

Лабораторная работа № 11

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых (содержит 3 самостоятельных задания, каждое из которых рассчитано на 2 часа аудиторных занятий).

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и геометрическому представлению операций над эллиптическими кривыми (ЭК):

- по алгоритмам согласования ключевой информации на основе ЭК;
- алгоритмам зашифрования/расшифрования информации на основе асимметричной криптографии и ЭК;
- алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и ЭК;
- оценке криптостойкости систем на основе ЭК.

2. Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.

3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

11.1. Теоретические сведения

11.1.1. Эллиптические кривые над действительными числами и конечными полями

11.1.1.1. ЭК над действительными числами

Мы ранее отмечали, что криптография базируется на задачах факторизации, дискретного логарифмирования и операциях над

точками эллиптической кривой (Elliptic Curve, EC; EC Cryptography, ECC). Последние являются предметом исследования в данной работе.

Перед выполнением лабораторной работы целесообразно ознакомиться с базовыми элементами теории эллиптических кривых (см., например, п. 5.4.4 в [3]).

Здесь вспомним основные определения и кратко проанализируем базовые операции над точками эллиптических кривых (ЭК).

Определение 1. Эллиптические кривые – математический объект, который может быть определен над любым полем.

Определение 2. Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением

$$y^2 = x^3 + ax + b, \quad (11.1)$$

при этом константы (a и b – вещественные числа) должны удовлетворять условию

$$4a^3 + 27b^2 \neq 0. \quad (11.2)$$

Нетрудно понять, что вид ЭК (11.1) также задается парой чисел: a и b .

Формула (11.1) называется **уравнением Вейерштрасса**, а условие (11.2) исключает из рассмотрения *кривые с особыми точками* или *особые кривые*.

В зависимости от значений a и b ЭК могут принимать на плоскости разные формы (см. также [3]).

Определение 3. Частью ЭК является **бесконечно удаленная точка** (также известная как **идеальная точка**), которую мы обозначим символом O .

Определение 4. Группа – непустое множество с определенной на нем бинарной операцией, называемой сложением и удовлетворяющей нескольким аксиомам.

На основе последнего определения мы можем определить группу для ЭК.

Определение 5. Группа для ЭК есть непустое множество, элементы которого являются точками ЭК, обладающими следующими свойствами:

- *единичный элемент* – это бесконечно удаленная точка O ;
- *обратная величина точки* R – это точка, симметричная относительно оси X ;

• *сложение* задается следующим правилом: сумма трех ненулевых точек P , Q и $-R$, лежащих на одной прямой, будет равна $P + Q + (-R) = O$.

В соответствии с этим можем сформулировать *законы сложения точек эллиптической кривой*:

• прямая, проходящая через точки R и $-R$, является вертикальной прямой, которая не пересекает ЭК ни в какой третьей точке; если $R = (x, -y)$, то $R + (x, y) = O$. Точка (x, y) является отрицательным значением точки R и обозначается $-R$. Таким образом, по определению $R + (-R) = O$;

• $P + Q = R$: пусть P и Q – две различные точки ЭК (рис. 11.1), и P не равно Q ; если проведем через P и Q прямую, то она пересечет ЭК еще только в одной точке, называемой $-R$; точка $-R$ отображается относительно оси X в точку R , равную сумме точек P и Q : $P + Q = R$.

Геометрическая интерпретация операции сложения двух точек показана на рис. 11.1.

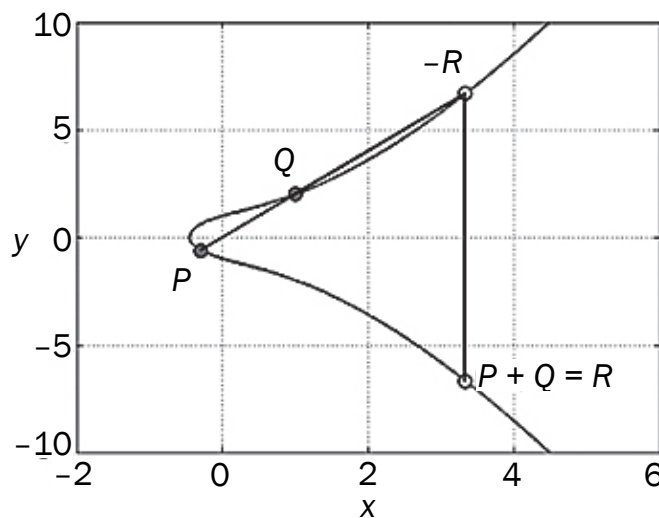


Рис. 11.1. Пояснение к операции сложения двух точек P и Q эллиптической кривой $y^2 = x^3 + 2x + 1$ ($a = 2$, $b = 1$)

Что будет, если $P = Q$? В этом случае мы можем говорить об операции *удвоения точки*: $P + P = 2P$. Обобщив (к точке $2P$ можно прибавить еще раз точку P : $2P + P$), сформулируем принцип умножения точки P на целое положительное число n – это сумма n точек P : $nP = P + P + P + \dots + P$.

Скалярное умножение осуществляется посредством нескольких комбинаций сложения и удвоения точек эллиптической кривой.

Например, точка $25P$ может быть представлена как $25P = 2(2(2(2P))) + 2(2(2P))) + P$.

Понятно, что каждая точка на плоскости задается парой координат: x и y .

Числа x и y являются *рациональными*, а точки P , Q , R и $-R$ (как и любые точки ЭК) – *рациональными точками*.

Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ определяется в соответствии с правилами:

$$x_3 = \lambda^2 - x_1 - x_2; \quad (11.3)$$

$$y_3 = \lambda(x_1 - x_3) - y_1, \quad (11.4)$$

где

$$\lambda = (y_2 - y_1)/(x_2 - x_1) \text{ при } P \neq Q \text{ и } \lambda = (3(x_1)^2 + a)/2y_1 \text{ при } P = Q. \quad (11.5)$$

Из этого следует, что число λ – угловой коэффициент секущей, проведенной через точки $P = (x_1, y_1)$ и $Q = (x_2, y_2)$. При $P = Q$ секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления λ .

Хорошее представление об операциях над точками различных ЭК можно получить, воспользовавшись онлайн-приложением, доступным по ссылке: <https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/real-add.html>.

Для примера на рис. 11.2 приведено окно этого приложения.

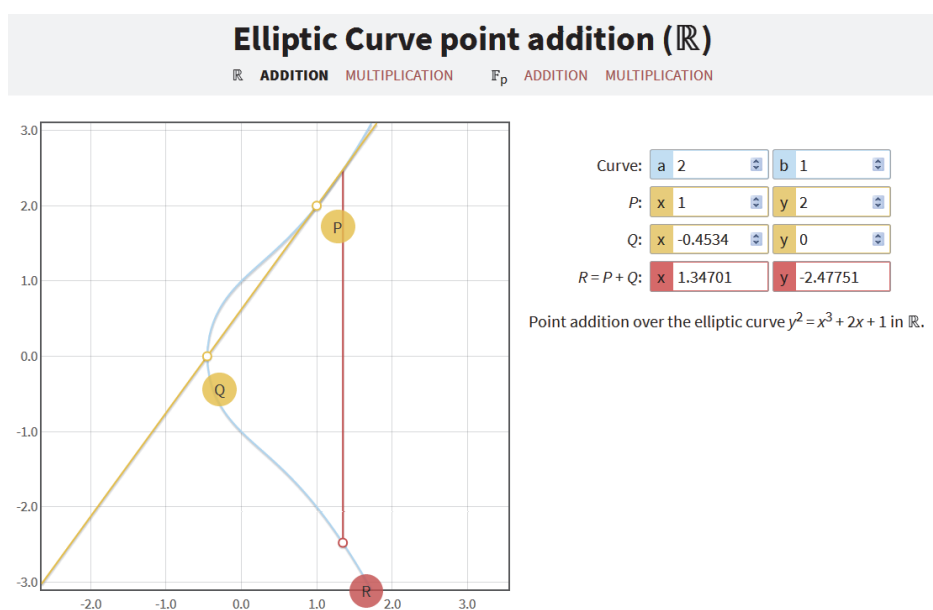


Рис. 11.2. Окно приложения *Elliptic Curve Points Addition*

На приведенном рисунке как раз представлен пример над точками (координаты в правой части экрана), упоминавшимися выше (см. рис. 11.1) ЭК. Отметим также, что при этом выбраны опции **R** и **Addition** (вторая строка), соответствующие операции сложения над рациональными числами.

Рассмотрим пример.

Пример 1. Пусть ЭК задается уравнением с параметрами $a = -7$, $b = 10$. Точки $P(1, 2)$ и $Q(3, 4)$. Нужно вычислить сумму точек: $P + Q = R$.

Воспользуемся выражениями (11.3)–(11.5):

$$\lambda = (2 - 4) / (1 - 3) = 1,$$

$$x_R = x_3 = 1^2 - 1 - 3 = -3,$$

$$y_R = y_3 = 2 + 1 \cdot (-3 - 1) = -2.$$

Тот же результат получаем и при использовании указанного выше приложения.

Пример 2. Для той же ЭК при $P(1, 2) = Q(1, 2)$ получим для $P + Q = R = 2P$:

$$\lambda = 3(1^2 - 7) / (2 \cdot 2) = -1,$$

$$x_R = x_3 = (-1)^2 - 1 - 1 = -1,$$

$$y_R = y_3 = 2 + (-1) \cdot (-1 - 1) = 4.$$

Таким образом, получили точку $2P(-1, 4)$.

С помощью упомянутого выше приложения (опции **R** и **Multiplication**) можно вычислить любые операции *скалярного умножения точки*.

Для заданных n и P существуют алгоритмы вычисления $Q = nP$. Если же известны Q и P , а нам нужно определить n , то такая задача нам известна как *задача логарифмирования*.

11.1.1.2. ЭК над конечными полями

Именно этот тип ЭК будет нас интересовать в плане практического применения.

Определение 6. Конечное поле – это множество конечного числа элементов. Примером конечного поля является множество целых чисел по модулю p , где p – простое число.

Поле обозначается как $GF(p)$ или F_p . Здесь операции сложения и умножения работают как в модулярной арифметике.

Например, поле F_{13} ($p = 13$) состоит из чисел: $0, 1, \dots, 12$.

Определение 7. Эллиптическая кривая над полем F_p задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю $p \pmod{p}$:

$$y^2 \equiv x^3 + ax + b \pmod{p}, \quad (11.6)$$

далее для упрощения используем знак простого неравенства:

$$4a^3 + 27b^2 \neq 0 \pmod{p} \quad (11.7)$$

и т. д.

Формально ЭК над полем задается так: $E_p(a, b)$.

Важно отметить, что, как и ранее, существует точка (бесконечно удаленная) O ; a и b – вещественные числа.

Прежде чем приступить к алгебраическим операциям над точками кривой, такими как суммирование двух разных точек на ЭК и удвоение точек, кратко проанализируем операции для расчета точек, принадлежащих ЭК. Должны быть приняты некоторые предположения, такие как площадь, на которой будут рассчитываться точки кривой, и функция кривой.

Рассмотрим конкретный пример.

Пример 3. Пусть ЭК формально задается записью $E_{13}(6, -9)$. Проверяем выполнение условия (11.7). Исходя из этого, координаты расположения точек должны быть ограничены квадратом некоторых чисел по модулю 13 (левая часть основного уравнения – y^2). Здесь стоит отметить известную нам цикличность в вычислениях на основе модулярной арифметики. Это видно для нашего случая из табл. 11.1.

Таблица 11.1

Цикличность квадратов целых чисел над полем F_{13}

$0^2 \bmod 13 = 0$	$13^2 \bmod 13 = 0$
$1^2 \bmod 13 = 1$	$14^2 \bmod 13 = 1$
$2^2 \bmod 13 = 4$	$15^2 \bmod 13 = 4$
$3^2 \bmod 13 = 9$	$16^2 \bmod 13 = 9$
$4^2 \bmod 13 = 3$	$17^2 \bmod 13 = 3$
$5^2 \bmod 13 = 12$	$18^2 \bmod 13 = 12$
$6^2 \bmod 13 = 10$	$19^2 \bmod 13 = 10$
$7^2 \bmod 13 = 10$	$20^2 \bmod 13 = 10$
$8^2 \bmod 13 = 12$	$21^2 \bmod 13 = 12$
$9^2 \bmod 13 = 3$	$22^2 \bmod 13 = 3$
$10^2 \bmod 13 = 9$	$23^2 \bmod 13 = 9$
$11^2 \bmod 13 = 4$	$24^2 \bmod 13 = 4$
$12^2 \bmod 13 = 1$	$25^2 \bmod 13 = 1$

Числа, приведенные после знаков равенства, являются *квадратичными вычетами* по модулю 13. В данном примере это числа из множества $\{1, 3, 4, 9, 10, 12\}$ (обычно число 0 не включают в такие множества).

Важным элементом рассматриваемой технологии является определение точек кривой с целочисленными координатами. Эти задачи в общем случае решаются на основе известных алгоритмов, которые мы здесь опустим. Имея приведенные в табл. 11.1 вычисления квадратов чисел по модулю 13, рассмотрим ситуацию для $x = 0$. Подставим это значение в правую часть уравнения (11.6), имея в виду ЭК $E_{13}(6, -9)$:

$$y^2 = 0^3 + 6 \cdot 0 - 9 \pmod{13},$$

откуда получим $y^2 = -9 \pmod{13}$, $y^2 = 4$ и $y = \pm 2$. Таким образом, пользуясь данными из табл. 11 (смотрим строки с числами 4 справа от знака равенства), определяем, что точками нашей ЭК будут: $(0, 2)$ и $(0, 11)$; здесь мы приняли во внимание то, что значение некоторого целого отрицательного числа $(-k)$ по модулю (p) вычисляется следующим образом:

$$(-k) \pmod{p} \equiv -(k \pmod{p}) + p.$$

Следуя приведенной логике рассуждений, определим, например, точки при $x = 3$: $y^2 = 3^3 + 6 \cdot 3 - 9 \pmod{13} = 36 \pmod{13} = 10$. Обращаем внимание на 7-ю и 8-ю строки левого столбца табл. 11.1 и устанавливаем координаты еще 2 точек ЭК: $(3, 6)$, $(3, 7)$.

Теперь вернемся к $x = 1$: $y^2 = 1^3 + 6 \cdot 1 - 9 \pmod{13} = -2 \pmod{13} = 11$. В табл. 11.1 не найдено ни одного соответствия. Это означает, что на рассматриваемой ЭК нет ни одной точки, координата x которой равна 3.

На рис. 11.3 представлены все точки для ЭК $E_{13}(6, -9)$.

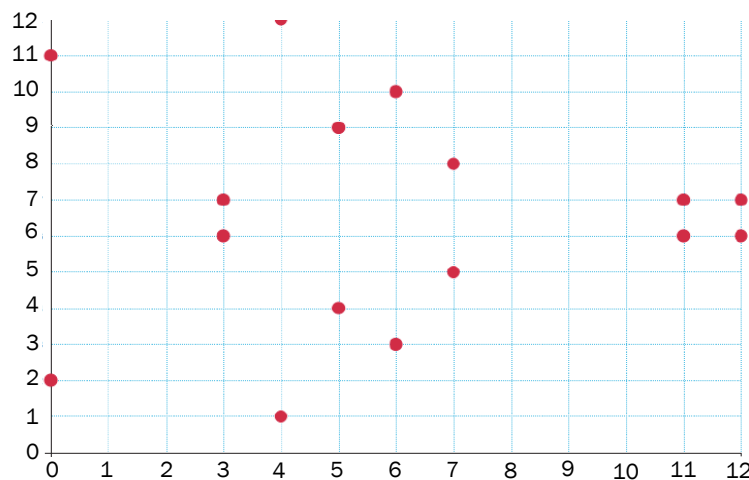


Рис. 11.3. Точки ЭК $E_{13}(6, -9)$

На рис. 11.4 показаны точки эллиптической кривой $(7, 10)$ из примера 1 для $p = 19$ (а) и для $p = 487$ (б).

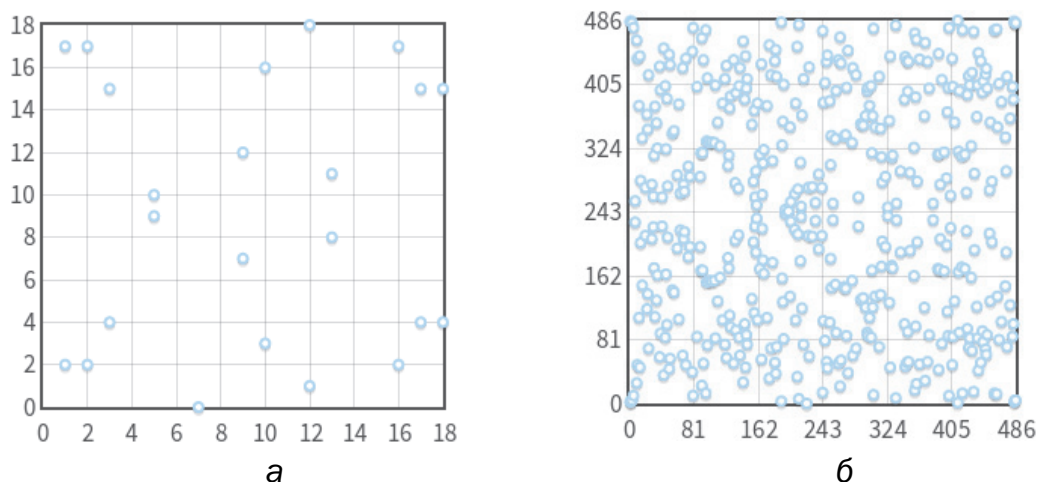
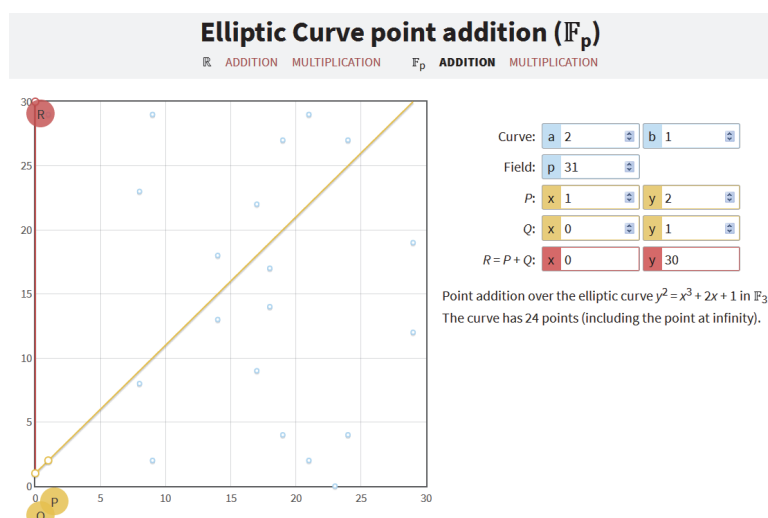


Рис. 11.4. Отображение точек ЭК $y^2 = x^3 - 7x + 10 \pmod{p}$
(источник: <https://habr.com/ru/post/335906/>)

Из приведенных примеров можно заметить, что для каждого x существует максимум две точки. Отметим также симметрию в расположении точек относительно $y = p/2$. То, что раньше было непрерывной кривой, теперь стало множеством отдельных точек на плоскости XY , координаты которых (x и y) являются целыми числами.

Можно также сказать, что три точки находятся на одной прямой, если существует прямая, соединяющая их. Рис. 11.3 и 11.4 дают более полное представление о числовом пространстве точек ЭК над конечным полем.

На рис. 11.5 показано геометрическое отображение операции суммирования двух точек с параметрами, примерно соответствующими рис. 11.2 (не для любых параметров выполняется операция).



Рассмотрим пример.

Пример 4. Пусть $p = 23$. Рассмотрим ЭК $y^2 = x^3 + x + 1 \pmod{23}$: $E_{23}(1, 1)$.

Кривая состоит из следующих точек: $(0, 1)$; $(0, 22)$; $(1, 7)$; $(1, 16)$; $(3, 10)$; $(3, 13)$; $(4, 0)$; $(5, 4)$; $(5, 19)$; $(6, 4)$; $(6, 19)$; $(7, 11)$; $(7, 12)$; $(9, 7)$; $(9, 16)$; $(11, 3)$; $(11, 20)$; $(12, 4)$; $(12, 19)$; $(13, 7)$; $(13, 16)$; $(17, 3)$; $(17, 20)$; $(18, 3)$; $(18, 20)$; $(19, 5)$; $(19, 18)$, т. е. всего 27 точек.

Не забываем, что во всех случаях эллиптической кривой принадлежит также точка O .

Пусть $P = (3, 10)$ и $Q = (9, 7)$. Найдем $P + Q$ и $2P$.

Пусть $P + Q = (x_3, y_3)$, тогда при $\lambda = (7 - 9) / (9 - 3) \pmod{23} = 11 \pmod{23}$ имеем:

$$x_3 = 121 - 3 - 9 \pmod{23} = 109 \pmod{23} = 17,$$

$$y_3 = 11(3 + 6) - 10 \pmod{23} = 89 \pmod{23} = 20.$$

Таким образом, $P + Q = (17, 20)$.

Такой же результат получен и с использованием упомянутого онлайн-ресурса (рис. 11.6).

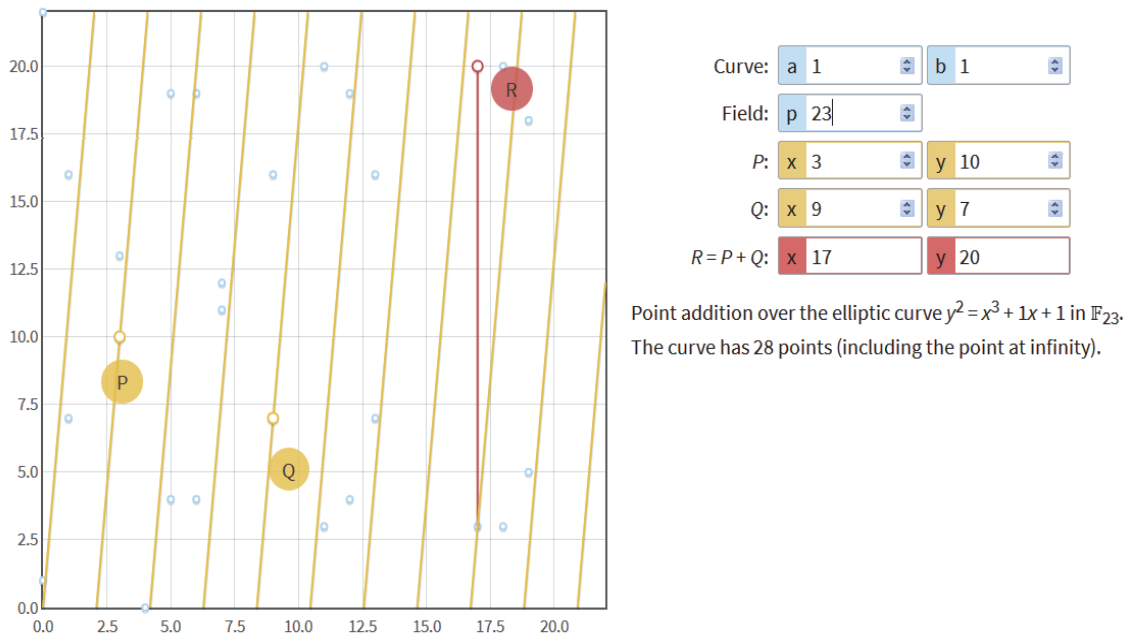


Рис. 11.6. Окно приложения с результатами выполнения операции сложения двух точек из примера 2

Найдем теперь точку $2P = P + P = (x_3, y_3)$ – с формальной точки зрения это также будет третья точка.

Для этого случая

$$\lambda = (3 \cdot 9 + 1) \pmod{23} = 6 \pmod{23}$$

и с учетом последнего для вычисления координаты y_3 :

$$x_3 = 36 - 6 \pmod{23} = 30 \pmod{23} = 7 \pmod{23};$$

$$y_3 = 6 \cdot (3 - 7) - 10 \pmod{23} = -34 \pmod{23} = 12 \pmod{23}.$$

Таким образом, $2P = (7, 12)$.

При последовательном выполнении сложения $nP = P + P + P + \dots + P$ на каждом шаге будет получаться точка, которая также должна принадлежать $E_p(a, b)$. В силу того что эллиптическая группа содержит конечное множество точек, наступает такой момент, что для некоторых результатов вычислений будет выполняться равенство $qP = O$ (см. пример 5.12 из [3], где $5A = O$, т. е. здесь $q = 5$).

Пример 5. Для точки $P(4, 2)$ ЭК вида $E_7(4, 1)$ справедливы следующие соотношения:

$$2P = (4, 2) + (4, 2) = (0, 1),$$

$$3P = (0, 1) + (4, 2) = (0, 6),$$

$$4P = 2(0, 1) = (4, 5),$$

$$5P = (0, 1) + (0, 6) = O.$$

Для данного случая также $q = 5$.

Если взять разные точки на одной и той же ЭК, получим разные q . В табл. 11.2 показаны умножения точки для ЭК $E_5(0, 1)$.

Таблица 11.2

Результаты выполнения операции $P + \dots + P$ для кривой $E_5(0, 1)$

+	(0, 1)	(0, 4)	(2, 2)	(2, 3)	(4, 0)
P	(0, 1)	(0, 4)	(2, 2)	(2, 3)	(4, 0)
$2P$	(0, 4)	(0, 1)	(0, 4)	(0, 1)	O
$3P$	O	O	(4, 0)	(4, 0)	(4, 0)
$4P$	(0, 1)	(0, 4)	(0, 1)	(0, 4)	O
$5P$	(0, 4)	(0, 1)	(2, 3)	(2, 2)	(0, 4)
$6P$	O	O	O	O	O

Данные приведенной таблицы подтверждают наши выводы.

Если требуется, например, точку P сложить самой с собой z раз, то это означает, что нужно выполнить вычисление zP . Для реализации этой операции существует простой метод на основе операции сложения точек. Число z представляется в двоичном виде. И далее

вычисляются необходимые составляющие общей суммы на основе весовых (единичных) разрядов двоичного числа z . Рассмотрим это на примере.

Пример 6. Пусть $z = 171$. Это число в двоичном виде выглядит так: 10101011. В соответствии с весом «1» мы должны сложить следующие составляющие (слагаемые) общей суммы: $171P = P + 2P + 8P + 32P + 128P$.

Первое из приведенных слагаемых известно. Второе слагаемое: $2P = P + P$, промежуточное вычисление: $4P = 2P + 2P$, третье слагаемое: $8P = 4P + 4P$, промежуточное вычисление: $16P = 8P + 8P$, промежуточное вычисление: $16P = 8P + 8P$, четвертое слагаемое: $32P = 16P + 16P$, промежуточное вычисление: $64P = 32P + 32P$, последнее слагаемое: $128P = 64P + 64P$.

Определение 8. Если мы складываем два значения, кратных P , то получаем значение, кратное P (т. е. значения, кратные P , замкнуты относительно операции сложения). Это означает, что *множество кратных P значений – это циклическая подгруппа группы, образованной эллиптической кривой.*

Определение 9. Наименьшее значение числа q , для которого выполняется равенство $qP = O$, называется *порядком точки P .*

Определение 10. *Порядок группы точек эллиптической кривой* равен числу различных точек ЭК, включая точку O .

Определение 11. Точка P называется *генератором* или *базовой точкой* циклической подгруппы (такую точку во многих документах обозначают символом G).

Порядок точки P связан с порядком m ЭК *теоремой Лагранжа*, согласно которой *порядок подгруппы – это делитель порядка исходной группы.* Иными словами, если ЭК содержит m точек, а одна из подгрупп содержит q , то q является делителем m .

Для ЭК $E_p(a, b)$ порядок m группы точек должен удовлетворять неравенству

$$p + 1 - 2p^{1/2} \leq m \leq p + 1 + 2p^{1/2}.$$

! Как и в случае с непрерывными ЭК, теперь важным является вычисление некоторого числа d , если мы знаем P и Q для $Q = dP$. Это и есть *задача дискретного логарифмирования* для эллиптических кривых.

Эта задача аналогична задаче дискретного логарифмирования, используемой в других криптосистемах, таких как алгоритм DSA, протокол Диффи – Хеллмана и схема Эль-Гамала.

! В криптографии на основе ЭК тайный ключ – это случайное целое d , выбранное из множества $\{1, 2, \dots, q - 1\}$, где q – порядок подгруппы; *открытый ключ* – это точка Q , такая, что $Q = dG$, где G – базовая точка подгруппы.

Криптостойкость алгоритмов на основе ЭК определяется, например, для алгоритма ЭЦП в стандарте Республики Беларусь [51] параметром l , называемым *уровнем стойкости* и принимающим значения (рекомендуется) из $\{128, 192, 256\}$. При этом для взлома ключа злоумышленнику нужно выполнить 2^l операций.

11.1.1.3. Основные этапы генерации ключевой информации на основе ЭК

Первый этап: выбор (генерация) ЭК. Обычно он основан на выполнении следующих условий и операций.

1.1. Входными параметрами являются: число l , число p , удовлетворяющее условию $2^{2l-1} < p < 2^{2l}$, $p \equiv 3 \pmod{4}$, $0 < a < p$. Можно использовать некоторое простое число $p = 2^{2l} - c$, где c – небольшое натуральное число.

1.2. Выбирается число b такое, что $0 < b < p$.

Таким образом, задана ЭК: $E_p(a, b)$.

1.3. Выбираются порядок q (простое число) и генерирующая точка G , которая задается двумя координатами, например $G = (0, y_G)$.

Дополнительно к рассмотренным действиям стандарт [51] предусматривает использование вспомогательного параметра $(s, seed)$ – произвольное 64-битное число.

Для примера в таблицах ниже (табл. 11.3 и 11.4) [51] приведены параметры ЭК для двух значений l . Здесь нижние индексы в левом столбце обозначают битовую длину числа.

Второй этап: генерация ключевой информации.

2.1. Входными параметрами являются: p, a, b, q и G .

2.2. Генерируется тайный ключ – число d , выбранное из множества $\{1, 2, \dots, q - 1\}$.

2.3. Вычисляется открытый ключ – точка Q :

$$Q = dG, \quad (11.8)$$

к открытому ключу также относятся p, a, b, q .

Отметим также, что можно сгенерировать ключевую информацию на основе ЭК, воспользовавшись известной нам библиотекой *OpenSSL*. Например, если воспользоваться версией *OpenSSL1.1.1L*

в системе *Debian 9* (с помощью команды с двумя разными псевдонимами (выделены жирным)):

*openssl ecparam -name secp192k1 -genkey -out **secp192k1**,*

*openssl ecparam -name secp521r1 -genkey -out **secp521r1**,*

то получим тайные ключи соответствующего содержания:

MFwCAQEEGLDsGwgZq/Kq4suR74ftkipbKMRmoWDtlqAHBgUrgQQA
H6E0AzIABPfKazFU+QKsh+I7a6K5taNUe3TZAdLMp92RpYo
T0PIrmGD3QVRcqAmqZSba6kanKg==

MIHcAgEBBEIAvv7P//lWx3QQis5Hb25eN/UY5isVJk+s56ZDSTle
Ucrqj2mNH4Y3xWLXGMtpmDJRiHalCv3MDt/T5h67daHaViagBwYF
K4EEACOhgYkDgYYABABgOPla5ygHB/j79g0R2N12/tv4Yllj6ZA+t2F
htvEMPvj9QHMG5sN45yjGKmLllwEMP2YWxjPj3YL0Z0uLO9BBYwB
UGVCPEWKylC8x5qGLlypG6shCPTUcXQxLuFMmKv+AaDH24TCd
Bvl9nYANhlxZKv96Pb/lari3OKZkmO5zgVWKCw==

Таблица 11.3

Стандартные параметры ЭК ($l = 128$)

p $\langle p \rangle_{256}$	$2^{256} - 189$ 43FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ₁₆
a $\langle a \rangle_{256}$	$2^{256} - 192$ 40FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ₁₆
$\langle b \rangle_{256}$	F1039CD6 6BD2EB2 53928B97 6950F54C BEFBD8E4 AB3AC1D2 EDA8F315 156CCE77 ₁₆
seed	5E380100 00000000 ₁₆
q $\langle q \rangle_{256}$	$2^{256} - 51$ 359303463 308904523 350978545 619999225 07663D26 99BF5A7E FC4DFB0D D68E5CD9 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ₁₆
$\langle y_G \rangle_{256}$	936A5104 18CF291E 52F608C4 66399178 5D83D651 A3C9E45C 9FD616FB 3CFCF76B ₁₆

Таблица 11.4

Стандартные параметры ЭК ($l = 192$)

p $\langle p \rangle_{384}$	$2^{384} - 317$ C3FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ₁₆
a $\langle a \rangle_{384}$	$2^{384} - 320$ C0FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF ₁₆
$\langle b \rangle_{384}$	64BF7368 23FCA7BC 7CBDCEF3 F0E2BD14 3A2E71E9 F96A21A6 96B1FB0F BB482771 D2345D65 AB5A0733 20EF9C95 E1DF75C ₁₆
seed	23AF0000 00000000 ₁₆

Окончание табл. 11.4

q $\langle q \rangle_{384}$	$2^{384} - 9886\ 438520659\ 958522437\ 788006980\ 66095037\ 549058207\ 958390857$ $B7A70CF3\ 3FDCB73D\ 0AFFA4A6\ E7DA4680\ C3C4CC6C\ FFFFFFFF$ $FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF_{16}$
$\langle y_G \rangle_{384}$	$51C433F7\ 31CB5EEA\ F9422A6B\ 273E4084\ 55D3B166\ 9EE74905$ $A0FF86DC\ 119A723A\ 89BF2D43\ 7E113063\ 9E9E2EA8\ 2482435D_{16}$

Полезные рекомендации по выбору параметров ЭК можно найти, например, в [52].

11.1.2. Использование ЭК в криптографии

Отметим еще раз, что ЭК в криптографических приложениях обычно используется на этапе генерации либо согласования ключевой информации. Таким образом, можно отметить 3 направления использования ЭК в криптографии:

- в алгоритмах согласования (передачи) ключевой информации (на основе идеи Диффи – Хеллмана);
- в алгоритмах асимметричного шифрования/дешифрования сообщений;
- в алгоритмах генерации/верификации ЭЦП.

11.1.2.1. Реализация алгоритма Диффи – Хеллмана на основе ЭК

Рассмотрим наиболее общий случай. Предположим, что E_p – это ЭК над F_p , а Q – заранее определенная и согласованная сторонами **A** и **B** точка на E .

Отправитель **A** выбирает тайное случайное число k_A , вычисляет точку $P_A = k_A Q$ и отправляет ее получателю **B**. **B** действует аналогично: он случайным образом выбирает число k_B , вычисляет случайное число k_A , вычисляет точку $P_B = k_B Q$ и отправляет результат стороне **A**.

Общий ключ $P = k_A k_B Q$. Отправитель **A** вычисляет P путем умножения числа P_B , полученного от получателя **B**, на его секретное число k_A . Похожим образом действует другая сторона.

11.1.2.2. Реализация алгоритма зашифрования/расшифрования на основе ЭК

Вспомним, что процедура предусматривает использование ключей получателя (стороны **B**). Рассмотрим это на примере алгоритма Эль-Гамала.

Принимаем также во внимание, что зашифрованное сообщение M или каждый зашифрованный блок (m_i) этого сообщения состоят из двух чисел. Обратимся к лабораторной работе № 8, где блок шифртекста (c_i) в соответствии с выражениями (8.9) и (8.10) мы обозначали двумя символами a_i и b_i и вычисляли как

$$a_i \equiv g^k \bmod p, b_i \equiv (y^k m_i) \bmod p.$$

Поскольку символы a и b мы зарезервировали в текущей работе для обозначения параметров ЭК, то блок шифртекста сейчас будем обозначать соответственно символами C_{i1} и C_{i2} .

При использовании ЭК зашифрование предполагает представление сообщения в виде точки P (или представления каждого блока сообщения в виде разных точек P_i) ЭК с известной точкой G и известным Q . Соответственно шифртекст – это две точки на той же ЭК: C_1 и C_2 или C_{i1} и C_{i2} .

Предположим, что шифруемое сообщение M – это точка P на ЭК.

Сторона **A** выбирает некоторое случайное число k и далее выполняет вычисления с использованием открытого ключа стороны **B**:

$$C_1 = kG, C_2 = P + kQ. \quad (11.9)$$

Получатель для расшифрования сообщения вычисляет:

$$P = C_2 - dC_1. \quad (11.10)$$

Знак « $-$ » в (11.10) означает сложение с инверсией: инверсией по отношению к точке (x, y) является точка $(x, -y)$ на ЭК.

Рассмотрим пример.

Пример 7. Пусть сторона **B** использует ЭК вида $E_{67}(2, 3)$, $G = (2, 22)$ и $d = 4$. Тогда $Q = dG = 4G = (13, 45)$; здесь расчеты, которые проводились на основе (11.3)–(11.5), опускаются.

Полагаем далее, что шифруемое сообщение M соответствует точке $P = (24, 26)$, а $k = 2$. Тогда в соответствии с (11.9) получен шифртекст:

$$C_1 = 2G = 2 \cdot (2, 22) = (35, 1), C_2 = P + kQ = (24, 26) + 2 \cdot (13, 45) = (21, 44).$$

Таким образом, сообщению соответствует шифртекст из двух точек: $C_1 = (35, 1)$, $C_2 = (21, 44)$.

Для расшифрования сторона **B** вычисляет последовательно:

$$dC_1 = 4 \cdot (35, 1) = (23, 25),$$

далее инвертирует точку $(23, 25)$: $(23, 42)$, поскольку $-25 \bmod 67 = 42$, и, наконец, выполняется сложение в соответствии с (11.10):

$C_2 + (23, 42) = (24, 26)$, что соответствует исходной точке P , т. е. сообщению M .

Сравнительная оценка влияния размера ключа (в битах) для классической асимметричной системы шифрования (RSA) и асимметричной системы на основе ЭК дана американским институтом стандартов NIST, которую мы приводим ниже в виде табл. 11.5.

Таблица 11.5

**Размер ключей, обеспечивающих
примерно одинаковый уровень криптостойкости**

Классический RSA	На основе ЭК
102	160
2048	224
3072	256
3680	384

11.1.2.3. Реализация ЭЦП на основе ЭК

Рассмотрим генерацию и верификацию ЭЦП на основе алгоритма DSA и ЭК (ЕК) – ECDSA. Обращаем внимание на то, что используется ключевая информация отправителя (стороны **A**). Генерация ключей происходит так же, как и в последнем примере. Однако в анализируемом здесь случае во внимание должен приниматься еще один известный параметр ЭК: порядок точки G , т. е. число q .

Краткая характеристика алгоритма генерации и верификации ЭЦП состоит в следующем. Полагаем, что отправитель подписывает хеш $H(M)$ сообщения M .

Генерация ЭЦП.

1. Выбрать число k ($1 < k < q$), q – порядок точки G .
2. Вычислить точку $kG = (x, y)$, вычислить $r \equiv x \bmod q$; при $r = 0$ изменить k и повторить шаг 2.
3. Вычислить $t \equiv k^{-1} \bmod q$ (например, на основе расширенного алгоритма Евклида).
4. Вычислить $s = (t (H(M) + dr)) \bmod q$; при $s = 0$ изменить k и повторить алгоритм.

Стороне **B** отсылаются сообщение M и ЭЦП (числа r и s).

Верификация ЭЦП. Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над M и полученной ЭЦП (обозначения чисел оставим без изменений).

1. Проверить выполнение условия: $1 < r, s < q$; если условие не выполняется, то легитимность подписи не подтверждается, в противном случае – выполняются дальнейшие шаги.

2. Вычисляются $H(M)$ и $w \equiv s^{-1} \pmod{q}$.

3. Вычисляются $u_1 \equiv w H(M) \pmod{q}$, $u_2 \equiv wr \pmod{q}$.

4. Вычисляются $Gu_1 + Qu_2 = (x', y')$, $v \equiv x' \pmod{q}$.

5. Сравниваются v и r ; если равенство выполняется, подтверждается легитимность подписи и целостность полученного сообщения.

Пример 8. Полагаем, что $H(M) = 12$. Используется ЭК $E_{751}(-1, 1)$ с генерирующей точкой $G = (384, 475)$, $q = 13$ и тайным ключом $d = 12$; $Q = dG = 12(384, 475) = (384, 276)$.

Генерация ЭЦП.

1. Выбирается число $k = 3$ ($1 < 3 < 13$), q – порядок точки G .

2. Вычисляется точка $kG = 3(384, 475) = (596, 318)$, т. е. $x = 596$, вычисляется $r = x \pmod{q} = 596 \pmod{13} = 11$.

3. Вычисляется $t = k^{-1} \pmod{q} = 3^{-1} \pmod{13} = 9$, $((9 \cdot 3) \pmod{13} = 1)$.

4. Вычисляется $s = (t(H(M) + dr)) \pmod{q} = (9 \cdot (12 + 12 \cdot 11)) \pmod{13} = 9$.

Стороне **В** отсылается сообщение M и ЭЦП (числа $r = 11$ и $s = 9$).

Верификация ЭЦП. Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над M и полученной ЭЦП (числа $r = 11$ и $s = 9$).

1. Подтверждается выполнение условия $1 < r, s < q$.

2. Вычисляется $H(M)$ – положим, что в результате хеширования полученного сообщения M его хеш не изменился: $H(M) = 12$; далее вычисляется $w = s^{-1} \pmod{q} = 9^{-1} \pmod{13} = 3$.

3. Вычисляются $u_1 = w H(M) \pmod{q} = 3 \cdot 12 \pmod{13} = 10$ и $u_2 = wr \pmod{q} = 3 \cdot 11 \pmod{13} = 7$.

4. Вычисляются $Gu_1 + Qu_2 = 10(384, 475) + 7(384, 276) = (596, 318) = (x', y')$; $v = x' \pmod{q} = 596 \pmod{13} = 11$.

5. Сравниваются $v = 11$ и $r = 11$: равенство выполняется – подтверждается легитимность подписи и целостность полученного сообщения M .

11.2. Практическое задание

В основе задания – ЭК вида $y^2 = x^3 - x + 1 \pmod{751}$: $a = -1$, $b = 1$, $p = 751$, т. е. $E_{751}(-1, 1)$.

Задание 1 (рассчитано на 2 часа аудиторных занятий).

1.1. Найти точки ЭК для значений x , указанных в табл. 11.6

Таблица 11.6

Диапазоны изменения координаты x для поиска точек ЭК

Параметр	Вариант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_{\min}	0	36	71	106	141	176	201	481	516	551	586	621	656	691	716
x_{\max}	35	70	105	140	175	200	235	515	550	585	620	655	690	715	750

1.2. Разработать приложение для выполнения операций над точками кривой:

а) kP ; б) $P + Q$; в) $kP + lQ - R$; г) $P - Q + R$.

Варианты коэффициентов приведены в табл. 11.7.

Таблица 11.7

Числовые значения коэффициентов для операций над точками

Параметр	Вариант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k	8	6	7	9	11	9	11	12	8	11	7	6	9	10	11
l	11	10	8	7	5	7	4	5	5	3	7	7	5	3	5

В табл. 11.6 указаны координаты точек, над которыми выполняются операции.

Результаты выполнения операций представить в табличной форме.

Задание 2 (рассчитано на 2 часа аудиторных занятий).

2.1. Создать оконное приложение для зашифрования/расшифрования собственной фамилии (или имени – по выбору) на основе ЭК, указанной в задании 1, для генерирующей точки $G = (0, 1)$. Тайный ключ – в соответствии с вариантом из табл. 11.8.

2.2. Вычислить самостоятельно значение открытого ключа Q . При этом следует воспользоваться основной формулой (11.9), а также соотношениями (11.3)–(11.5) для случая $P = Q$; не следует также забывать, что все вычисления производятся по $\text{mod } 751$; см. также пример 5 (вычисление $2P$) и пример 7.

Принять, что шифруемым блоком является один символ сообщения, координаты которого на ЭК соответствуют табл. 11.9 (может быть принята за основу и иная таблица).

Параметры k – по собственному усмотрению.

Таблица 11.8

Координаты точек ЭК

Вариант	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)	(56, 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)

Таблица 11.9

Варианты численных значений тайного ключа

Параметр	Вариант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
d	41	27	25	12	29	44	32	34	16	18	19	51	20	43	50

Задание 3 (рассчитано на 2 часа аудиторных занятий).

3.1. Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ECDSA: ЭК $E_{751}(-1, 1)$ с генерирующей точкой $G = (416, 55)$; порядок точки $q = 13$. Дополнительные параметры – в соответствии с вариантом из табл. 11.8 и 11.10.

3.2. Вычислить самостоятельно значение открытого ключа Q . При этом следует воспользоваться основной формулой (11.8), а также соотношениями (11.3)–(11.5) для случая $P = Q$; не следует также забывать, что все вычисления производятся по $\text{mod } 751$; см. также пример 5 (вычисление $2P$) и пример 7.

Параметры k – по собственному усмотрению.

3.3. Хешем подписываемого сообщения ($H(M)$) является модуль по основанию 13 координаты x точки ЭК, соответствующей первому символу собственной фамилии из табл. 11.10. Например, фамилия начинается на букву «Я»: $x = 227$, тогда $227 \bmod 13 = 6$, значит, в данном конкретном случае $H(M) = 6$.

Таблица 11.10

Координаты точек ЭК, соответствующие символам алфавита

А	(189, 297)	Р	(206, 106)
Б	(189, 454)	С	(206, 645)
В	(192, 32)	Т	(209, 82)
Г	(192, 719)	У	(209, 669)
Д	(194, 205)	Ф	(210, 31)
Е	(194, 546)	Х	(210, 720)
Ж	(197, 145)	Ц	(215, 247)
З	(197, 606)	Ч	(215, 504)
И	(198, 224)	Ш	(218, 150)
Й	(198, 527)	Щ	(218, 601)
К	(200, 30)	Ъ	(221, 138)
Л	(200, 721)	Ы	(221, 613)
М	(203, 324)	Ь	(226, 9)
Н	(203, 427)	Э	(226, 742)
О	(205, 372)	Ю	(227, 299)
П	(205, 379)	Я	(227, 452)

Таблица 11.11

Варианты численных значений тайного ключа

Параметр	Вариант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
d	3	12	7	4	10	5	6	9	4	10	12	11	5	9	7

Отчет по каждой части задания выполняется отдельно по установленной форме.

Отчет содержит краткие теоретические сведения, описание разработанного приложения, результаты использования приложения в соответствии с целью работы, анализ результатов.

ВОПРОСЫ ДЛЯ КОНТРОЛЯ И САМОКОНТРОЛЯ ЗНАНИЙ

1. Дать определение эллиптической кривой.
2. Записать уравнение ЭК над вещественными числами (ЭК в криптографии, ЕСС).
3. Объяснить и показать на примере правила выполнения основных операций над точками ЭК.
4. Что такое «рациональная точка»?

5. Как производится умножение точки ЭК?
6. Как производится умножение точки P на число k , если k принимает значение: 2, 5, 11, 20, 32, 100, 256, 751, 1024?
7. Составить алгоритм многократного сложения точки ЭК (умножения точки на число) на основе примера 7.
8. Привести расчеты для точки Q при известных d и G из примера 7.
9. Есть ли отличия в применении операций над точками ЭК над конечными полями и над действительными числами?
10. Записать уравнение ЭК при формальном ее представлении в следующем виде: $E_p(a, b)$.
11. Из какого числа точек состоит ЭК $E_{11}(6, -9)$? Дать их координаты.
12. Найти все точки ЭК $E_{11}(1, 2)$.
13. На чем основана криптостойкость систем на основе ЭК? Области применения ЭК в криптографии.
14. Что такое «порядок точки» ЭК? Показать на примере. Какую роль этот параметр играет в криптографии на основе ЭК?
15. Что такое «базовая точка» ЭК? Какую роль этот параметр играет в криптографии на основе ЭК?
16. Объяснить порядок формирования ключевой информации на основе ЭК.
17. Сгенерировать ключевую информацию на основе кривой $E_{11}(1, 2)$.