d, что $de \equiv 1(\mathrm{mod\ N})$. Если А хочет послать Б сообщение P_m, то он сначала посылает ему точку $e_A P_m$ (индекс А указывает на пользователя А). Это ничего не говорит Б, который, не зная ни e_A, ни, d_A, не может восстановить P_m. Однако, не придавая этому значения, он умножает ее на свое e_B и посылает обратно А. На третьем шаге А должен частично раскрыть свое сообщение, умножив $e_B e_A P_m$ на d_A. Так как $NP_m = O$ и $d_A e_A = 1(\mathrm{mod}\ N)$, при этом получается точка $e_B P_m$, которую А возвращает Б. Тот может теперь прочитать сообщение, умножив точку $e_B P_m$ на d_B.

Заметим, что злоумышленник может узнать $e_A P_m$, $e_B e_A P_m$ и $e_B P_m$ Если бы он умел решать задачу дискретного логарифмирования на E, то он мог бы определить e_B по первым двум точкам, вычислить $d_B = e_B (\mathrm{mod}\ N)$ и $P_m = d_B e_B P_m$.

Аналог системы Эль-Гамаля.

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

а) конечного поля F_q;

б) определенной над ним эллиптической кривой E;

в) точки-«основания» B на ней (знать общее число N точек на E нам 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 P_m, А выбирает случайно целое число k и посылает пару точек $\{kB,\ P_m + k a_B B\}$ (где $a_B B$ — открытый ключ Б). Чтобы прочитать сообщение, Б умножает первую точку из полученной пары на свое секретное число a_B и вычитает результат умножения из второй точки:

$$P_m + k(a_B B) - a_B(kB) = P_m.$$

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

Пример 3. Рассмотрим случай p = 751, E_p(-1,188) (что соответствует кривой $y^2 = x^3 - x + 188$ и G = (0, 376)). Предположим, что пользователь А собирается отправить

пользователю Б сообщение, которое кодируется эллиптической точкой P_m = (562,201), и что пользователь А выбирает случайное число k = 386. Открытым ключом Б является P_B = (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 B на ней.

1) Случайный выбор (E, B). Взяв какое-либо большое конечное поле F_q, можно следующим образом осуществить одновременный выбор E и $B = (x, y) \in E$. Будем предполагать, что характеристика p поля F_q больше 3, так что эллиптическая кривая задана уравнением (1) из § 1; при $q = 2^r$ или 3^r нетрудно сделать очевидные изменения в дальнейшем изложении. Выбираем сначала случайным образом три элемента из F_q^* в качестве x, y, a. Далее полагаем $b = y^2 - (x^3 + ax)$. Убеждаемся в том, что кубический многочлен $x^3 + ax + b$ не имеет кратных корней, что равносильно проверке условия $4a^3 + 27b^2 \neq 0$. Если это условие не выполняется, берем другую случайную тройку x, y, a. Полагаем $B = (x, y)$. Тогда B – точка на эллиптической кривой $y^2 = x^3 + ax + b$.

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

В статье Шуфа оценка времени работы была фактически $O(\log^8 q)$, 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 (A.O.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 F_q, если q – степень простого числа, записываемая 50 или даже 100 знаками. 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 F_q^*). 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 (E, B) по модулю p. 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 E – эллиптическая кривая, определенная над полем рациональных чисел (или, для большей общности, можно было бы использовать эллиптическую кривую, определенную над некоторым числовым полем), и B – точка бесконечного порядка на E.

Пример 4. Точка $B = (0, 0)$ является точкой бесконечного порядка на эллиптической кривой E: $y^2 + y = x^3 - x$ и фактически порождает всю группу рациональных точек на E.

Пример 5. Точка $B = (0, 0)$ является точкой бесконечного порядка на E: $y^2 + y = x^3 - x^2$ и порождает всю группу рациональных точек.

Далее, мы выбираем большое простое число p (или, если наша эллиптическая кривая определена над расширением K поля Q, выбираем некоторый простой идеал в K) и рассматриваем редукцию E и B по модулю p. Точнее, для всех p, за исключением нескольких малых простых чисел, коэффициенты в уравнении для E имеют взаимно простые с p знаменатели и, следовательно, могут рассматриваться как коэффициенты в уравнении по модулю p. Если сделать замену переменных, приведя полученное уравнение над F_p к виду $y^2 = x^3 + ax + b$ то кубический многочлен в главной части не будет иметь кратных корней (за исключением нескольких малых простых p) и дает поэтому эллиптическую кривую над F_p (которую мы будем обозначать $E(\mathrm{mod}\ p)$). Координаты точки B, будучи также приведенными по модулю p, дают точку на эллиптической кривой $E(\mathrm{mod}\ p)$, которую мы будем обозначать $B(\mathrm{mod}\ p)$.

При использовании этого второго способа мы раз и навсегда фиксируем E и B и за счет этого получаем много различных возможностей посредством изменения простого p.

Порядок точки *B*.

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

Как упоминалось выше, описанные криптосистемы могут быть надежными даже если точка B не является порождающим элементом Фактически нужно, чтобы в циклической группе, порождаемой B, 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 $B \neq O$ будет порождающим элементом. Если использовать первый из описанных выше методов, то при фиксированном F_p можно продолжать выбор пар (E, B), пока не найдется такая, для которой число точек на E есть простое число (что можно определить одним из известных тестов на простоту). Если применять второй метод, то для фиксированной глобальной эллиптической кривой E над Q можно продолжать выбирать простые p, пока не найдем кривую $E(\mathrm{mod}\ p)$, число точек на которой простое. Как долго нам придется ждать? Этот вопрос аналогичен следующему вопросу о группах F_p^*: является ли $(p - 1)/2$ 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 p с требующимся свойством есть $O(1/\log p)$

Замечание. Для того чтобы $E(\mathrm{mod}\ p)$ имела простой порядок N при большом p, надо выбирать E 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 *P*. Наиболее быстрым из известных на сегодня методов логарифмирования на эллиптический кривой является так называемый ρ-метод Полларда (Pollard). В таблице 2 сравнивается эффективность этого метода и метода разложения на простые множители с помощью решета в поле чисел общего вида. Как видите, 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 2 Вычислительные усилия, необходимые для криптоанализа при использовании эллиптических кривых и RSA

Размер ключа	MIPS-годы
150	$3{,}8\times10^{10}$
205	$7{,}1\times10^{18}$
234	$1{,}6\times10^{28}$

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

Размер ключа	MIPS-годы
512	3×10^{4}
768	3×10^{2}
1024	3×10^{11}
1280	1×10^{14}
1536	3×10^{16}
2048	3×10^{20}

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 $E(F_p)$, то должны выполняться следующие условия:

$$\begin{cases} p+1-2\sqrt{p} \le N \le p+1+2\sqrt{p}, & (1) \\ G \in E(F_p) \Rightarrow N \cdot G = O. & (2) \end{cases}$$

Таким образом, чтобы отсеять лишние числа из интервала $\left(p+1-2\sqrt{p}, p+1+2\sqrt{p}\right)$, 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, $n > \max\left\{2^{160}, 4\sqrt{p}\right\}$.

2) $N \neq p$ и $N \neq p+1$, где N – порядок кривой.

3) $p^k \neq 1 (\mathrm{mod}\, n)$ для всех $k = 1, \ldots, C$, где C настолько велико, что вычислить дискретный логарифм в F_{p^C} 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 $G' \in E(F_p)$ и вычислим $G = \frac{N}{n} \cdot G'$. Если $G \neq O$, то требуемая точка найдена, если же $G = O$, то выбираем другую точку G'.

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, $0 < d < n$. Ключ проверки подписи (открытый ключ) – это точка эллиптической кривой $Q = d \cdot G$. Алгоритм ЭЦП также использует хеш-функцию, обозначаемую h.

Генерация подписи.

Входные данные: сообщение m, исходные параметры и ключ подписи. Выходные данные: подпись (r, s).

Алгоритм:

1. Выбрать случайное число k в интервале $[1, n-1]$.
2. Вычислить $(x, y) = k \cdot G$.
3. Вычислить $r = x \bmod n$.
4. Если $r = 0$, то вернуться к шагу 1.
5. Вычислить $z = k^{-1} \bmod n$.
6. Вычислить $e = h(m)$.
7. Вычислить $s = z(e + dr) \bmod n$.
8. Если $s = 0$, то вернуться к шагу 1.
9. Вывести пару (r, s) – подпись к m.

Замечания.

1. При $r = 0$ результат вычисления s не зависит от секретного ключа d.

2. При $s = 0$ необходимого для проверки подписи числа $s^{-1} \bmod n$ 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 $1 \le r \le n-1$, $1 \le s \le n-1$ нарушается, то подпись фальшивая и работа алгоритма закончена.
2. Вычислить $e = h(m)$.
3. Вычислить $v = s^{-1} \bmod n$.
4. Вычислить $u_1 = ev \bmod n$.

5. Вычислить $u_2 = rv \bmod n$.

6. Вычислить $X = u_1 \cdot G + u_2 \cdot Q = (x, y)$.

7. Если $r = x \bmod n$, то подпись действительная, иначе подпись фальшивая.

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

Задачи к лабораторным работам
по криптографии на эллиптических кривых

1) Пример кодирования и декодирования текста.

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

Для заданий лабораторной работы выбрана кривая $E_{751}(-1,1)$, т.е. $y^2 = x^3 - x + 1 (\text{mod } 751)$. Предлагается следующий (один из возможных) алфавит, приведенный в таблице 3.

Таблица 3. Алфавит точек эллиптической кривой для выполнения лабораторных работ

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

140	м	(238, 175)	145	с	(243, 664)	150	ц	(250, 14)	155	ы	(253, 540)
141	н	(238, 576)	146	т	(247, 266)	151	ч	(250, 737)	156	ь	(256, 121)
142	о	(240, 309)	147	у	(247, 485)	152	ш	(251, 245)	157	э	(256, 630)
143	п	(240, 442)	148	ф	(249, 183)	153	щ	(251, 506)	158	ю	(257, 293)
144	р	(243, 87)	149	х	(249, 568)	154	ъ	(253, 211)	159	я	(257, 458)

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 В сообщение: строчную латинскую букву «А». В нашем алфавите эта буква кодируется точкой $P_m = (66, 522)$. Пусть пользователь А выбрал случайное значение $k = 3$, а открытым ключом В является точка $P_B = (406, 397)$, при этом секретным ключом В является число $n_b = 45$.

Шифрованный текст имеет вид $C_m = \{kG,\ P_m + kP_B\}$.

Находим $kG = 3 \cdot (0, 1)$.

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

$$x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\, p)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p)$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, \text{если } P \neq Q; \\ \dfrac{3x_1^2 + a}{2y_1}, \text{если } P = Q. \end{cases}$$

Вычисляем 2G:

$$\lambda = \frac{3(0^2) - 1}{2 \times 1} = \frac{-1}{2} \equiv 375 \bmod 751 \left(\frac{-1 + 751}{2} = 375 \right)$$

$$x_3 = 375^2 - 0 - 0 = 140625 \equiv 188 \bmod 751$$

$$y_3 = 375(0 - 188) - 1 = -70501 \equiv 93 \bmod 23$$

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

$$\lambda = \frac{188 - 0}{93 - 1} = \frac{188}{92} \equiv 368 \bmod 751$$

$$x_3 = 368^2 - 0 - 188 = 135236 \equiv 56 \bmod 751$$

$$y_3 = 368(0 - 56) - 1 = 20607 \equiv 419 \bmod 751$$

Таким образом, мы нашли точку $kG = 3 \cdot (0, 1) = (56, 419)$.

Вычисляем $P_m + kP_B = (66, 552) + 3 \cdot (406, 397) = (301, 734)$.

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

Пользователь В для расшифрования сообщения должен провести следующие вычисления: $P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(kG) = (301, 734) - 45 \cdot (56, 419) = (301, 734) + (175, 559) = (66, 552)$.

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

3) Пример генерации и проверки подписи.

Пусть используется эллиптическая кривая $E_{751}(-1,1)$ 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 $kG = (x, y) = 3 \cdot (384, 475)$ = (596, 318) и затем $r = x \bmod n = 596 \bmod 13 = 11$. Используя расширенный алгоритм Евклида, определяем $z = k^{-1} \bmod n = 3^{-1} \bmod 13 = 9$ (так как $3 \cdot 9 = 27 \equiv 1 (\bmod 13)$). Наконец, $s = z(e + dr) \bmod n = 9 \cdot (12 + 12 \cdot 11) \bmod 13 = 9$. Таким образом, $(r, s) = (11,9)$ – цифровая подпись данного абонента для сообщения.

Пусть теперь необходимо проверить подлинность данной подписи. Открытый ключ абонента, подписавшего сообщение, равен $Q = dG = 12 \cdot (384,475) = (384,276)$. Проверка подписи начинается с проверки условий $1 \le r \le n-1$, $1 \le s \le n-1$ – в данном случае они соблюдаются. Затем последовательно вычисляем $v = s^{-1} \bmod n = 9^{-1} \bmod 13 = 3$, $u_1 = ev \bmod n = 12 \cdot 3 \bmod 13 = 10$ и $u_2 = 11 \cdot 3 \bmod 13 = 7$. Находим точку $X = u_1 \cdot G + u_2 \cdot Q =$ $= 10 \cdot (384,475) + 7 \cdot (384,276) = (596,318)$. Наконец, сравниваем значения r = 11 и $x \bmod n =$ $= 596 \bmod 13 = 11$ – они совпадают, следовательно, подпись действительная.

Варианты заданий

Задача 1. Зашифровать открытый текст, используя алфавит, приведенный в примере (используется кривая $E_{751}(-1,1)$ 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

Задача 2. Дан шифртекст. Используя алфавит, приведенный в примере (используется кривая $E_{751}(-1,1)$ и генерирующая точка $G = (-1, 1)$), и зная секретный ключ n_b, найти открытый текст.

№ варианта	Секретный ключ n_b	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)}

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 $E_{751}(-1,1)$. Найти точку $2P + 3Q - R$.

№ 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 $E_{751}(-1,1)$ 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 $E_{751}(-1,1)$ 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 (r, s) для сообщения с известным значением хэш-свертки *e*, зная открытый ключ проверки подписи *Q*. Используется кривая $E_{751}(-1,1)$ 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)

Ответы к задачам

Задача 1. Шифрование.

Вариант 1. {(618, 206), (253, 211)}; {(745, 210), (318, 429)}; {(596, 433), (85, 716)}; {(618, 206), (90, 730)}; {(425, 663), (43, 527)}; {(377, 456), (652, 315)}; {(568, 355), (675, 505)}; {(596, 433), (376, 686)}; {(568, 355), (85, 35)}.

Вариант 2. {(745, 210), (434, 136)}; {(440, 539), (229, 600)}; {(286, 136), (520, 2)}; {(188, 93), (642, 698)}; {(188, 93), (45, 720)}; {(16, 416), (719, 538)}; {(346, 242), (45, 31)}; {(725, 195), (438, 711)}; {(440, 539), (395, 414)};

Вариант 3. {(725, 195), (86, 726)}; {(286, 136), (681, 366)}; {(72, 254), (86, 25)}; {(16, 416), (138, 453)}; {(489, 468), (157, 175)}; {(16, 416), (31, 136)}; {(568, 355), (109, 551)}; {(489, 468), (143, 602)}; {(618, 206), (652, 315)};

Вариант 4. {(179, 275), (383, 411)}; {(440, 539), (229, 151)}; {(618, 206), (466, 214)}; {(568, 355), (156, 704)}; {(72, 254), (564, 38)}; {(725, 195), (145, 143)}; {(286, 136), (176, 413)}; {(346, 242), (12, 314)}; {(188, 93), (275, 456)};

Вариант 5. {(725, 195), (620, 680)}; {(596, 433), (39, 171)}; {(425, 663), (654, 102)}; {(135, 82), (85, 716)}; {(286, 136), (99, 295)}; {(179, 275), (526, 412)}; {(16, 416), (458, 490)}; {(489, 468), (140, 115)}; {(568, 355), (400, 56)};

Вариант 6. {(346, 242), (594, 414)}; {(596, 433), (34, 677)}; {(440, 539), (546, 670)}; {(440, 539), (694, 581)}; {(188, 93), (515, 684)}; {(377, 456), (517, 573)}; {(346, 242), (288, 639)}; {(188, 93), (209, 82)}; {(188, 93), (205, 379)};

Вариант 7. {(440, 539), (663, 275)}; {(425, 663), (638, 131)}; {(16, 416), (228, 480)}; {(440, 539), (329, 447)}; {(283, 493), (463, 736)}; {(188, 93), (688, 741)}; {(440, 539), (407, 669)}; {(596, 433), (6, 218)}; {(568, 355), (561, 140)};

Вариант 8. {(188, 93), (458, 261)}; {(188, 93), (184, 217)}; {(16, 416), (374, 436)}; {(618, 206), (267, 81)}; {(745, 210), (506, 92)}; {(568, 355), (256, 121)}; {(179, 275), (110, 622)}; {(188, 93), (576, 286)}; {(745, 210), (376, 686)};

Вариант 9. {(188, 93), (6, 218)}; {(568, 355), (234, 164)}; {(16, 416), (390, 603)}; {(346, 242), (307, 693)}; {(188, 93), (45, 31)}; {(188, 93), (45, 31)}; {(72, 254), (229, 600)}; {(377, 456), (685, 655)}; {(188, 93), (45, 31)};

Вариант 10. {(286, 136), (269, 187)}; {(179, 275), (490, 434)}; {(618, 206), (371, 14)}; {(135, 82), (438, 40)}; {(72, 254), (438, 711)}; {(618, 206), (407, 82)};

{(440, 539), (532, 50)}; {(188, 93), (228, 480)}; {(56, 419), (538, 325)};

Вариант 11. {(489, 468), (210, 720)}; {(425, 663), (151, 518)}; {(440, 539), (594, 337)};
{(188, 93), (422, 162)}; {(188, 93), (290, 509)}; {(188, 93), (79, 640)};
{(56, 419), (496, 31)}; {(440, 539), (26, 366)}; {(745, 210), (240, 442)};

Вариант 12. {(377, 456), (558, 359)}; {(745, 210), (688, 741)}; {(72, 254), (679, 73)};
{(188, 93), (36, 664)}; {(56, 419), (588, 44)}; {(16, 416), (558, 392)};
{(188, 93), (606, 147)}; {(179, 275), (269, 564)}; {(72, 254), (395, 414)};

Вариант 13. {(56, 419), (454, 628)}; {(72, 254), (67, 84)}; {(440, 539), (397, 567)};
{(425, 663), (53, 474)}; {(72, 254), (414, 563)}; {(618, 206), (253, 211)};
{(56, 419), (688, 10)}; {(135, 82), (160, 142)}; {(745, 210), (48, 49)};

Вариант 14. {(135, 82), (69, 510)}; {(489, 468), (481, 369)}; {(56, 419), (426, 89)};
{(346, 242), (594, 414)}; {(618, 206), (100, 387)}; {(618, 206), (350, 184)};
{(346, 242), (86, 726)}; {(179, 275), (660, 476)}; {(72, 254), (642, 53)};

Вариант 15. {(425, 663), (99, 295)}; {(56, 419), (606, 147)}; {(56, 419), (151, 233)};
{(188, 93), (279, 398)}; {(16, 416), (218, 601)}; {(568, 355), (328, 461)};
{(188, 93), (390, 603)}; {(16, 416), (585, 540)}; {(377, 456), (237, 297)};

Вариант 16. {(188, 93), (62, 372)}; {(346, 242), (329, 447)}; {(16, 416), (376, 686)};
{(188, 93), (358, 491)}; {(725, 195), (143, 602)}; {(377, 456), (243, 87)};
{(56, 419), (185, 105)}; {(56, 419), (396, 481)}; {(618, 206), (558, 359)};

Вариант 17. {(568, 355), (461, 747)}; {(188, 93), (675, 246)}; {(283, 493), (328, 290)};
{(425, 663), (543, 357)}; {(568, 355), (206, 106)}; {(425, 663), (496, 31)};
{(135, 82), (394, 731)}; {(346, 242), (594, 414)}; {(425, 663), (454, 628)};

Вариант 18. {(568, 355), (321, 467)}; {(286, 136), (99, 295)}; {(283, 493), (358, 491)};
{(188, 93), (314, 127)}; {(286, 136), (685, 655)}; {(596, 433), (515, 67)};
{(568, 355), (205, 379)}; {(618, 206), (405, 747)}; {(286, 136), (525, 674)};

Вариант 19. {(188, 93), (221, 613)}; {(188, 93), (446, 227)}; {(135, 82), (426, 89)};
{(179, 275), (102, 267)}; {(568, 355), (599, 696)}; {(16, 416), (151, 233)};
{(188, 93), (27, 120)}; {(745, 210), (27, 631)}; {(725, 195), (235, 732)};

Вариант 20. {(489, 468), (599, 696)}; {(489, 468), (61, 622)}; {(188, 93), (13, 134)};
{(56, 419), (447, 0)}; {(346, 242), (197, 145)}; {(568, 355), (554, 330)};
{(725, 195), (705, 687)}; {(618, 206), (295, 219)}; {(489, 468), (407, 82)};

Вариант 21. {(286, 136), (612, 329)}; {(425, 663), (526, 412)}; {(135, 82), (27, 120)}; {(745, 210), (707, 195)}; {(618, 206), (281, 518)}; {(188, 93), (390, 603)}; {(286, 136), (612, 329)}; {(377, 456), (160, 609)}; {(179, 275), (530, 22)};

Вариант 22. {(596, 433), (66, 552)}; {(618, 206), (90, 730)}; {(179, 275), (590, 376)}; {(179, 275), (687, 91)}; {(725, 195), (535, 374)}; {(725, 195), (203, 324)}; {(440, 539), (344, 400)}; {(188, 93), (461, 747)}; {(425, 663), (269, 564)};

Вариант 23. {(725, 195), (4, 567)}; {(440, 539), (727, 65)}; {(618, 206), (13, 134)}; {(179, 275), (79, 640)}; {(618, 206), (147, 361)}; {(188, 93), (288, 639)}; {(16, 416), (362, 446)}; {(188, 93), (267, 81)}; {(286, 136), (395, 414)};

Вариант 24. {(425, 663), (636, 4)}; {(568, 355), (660, 275)}; {(346, 242), (229, 151)}; {(188, 93), (606, 147)}; {(425, 663), (652, 315)}; {(346, 242), (414, 563)}; {(745, 210), (340, 78)}; {(568, 355), (422, 589)}; {(725, 195), (422, 589)};

Вариант 25. {(489, 468), (517, 573)}; {(377, 456), (151, 233)}; {(283, 493), (629, 403)}; {(188, 93), (682, 179)}; {(188, 93), (165, 382)}; {(286, 136), (75, 433)}; {(286, 136), (417, 614)}; {(425, 663), (275, 456)}; {(135, 82), (729, 578)};

Вариант 26. {(440, 539), (705, 64)}; {(440, 539), (350, 567)}; {(489, 468), (273, 270)}; {(286, 136), (243, 664)}; {(440, 539), (229, 151)}; {(135, 82), (99, 456)}; {(745, 210), (668, 409)}; {(135, 82), (394, 731)}; {(72, 254), (611, 579)};

Вариант 27. {(377, 456), (47, 349)}; {(596, 433), (45, 31)}; {(188, 93), (422, 162)}; {(188, 93), (290, 509)}; {(377, 456), (240, 309)}; {(377, 456), (47, 349)}; {(596, 433), (533, 299)}; {(56, 419), (414, 563)}; {(135, 82), (394, 20)};

Вариант 28. {(179, 275), (237, 297)}; {(440, 539), (86, 726)}; {(377, 456), (681, 366)}; {(377, 456), (114, 607)}; {(425, 663), (147, 361)}; {(188, 93), (319, 233)}; {(377, 456), (445, 271)}; {(568, 355), (67, 667)}; {(16, 416), (243, 664)};

Вариант 29. {(72, 254), (218, 601)}; {(188, 93), (86, 726)}; {(440, 539), (334, 226)}; {(568, 355), (251, 245)}; {(346, 242), (228, 480)}; {(16, 416), (6, 533)}; {(56, 419), (320, 7)}; {(188, 93), (138, 453)}; {(346, 242), (192, 719)};

Вариант 30. {(188, 93), (557, 28)}; {(489, 468), (589, 429)}; {(618, 206), (229, 151)}; {(188, 93), (13, 617)}; {(568, 355), (324, 128)}; {(16, 416), (307, 693)}; {(425, 663), (269, 187)}; {(179, 275), (177, 189)}; {(568, 355), (266, 91)};

Задача 2. Расшифрование.

Вариант 1. «бархатный».
Вариант 2. «бадминтон».
Вариант 3. «вздремнуть».
Вариант 4. «взломщик».
Вариант 5. «допустимый».
Вариант 6. «заостренный».
Вариант 7. «изготовление».
Вариант 8. «итальянский».
Вариант 9. «ихтиология».
Вариант 10. «коммуникатор».
Вариант 11. «летательный».
Вариант 12. «метаболизм».
Вариант 13. «наваждение».
Вариант 14. «облицовывать».
Вариант 15. «парфюмерия».
Вариант 16. «равнозначно»
Вариант 17. «симплексный»
Вариант 18. «терпеливость»
Вариант 19. «уверенность».
Вариант 20. «укрупненный».
Вариант 21. «феерический».
Вариант 22. «целлюлозный».
Вариант 23. «хрестоматия».
Вариант 24. «черномазый».
Вариант 25. «шишковатый».
Вариант 26. «экскаватор».
Вариант 27. «последствие».
Вариант 28. «ястребиный»
Вариант 29. «фейерверк».
Вариант 30. «урожденный».

Задача 3. Сложение точек.

Вариант 1. (446, 227).
Вариант 2. (612, 329).
Вариант 3. (517, 178).
Вариант 4. (257, 458).
Вариант 5. (177, 189).
Вариант 6. (320, 744).
Вариант 7. (318, 429).
Вариант 8. (198, 527).
Вариант 9. (562, 89).
Вариант 10. (719, 213).
Вариант 11. (552, 237).
Вариант 12. (688, 741).
Вариант 13. (371, 737).
Вариант 14. (203, 427).
Вариант 15. (642, 698).
Вариант 16. (326, 675).
Вариант 17. (487, 55).
Вариант 18. (536, 657).
Вариант 19. (356, 175).
Вариант 20. (108, 247).
Вариант 21. (109, 200).
Вариант 22. (679, 73).
Вариант 23. (110, 622).
Вариант 24. (9, 601).
Вариант 25. (685, 96).
Вариант 26. (307, 693).
Вариант 27. (612, 329).
Вариант 28. (325, 454).
Вариант 29. (120, 604).
Вариант 30. (446, 227).

Задача 4. Умножение точек.

Вариант 1. (188, 658).
Вариант 2. (188, 93).
Вариант 3. (168, 516).
Вариант 4. (334, 226).
Вариант 5. (36, 664).
Вариант 6. (417, 614).
Вариант 7. (509, 341).
Вариант 8. (156, 704).
Вариант 9. (45, 31).
Вариант 10. (463, 15).
Вариант 11. (120, 604).
Вариант 12. (703, 626).
Вариант 13. (126, 718).
Вариант 14. (589, 322).
Вариант 15. (21, 637).
Вариант 16. (321, 467).
Вариант 17. (33, 396).
Вариант 18. (642, 53).
Вариант 19. (508, 353).
Вариант 20. (73, 679).
Вариант 21. (151, 233).
Вариант 22. (66, 552).
Вариант 23. (508, 398).
Вариант 24. (45, 31).
Вариант 25. (704, 46).
Вариант 26. (657, 285).
Вариант 27. (307, 58).
Вариант 28. (102, 484).
Вариант 29. (397, 567).
Вариант 30. (618, 545).

Задача 5. Генерация подписи.

Вариант 1. (3, 1).
Вариант 2. (11, 4).
Вариант 3. (7, 5).
Вариант 4. (11, 3).
Вариант 5. (11, 12).
Вариант 6. (11, 3).
Вариант 7. (3, 2).
Вариант 8. (3, 8).
Вариант 9. (11, 11).
Вариант 10. (7, 1).
Вариант 11. (7, 4).
Вариант 12. (3, 7).
Вариант 13. (5, 4).
Вариант 14. (11, 8).
Вариант 15. (7, 3).
Вариант 16. (7, 7).
Вариант 17. (3, 7).
Вариант 18. (7, 10).
Вариант 19. (11, 2).
Вариант 20. (11, 11).
Вариант 21. (7, 9).
Вариант 22. (7, 12).
Вариант 23. (11, 6).
Вариант 24. (3, 12).
Вариант 25. (3, 6).
Вариант 26. (11, 8).
Вариант 27. (7, 5).
Вариант 28. (11, 2).
Вариант 29. (7, 4).
Вариант 30. (3, 10).

Задача 6. Проверка подписи.

Вариант 1. Подпись фальшивая.
Вариант 2. Подпись фальшивая.
Вариант 3. Подпись фальшивая.
Вариант 4. Подпись подлинная.
Вариант 5. Подпись фальшивая.
Вариант 6. Подпись подлинная.
Вариант 7. Подпись подлинная.
Вариант 8. Подпись фальшивая.
Вариант 9. Подпись подлинная.
Вариант 10. Подпись фальшивая.
Вариант 11. Подпись фальшивая.
Вариант 12. Подпись фальшивая.
Вариант 13. Подпись фальшивая.
Вариант 14. Подпись подлинная.
Вариант 15. Подпись подлинная.
Вариант 16. Подпись подлинная.
Вариант 17. Подпись подлинная.
Вариант 18. Подпись фальшивая.
Вариант 19. Подпись подлинная.
Вариант 20. Подпись подлинная.
Вариант 21. Подпись фальшивая.
Вариант 22. Подпись фальшивая.
Вариант 23. Подпись подлинная.
Вариант 24. Подпись подлинная.
Вариант 25. Подпись фальшивая.
Вариант 26. Подпись подлинная.
Вариант 27. Подпись подлинная.
Вариант 28. Подпись фальшивая.
Вариант 29. Подпись подлинная.
Вариант 30. Подпись фальшивая.

ПРИЛОЖЕНИЕ 1

ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

Официальный текст

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.

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

3. Настоящий стандарт разработан с учетом терминологии и концепций международных стандартов ИСО 2382-2-76 «Обработка данных. Словарь. Часть 2. Арифметические и логические операции», ИСО/МЭК 9796-91 «Информационная технология. Методы защиты. Схема цифровой подписи с восстановлением сообщения», серии ИСО/МЭК 14888 «Информационная технология. Методы защиты. Цифровые подписи с приложением» и серии ИСО/МЭК 10118 «Информационная технология. Методы защиты. Хэш-функции».

4. ВЗАМЕН ГОСТ Р 34.10-94.

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.

Стандарт разработан взамен ГОСТ Р 34.10-94. Необходимость разработки настоящего стандарта вызвана потребностью в повышении стойкости ЭЦП к несанкционированным изменениям. Стойкость ЭЦП основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции по ГОСТ Р 34.11-94.

Настоящий стандарт терминологически и концептуально увязан с международными стандартами ИСО 2382-2, ИСО/МЭК 9796, серии ИСО/МЭК 14888 и серии ИСО/МЭК 10118.

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 использована ссылка на следующий стандарт:

ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функции хеширования.

3. Определения и обозначения

3.1. Определения.

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:

V_{256} – множество всех двоичных векторов длиной 256 бит;

V_{∞} – множество всех двоичных векторов произвольной конечной длины;

Z – множество всех целых чисел;

p – простое число, $p > 3$;

F_p – конечное простое поле, представляемое как множество из p целых чисел $\{0,1,\ldots, p-1\}$;

$b \pmod p$ – минимальное неотрицательное число, сравнимое с b по модулю p;

M – сообщение пользователя, $M \in V_{\infty}$;

$\left(\overline{h}_1 \| \overline{h}_2\right)$ – конкатенация (объединение) двух двоичных векторов;

a, b – коэффициенты эллиптической кривой;

m – порядок группы точек эллиптической кривой;

q – порядок подгруппы группы точек эллиптической кривой;

O – нулевая точка эллиптической кривой;

P – точка эллиптической кривой порядка q;

d – целое число – ключ подписи;

Q – точка эллиптической кривой – ключ проверки;

ζ – цифровая подпись под сообщением M.

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.

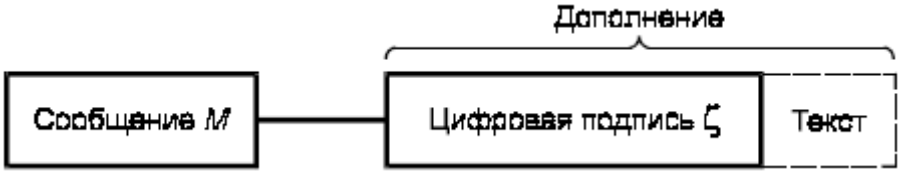

Рисунок 1 – Схема подписанного сообщения

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.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритм вычисления хэш-функции установлен в ГОСТ Р 34.11-94.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки, определены в 5.2.

Стандарт не определяет процесс генерации параметров схемы цифровой подписи. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы цифровой подписи исходя из требований к аппаратно-программным средствам, реализующим электронный документооборот.

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

Набор правил, позволяющих либо принять, либо отвергнуть цифровую подпись под полученным сообщением, установлен в 6.2.

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 $p > 3$. Тогда эллиптической кривой E, определенной над конечным простым полем F_p, называется множество пар чисел (x, y), $x, y \in F_p$, удовлетворяющих тождеству

$$y^2 \equiv x^3 + ax + b \pmod{p}, \quad (1)$$

где $a, b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p.

Инвариантом эллиптической кривой называется величина $J(E)$, удовлетворяющая тождеству

$$J(E) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} \pmod{p}. \quad (2)$$

Коэффициенты a, b эллиптической кривой E, по известному инварианту $J(E)$, определяются следующим образом:

$$\begin{cases} a \equiv 3k \pmod{p}, \\ b \equiv 3k \pmod{p}, \end{cases} \quad (3)$$

где $k = \dfrac{J(E)}{1728 - J(E)} \pmod{p}$, $J(E) \neq 0$ или 1728.

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

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

На множестве всех точек эллиптической кривой E введем операцию сложения, которую будем обозначать знаком «+». Для двух произвольных точек $Q_1(x_1, y_1)$ и $Q_2(x_2, y_2)$ эллиптической кривой E рассмотрим несколько вариантов.

Пусть координаты точек Q_1 и Q_2 удовлетворяют условию $x_1 \neq x_2$. В этом случае их суммой будем называть точку $Q_3(x_3, y_3)$, координаты которой определяются сравнениями

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\, p), \\ y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p), \end{cases} \quad (4)$$

где $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\, p)$.

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то определим координаты точки Q_3 следующим образом:

$$\begin{cases} x_3 = \lambda^2 - 2x_1 (\mathrm{mod}\, p), \\ y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p), \end{cases} \quad (5)$$

где $\lambda = \dfrac{3x_1^2 + a}{2y_1} (\mathrm{mod}\, p)$.

В случае, когда выполнено условие $x_1 = x_2$ и $y_1 \equiv -y_2 (\mathrm{mod}\, p)$, сумму точек Q_1 и Q_2 будем называть нулевой точкой O, не определяя ее x- и y-координаты. В этом случае точка Q_2 называется отрицанием точки Q_1. Для нулевой точки O выполнены равенства

$$Q + O = O + Q = Q, \quad (6)$$

где Q – произвольная точка эллиптической кривой E.

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

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}. \quad (7)$$

Точка Q называется точкой кратности k, или просто кратной точкой эллиптической кривой E, если для некоторой точки P выполнено равенство

$$Q = \underbrace{P + \ldots + P}_{k} = kP. \quad (8)$$

5.2. Параметры цифровой подписи.

Параметрами схемы цифровой подписи являются:

- простое число p – модуль эллиптической кривой, удовлетворяющее неравенству $p > 2^{255}$. Верхняя граница данного числа должна определяться при конкретной реализации схемы цифровой подписи;

- эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$;

- целое число m – порядок группы точек эллиптической кривой E;

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

$$\begin{cases} m = nq, n \in Z, n \geq 1 \\ 2^{254} < q < 2^{256} \end{cases}; \quad (9)$$

- точка $P \neq O$ эллиптической кривой E, с координатами (x_p, y_p), удовлетворяющая равенству $qP = O$;

-хэш-функция $h(\cdot): V_\infty \to V_{256}$, 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 (x_q, y_q), удовлетворяющей равенству $dP = Q$.

На приведенные выше параметры схемы цифровой подписи накладываются следующие требования:

- должно быть выполнено условие $p^t \neq 1 (\mathrm{mod}\, q)$, для всех целых $t = 1,2,\ldots,B$, где B удовлетворяет неравенству $B \geq 31$;
- должно быть выполнено неравенство $m \neq p$;
- инвариант кривой должен удовлетворять условию $J(E) \neq 0$ 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:

$$\overline{h} = (\alpha_{255}, \ldots, \alpha_0), \overline{h} \in V_{256}, \quad (10)$$

где $\alpha_i, i = 0,\ldots,255$ равно либо 1, либо 0. Будем считать, что число $\alpha \in Z$ соответствует двоичному вектору $\overline{h}$, если выполнено равенство

$$\alpha = \sum_{i=0}^{255} \alpha_i 2^i. \quad (11)$$

Для двух двоичных векторов $\overline{h}_1$ и $\overline{h}_2$, соответствующих целым числам α и β, определим операцию конкатенации (объединения) следующим образом. Пусть

$$\overline{h}_1 = (\alpha_{255}, \ldots, \alpha_0),$$
$$\overline{h}_2 = (\beta_{255}, \ldots, \beta_0), \quad (12)$$

тогда их объединение имеет вид

$$\overline{h}_1 \| \overline{h}_2 = (\alpha_{255}, \ldots, \alpha_0, \beta_{255}, \ldots, \beta_0) \quad (13)$$

и представляет собой двоичный вектор длиной 512 бит, составленный из коэффициентов векторов $\overline{h}_1$ и $\overline{h}_2$.

С другой стороны, приведенные формулы определяют способ разбиения двоичного вектора $\overline{h}$ длиной 512 бит на два двоичных вектора длиной 256 бит, конкатенацией которых он является.

6. Основные процессы

В данном разделе определены процессы формирования и проверки цифровой подписи под сообщением пользователя.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, удовлетворяющие требованиям 5.2.

Кроме того, каждый пользователь должен иметь ключ подписи d и ключ проверки подписи $Q(x_q, y_q)$, которые также должны удовлетворять требованиям 5.2.

6.1. Формирование цифровой подписи.

Для получения цифровой подписи под сообщением $M \in V_\infty$ необходимо выполнить следующие действия (шаги) по алгоритму I.

Шаг 1 – вычислить хэш-код сообщения M: $\bar{h} = h(M)$. (14)

Шаг 2 – вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить

$$e \equiv \alpha \pmod{p}. \quad (15)$$

Если $e = 0$, то определить $e = 1$.

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

$$0 < k < q. \quad (16)$$

Шаг 4 – вычислить точку эллиптической кривой $C = kP$ и определить

$$r \equiv x_C \pmod{q}, \quad (17)$$

где x_C – x-координата точки C. Если $r = 0$, то вернуться к шагу 3.

Шаг 5 – вычислить значение

$$s \equiv (rd + ke) \pmod{q}. \quad (18)$$

Если $s = 0$, то вернуться к шагу 3.

Шаг 6 – вычислить двоичные векторы $\bar{r}$ и $\bar{s}$, соответствующие r и s, и определить цифровую подпись $\zeta = (\bar{r} \| \bar{s})$ как конкатенацию двух двоичных векторов.

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

Схематическое представление процесса формирования цифровой подписи приведено на рисунке 2.

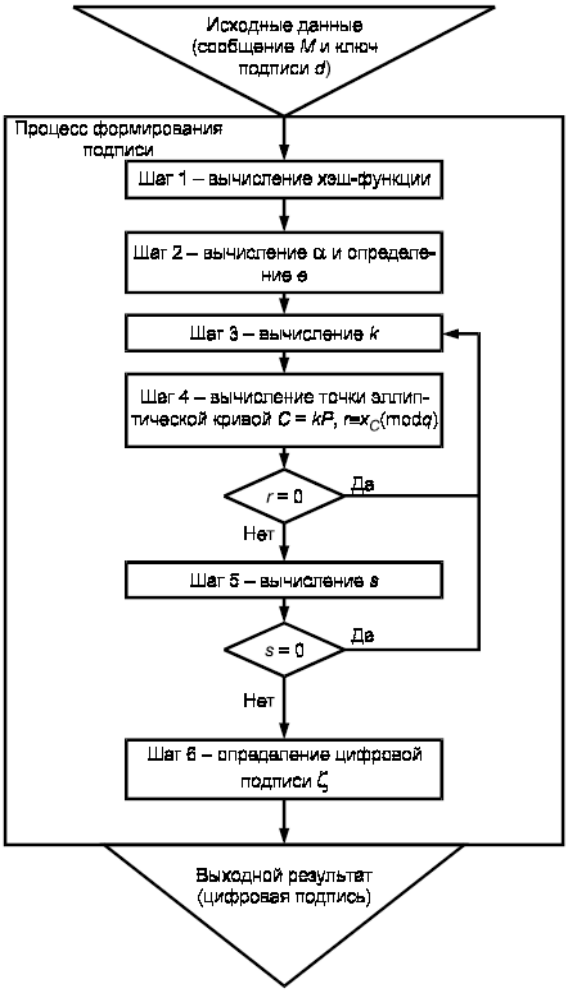

Рисунок 2 – Схема процесса формирования цифровой подписи

6.2. Проверка цифровой подписи.

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

Шаг 1 – по полученной подписи ζ вычислить целые числа r и s. Если выполнены неравенства $0 < r < q$, $0 < s < q$, то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2 – вычислить хэш-код полученного сообщения M:

$$\overline{h} = h(M). \quad (19)$$

Шаг 3 – вычислить целое число α, двоичным представлением которого является вектор $\overline{h}$, и определить

$$e \equiv \alpha \pmod{q}. \quad (20)$$

Если $e = 0$, то определить $e = 1$.

Шаг 4 – вычислить значение $v \equiv e^{-1} \pmod{q}$. (21)

Шаг 5 – вычислить значения

$$z_1 \equiv sv \pmod{q}, \; z_2 \equiv -rv \pmod{q}. \quad (22)$$

Шаг 6 – вычислить точку эллиптической кривой $C = z_1 P + z_2 Q$ и определить

$$R \equiv x_C \pmod{q}, \quad (23)$$

где x_C – x-координата точки C.

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

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

Схематическое представление процесса проверки цифровой подписи приведено на рисунке 3.

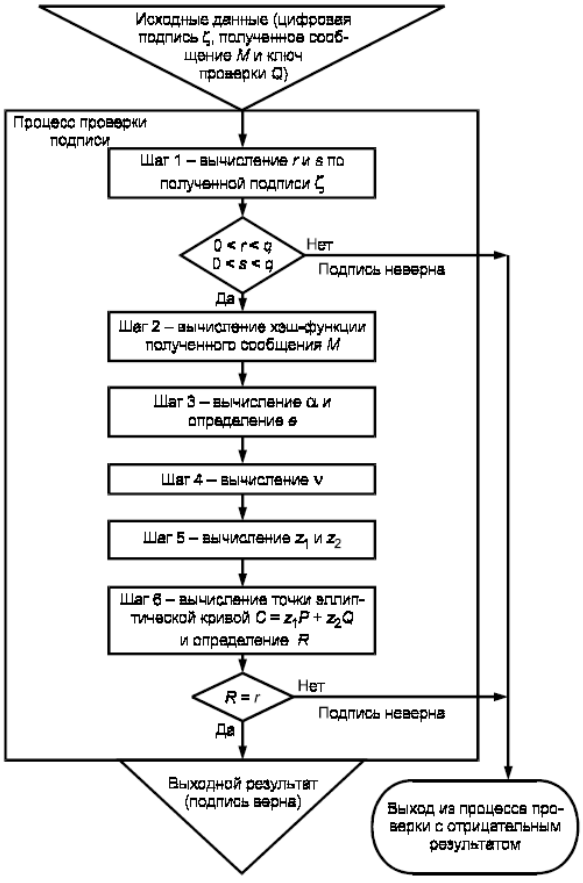

Рисунок 3 – Схема процесса проверки цифровой подписи

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.3. 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 p, a, b, m, q, P, 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

$$12345\backslash\backslash$$
$$67890_{10}$$
$$499602D2_{16}$$

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 p присвоено следующее значение:

$$p = 57896044618658097711785492504343953926\backslash\backslash$$
$$6349923328202820197287920039565648210 41_{10}$$
$$p = 8000000000000000000000000000000000000000000000000000000000000431_{16}$$

Б.1.2 Коэффициенты эллиптической кривой.

В данном примере параметры a и b принимают следующие значения:

$$a = 7_{10}$$
$$a = 7_{16}$$
$$b = 43308876546767276905765904595650931995\backslash\backslash$$
$$942111794451039583252968842033849580414_{10}$$
$$b = 5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514C0CE9DAE23B7E_{16}$$

Б.1.3. Порядок группы точек эллиптической кривой.

В данном примере параметр m принимает следующее значение:

$$m = 57896044618658097711785492504343953926\backslash\backslash$$

$$70829345837254506223809735921376310696 19_{10}$$

$$m = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3_{16}$$

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

В данном примере параметр q принимает следующее значение:

$$q = 57896044618658097711785492504343953 92\backslash\backslash$$

$$70829345837254506223809735921376310696 19_{10}$$

$$q = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3_{16}$$

Б.1.5. Коэффициенты точки эллиптической кривой.

В данном примере координаты точки P принимают следующие значения:

$$x_p = 2_{10}$$

$$x_p = 2_{16}$$

$$y_p = 4018974056539037503354494229370597\backslash\backslash$$

$$7563573938990554508069097936521343156628 0_{10}$$

$$y_p = 8E2A8A0E65147D4BD6316030E16D19\backslash\backslash$$

$$C85C97F0A9CA267122B96ABBCEA7E8FC8_{16}$$

Б.1.6. Ключ подписи.

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

$$d = 554411960653632461263556241303241831\backslash\backslash$$

$$9657670922234001657210809775000609752554 4_{10}$$

$$d = 7A929ADE789BB9BE10ED359DD39A72C\backslash\backslash$$

$$11B60961F49397EEE1D19CE9891EC3B28_{16}$$

Б.1.7. Ключ проверки.

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

$$x_q = 57520216126176808443631405023338071\backslash\backslash$$

$$1766301049063136321828967413422066048594 03_{10}$$

$$x_q = 7F2B49E270DB6D90D8595BEC458B5\backslash\backslash$$

$$0C58585BA1D4E9B788F6689DBD8E56FD80B_{16}$$

$$y_q = 1761494441921378154380939194965408 0\backslash\backslash$$

$$0319426620453636392607098478594382867639 94_{10}$$

$$y_q = 26F1B489D6701DD185C8413A977B3\backslash\backslash$$

$$CBBAF64D1C593D26627DFFB101A87FF77DA_{16}$$

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

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

$$e = 20798893674476452017134061561508270 13\backslash\backslash$$

$$0637142515379653289952617252661468872421_{10}$$

$$e = 2DFBC1B372D89A1188C09C52E0EE\backslash\backslash$$

$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$$

$$k = 53854137677348463731403841147996619 2\backslash\backslash$$

$$4150400343430202071296083852893196233395_{10}$$

$$k = 77105C9B20BCD3122823C8CF6FCC\backslash\backslash$$

$$7B956DE33814E95B7FE64FED924594DCEAB3_{16}$$

При этом кратная точка $C = kP$ имеет координаты:

$$x_C = 29700980915817952874371204983938256 9\backslash\backslash$$

$$9042275210799431965163268798205921093339 5_{10}$$

$$x_C = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$

$$A41974053554A42767B83AD043FD39DC0493_{16}$$

$$y_C = 32842535278684663477094665322517084 5\backslash\backslash$$

$$0680472103245454326813285455653927406091 0_{10}$$

$$y_C = 489C375A9941A3049E33B34361DD\backslash\backslash$$

$$204172AD98C3E5916DE27695D22A61FAE46E_{16}$$

Параметр $r \equiv x_C \pmod q$ принимает значение:

$$r = 297009809158179528743712049839382569\backslash\backslash$$
$$90422752107994319651632687982059210933395_{10}$$
$$r = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$

Параметр $s \equiv (rd + ke) \pmod q$ принимает значение:

$$s = 57497340027008465417892531001914703\backslash\backslash$$
$$84552270426490985639337189991755158395 52_{10}$$
$$s = 1456C64BA4642A1653C235A98A60249BCD6D3F746B631DF928014F6C5BF9C40_{16}$$

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

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

$$e = 20798893674476452017134061561508270 13\backslash\backslash$$
$$06371425153796532899526172526614688724 21_{10}$$
$$e = 2DFBC1B372D89A1188C09C52E0EE\backslash\backslash$$
$$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$$

При этом параметр $v \equiv e^{-1} \pmod q$ принимает значение:

$$v = 17686683605934468677301713824900268 5\backslash\backslash$$
$$62746883080675496715288036572431145718978_{10}$$
$$v = 271A4EE429F84EBC423E388964555BB\backslash\backslash$$
$$29D3BA53C7BF945E5FAC8F381706354C2_{16}$$

Параметры $z_1 \equiv sv \pmod q$ и $z_2 \equiv -rv \pmod q$ принимают значения:

$$z_1 = 37699167500901938556841057293512656 1\backslash\backslash$$
$$08841345190491942619304532412743720999759_{10}$$
$$z_1 = 5358F8FFB38F7C09ABC782A2DF2A\backslash\backslash$$
$$3927DA4077D07205F763682F3A76C9019B4F_{16}$$
$$z_2 = 14171998427343472112515917969500765 7\backslash\backslash$$
$$69246655838972862114499932653333671092 21_{10}$$
$$z_2 = 3221B4FBBF6D101074EC14AFAC2D4F7\backslash\backslash$$
$$EFAC4CF9FEC1ED11BAE336D27D527665_{16}$$

Точка $C = z_1 P + z_2 Q$ имеет координаты:

$$x_C = 297009809158179528743712049839382569 9\backslash\backslash$$
$$04227521079943196516326879820592109333 95_{10}$$
$$x_C = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$
$$y_C = 32842535278684663477094665322517084 50\backslash\backslash$$
$$68047210324545432681328545565392740609 10_{10}$$
$$y_C = 489C375A9941A3049E33B34361DD\backslash\backslash$$
$$204172AD98C3E5916DE27695D22A61FAE46E_{16}$$

Тогда параметр $R \equiv x_C \pmod q$ принимает значение:

$$R = 297009809158179528743712049839382569 9\backslash\backslash$$
$$04227521079943196516326879820592109333 95_{10}$$
$$R = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}$$

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

ПРИЛОЖЕНИЕ 2
Федеральный закон от 10 января 2002 г. № 1-ФЗ
«Об электронной цифровой подписи»

Принят Государственной Думой 13 декабря 2001 года
Одобрен Советом Федерации 26 декабря 2001 года

Глава I. Общие положения

Статья 1. Цель и сфера применения настоящего Федерального закона.

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Статья 2. Правовое регулирование отношений в области использования электронной цифровой подписи.

Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с настоящим Федеральным законом, Гражданским кодексом Российской Федерации, Федеральным законом "Об информации, информатизации и защите информации", Федеральным законом "О связи", другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также осуществляется соглашением сторон.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе.

Для целей настоящего Федерального закона используются следующие основные понятия:

- электронный документ - документ, в котором информация представлена в электронно-цифровой форме;
- электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;
- владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);
- средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

- сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;
- закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;
- открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;
- сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;
- подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;
- пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;
- информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;
- корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Глава II. Условия использования электронной цифровой подписи

Статья 4. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи.

1. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:
- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

2. Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Статья 5. Использование средств электронной цифровой подписи.

1. Создание ключей электронных цифровых подписей осуществляется для использования в:

- информационной системе общего пользования ее участником или по его обращению удостоверяющим центром;
- корпоративной информационной системе в порядке, установленном в этой системе.

2. При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством Российской Федерации.

3. Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается.

4. Сертификация средств электронной цифровой подписи осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг.

Статья 6. Сертификат ключа подписи.

1. Сертификат ключа подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

2. В случае необходимости в сертификате ключа подписи на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи, а по его заявлению в письменной форме - иные сведения, подтверждаемые соответствующими документами.

3. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

4. Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется

собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

Статья 7. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре.

1. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

2. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации.

3. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Глава III. Удостоверяющие центры

Статья 8. Статус удостоверяющего центра.

1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы.

2. Деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности.

Статья 9. Деятельность удостоверяющего центра.

1. Удостоверяющий центр:

- изготавливает сертификаты ключей подписей;
- создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;
- может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

2. Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в статье 6 настоящего Федерального закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

3. При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй - остается в удостоверяющем центре.

4. Услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов оказываются безвозмездно.

Статья 10. Отношения между удостоверяющим центром и уполномоченным федеральным органом исполнительной власти.

1. Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченного лица удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра.

2. Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц удостоверяющих центров.

3. Электронные цифровые подписи уполномоченных лиц удостоверяющих центров могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих электронных цифровых подписей для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

4. Уполномоченный федеральный орган исполнительной власти:

- осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;
- осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия настоящего Федерального закона.

Статья 11. Обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи.

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

- вносить сертификат ключа подписи в реестр сертификатов ключей подписей;
- обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;
- приостанавливать действие сертификата ключа подписи по обращению его владельца;
- уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;
- иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Статья 12. Обязательства владельца сертификата ключа подписи.

1. Владелец сертификата ключа подписи обязан:

- не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;
- хранить в тайне закрытый ключ электронной цифровой подписи;
- немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

2. При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

Статья 13. Приостановление действия сертификата ключа подписи.

1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования.

2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен.

3. Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по ис-

течении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

4. В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

Статья 14. Аннулирование сертификата ключа подписи.

1. Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

- по истечении срока его действия;
- при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;
- в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;
- по заявлению в письменной форме владельца сертификата ключа подписи;
- в иных установленных нормативными правовыми актами или соглашением сторон случаях.

2. В случае аннулирования сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата ключа подписи.

Статья 15. Прекращение деятельности удостоверяющего центра.

1. Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, может быть прекращена в порядке, установленном гражданским законодательством.

2. В случае прекращения деятельности удостоверяющего центра, указанного в пункте 1 настоящей статьи, сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы другому удостоверяющему центру по согласованию с владельцами сертификатов ключей подписей.

Сертификаты ключей подписей, не переданные в другой удостоверяющий центр, аннулируются и передаются на хранение в соответствии со статьей 7 настоящего Федерального закона уполномоченному федеральному органу исполнительной власти.

3. Деятельность удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, прекращается по решению владельца этой системы, а также по договоренности участников этой системы в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы.

Глава IV. Особенности использования электронной цифровой подписи

Статья 16. Использование электронной цифровой подписи в сфере государственного управления.

1. Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организа-

ции, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

2. Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном настоящим Федеральным законом для удостоверяющих центров.

3. Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов.

Статья 17. Использование электронной цифровой подписи в корпоративной информационной системе.

1. Корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, установленным настоящим Федеральным законом для информационных систем общего пользования.

2. Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

3. Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Статья 18. Признание иностранного сертификата ключа подписи.

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов.

Статья 19. Случаи замещения печатей.

1. Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

2. В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Глава V. Заключительные и переходные положения

Статья 20. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом.

1. Нормативные правовые акты Российской Федерации подлежат приведению в соответствие с настоящим Федеральным законом в течение трех месяцев со дня вступления в силу настоящего Федерального закона.

2. Учредительные документы удостоверяющих центров, выдающих сертификаты ключей подписей для использования в информационных системах общего пользования, подлежат приведению в соответствие с настоящим Федеральным законом в течение шести месяцев со дня вступления в силу настоящего Федерального закона.

Статья 21. Переходные положения.

Удостоверяющие центры, создаваемые после вступления в силу настоящего Федерального закона до начала ведения уполномоченным федеральным органом исполнительной власти реестра сертификатов ключей подписей, должны отвечать требованиям настоящего Федерального закона, за исключением требования предварительно представлять сертификаты ключей подписей своих уполномоченных лиц уполномоченному федеральному органу исполнительной власти. Соответствующие сертификаты должны быть представлены указанному органу не позднее чем через три месяца со дня вступления в силу настоящего Федерального закона.

ЛИТЕРАТУРА

1. Fulton W. Algebraic Curves. Menlo Park: Benjamin, 1969.
2. Husemoller D. Elliptic Curves. Heidelberg etc.: Springer, 1987.
3. Koblitz N. Introduction to Elliptic Curves and Modular Forms. 2nd ed. Heidelberg etc.: Springer, 1993.
4. Koblitz N. Why study equations over finite fields? – Math Mag., 1982, v. 55, p. 144-149.
5. Lang S. Elliptic Curves: Diophantine Analysis. Heidelberg etc.: Springer, 1978.
6. Silverman J. The Arithmetic of Elliptic Curves. Heidelberg etc.: Springer, 1986.