# ЛАБОРАТОРНАЯ РАБОТА № 11

**Исследование криптографических алгоритмов на основе эллиптических кривых**

**Цель**: изучение и приобретение практических навыков разработки и ис- пользования 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 гео- метрическому представлению операций над эллиптическими кривыми (ЭК):

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

1. Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.
2. Результаты выполнения лабораторной работы оформить в виде описа- ния разработанного приложения, методики выполнения экспериментов с ис- пользованием приложения и результатов эксперимента.

# 11.1 Теоретические сведения

## *Эллиптические кривые над действительными числами*

***и конечными полями***

* + - 1. ***ЭК над действительными числами***

Мы ранее отмечали, что криптография базируется на задачах факториза- ции, дискретного логарифмирования и операциях над точками эллиптичекой кривой (Elliptic Curve, ЕС; ЕС Cryptography, ЕСС). 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 [2]).

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

*Определение* 1. *Эллиптические кривые* – математический объект, кото- рый может быть определен над любым полем.

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

*у*2 = *х*3 + *aх* + *b* (11.1)

при этом константы (*а* и *b –* вещественные числа) должны удовлетворять условию:

4*a3+*27*b2 ≠ 0*. (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 раз- ные формы (см. также [2]).

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

*Определение* 4. *Группа* – непустое [множество](https://dic.academic.ru/dic.nsf/ruwiki/4759) с определенной на нем [би-](https://dic.academic.ru/dic.nsf/ruwiki/7186) [нарной операцией](https://dic.academic.ru/dic.nsf/ruwiki/7186), называемой сложением и удовлетворяющей нескольким [аксиомам](https://dic.academic.ru/dic.nsf/ruwiki/5015).

На основе последнего определения мы можем определить группу для

ЭК.

*Определение* 5. *Группа для ЭК* есть непустое множество, элементы кото-

рого являются точками ЭК, обладающими следующими свойствами:

* *единичный элемент* – это бесконечно удалённая точка *О*;
* *обратная величина точки R* – это точка, симметричная относительно оси Х;
* *сложение* задается следующим правилом: сумма трех ненулевых точек

*P*, *Q* и -*R*, лежащих на одной прямой, будет равна *P* + *Q* + (-*R*) = *О*.

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

* прямая, проходящая через точки *R* и –*R*, является вертикальной пря- мой, которая не пересекает ЭК ни в какой третьей точке; если *R* = (*х, – у*), то *R* + (*х,у*) = *О*. Точка (*х,у*) является отрицательным значением точ- ки *R* и обозначается –*R*. Таким образом, по определению *R + (–R) = О*;
* *P + Q = R*: пусть *P* и *Q* – две различные точки ЭК (рис. 11.1), и *Р* не равно *Q*; если проведем через *P* и *Q* прямую, то она пересечет ЭК еще только в одной точке, называемой –*R*; точка –*R* отображается относи- тельно оси Х в точку *R*, равную сумме точек *P* и *Q*: *P + Q = R*;

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



**Рисунок 11.1 Пояснение к операции сложения двух точек *P* и *Q***

**эллиптической кривой** *у*2 = *х*3 + 2*х* +1 (*а* = 2, *b* = 1)

Что будет, если *P* = *Q*? В этом случае мы можем говорить об операции *удвоения точки*: *P* + *Р* = 2*Р*. Обобщив (к точке 2*Р* можно прибавить еще раз точку *Р*: 2*Р* + *Р*), сформулируем принцип умножения точки *Р* на целое поло- жительное число *n* – определяется как сумма *n* точек *Р*: *nP* = *P + P + P + …*

*+ P*.

Скалярное умножение осуществляется посредством нескольких комби- наций сложения и удвоения точек эллиптической кривой. Например, точка 25P может быть представлена, как 25P = 2(2(2(2*P*)) + 2(2(2*P*))) + *P*.

Понятно, что каждая точка на плоскости задается парой координат: *х* и *у*.

Числа *х* и *у* являются *рациональными*, а точки *P*, *Q*, *R* и *-R* (как и любые точки ЭК) – *рациональными точками*

Если *Р =* (*х1, у1*) и *Q* = (*х2, у2*), то *Р + Q =* (*х3, у3*) определяется в соответ- ствии с правилами:

где

*x =* λ2 *– х – х* ; (11.3)

*у3=* λ (*х1–х3*) *– у1*, (11.4)

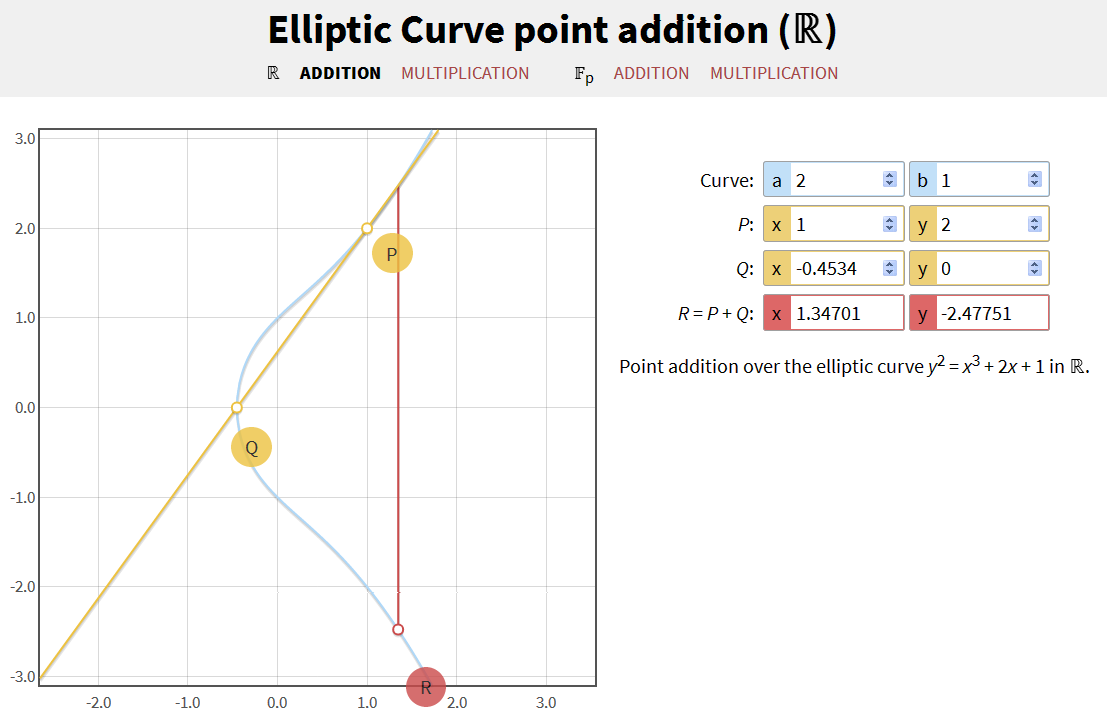
*3 1 2*

 ** ( *у2 – у1*)*/*( *х2 – х1)*, если *Р ≠ Q* и ** (*х1*)*2+а)/*2 *у1,* если *Р = Q.* (11.5) Из этого следует, что число  – угловой коэффициент секущей, прове-

денной через точки *Р =* (*х1, у1)* и *Q* = (*х2, у2*). При *Р* = *Q* секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления **

Очень хорошее представление об операциях над точками различных ЭК можно получить, воспользовавшись онлайн-приложением, доступном по ссылке: [https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-](https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html) [add.html](https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html).

Для примера на рис. 11.2 приведено окно приложения.



Источник: <https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html>

**Рисунок 11.2 Окно приложения *Elliptic Curve Points Addition***

На приведенном рисунке как раз представлен пример над точками (коор- динаты – правой части экрана) упоминавшейся выше (см. рис. 11.1) ЭК. От- метим также, что при этом выбраны опции R и **Addition** (вторая строка), со- ответствующие операции сложения над рациональными числами.

Рассмотрим пример.

*Пример* 1. Пусть ЭК задается уравнением с параметрами *а* = –7, *b* = 10.

Точки *Р* (1, 2) и Q (3, 4). Нужно вычислить сумму точек: *P + Q = R.*

Воспользуемся (11.3) – (11.5):

λ = (2 – 4)/(1 – 3) = 1,

*x*R = *x*3 = 12 – 1 – 3 = –3,

*y*R = *y*3 = 2 + 1 (– 3 – 1) = – 2.

Тот же результат получаем и при использовании указанного выше при- ложения.

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

*=* 2*Р:*

λ = 3(12 – 7)/(2 \* 2) = – 1,

*x*R = *x*3 = (–1)2 – 1 – 1 = –1,

*y*R = *y*3 = 2 + (–1) (– 1 – 1) = 4.

Таким образом, получили точку 2*Р*(–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 = n P*. Если же известны *Q* и *P*, а нам нужно определить *n*, то такая задача нам известна как

*задача логарифмирования*.

## *ЭК над конечными полями*

Именно этот тип ЭК будет нас интересовать в плане практического приме- нения.

*Определение* 6. *Конечное поле* – это множество конечного числа элемен- тов. 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 умно- жения работают как в модулярной арифметике.

Например, поле *F*13 (*р* = 13) состоит из чисел: 0, 1, … , 12.

*Определение* 7. *Эллиптическая кривая над полем F*p задается теми же урав- нениями, что и ЭК над действительными числами, только все вычисления производятся по модулю *р* (mod *p*),

нп.:

*у*2 ≡ *х*3 + *aх* + *b* (mod *p*), (11.6) далее для упрощения знак «≡» будем заменять простым неравенством:

4*a3+*27*b2 ≠ 0* (mod *p*) (11.7)

и т.д.

Формально ЭК над полем задается так: *Е*р(*а*, *b*).

Важно отметить, что, как и ранее, существует точка (бесконечно удален- ная) *О*; *а* и b – вещественные числа.

Прежде, чем приступить к алгебраическим операциям над точками кри- вой, 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 ко- торой будут рассчитываться точки кривой, и функция кривой.

Рассмотрим конкретный пример.

*Пример* 4. Пусть ЭК формально задается в записью *Е*13(6, –9). Проверяем выполнение условия (11.7). Исходя из этого, координаты расположения то- чек должны быть ограничены квадратом некоторых чисел по модулю 13 (ле- вая часть основного уравнения – *у*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**



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, рас- смотрим ситуацию для *х* = 0. Подставим это значение в правую часть уравне- ния (11.6), имея в виду ЭК *Е*13(6, –9):

*у*2 = 03 + 6\*0 – 9 (mod 13),

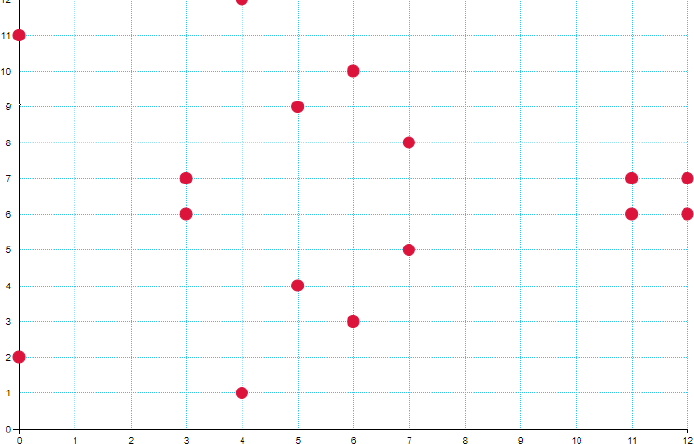
откуда получим *у*2 = – 9 (mod 13), *у*2 = 4 и *у* = ± 2. Таким образом, пользуясь данными из табл. 11 (смотрим строки с числами 4 справа от знака равенства), определяем, что точками нашей ЭК будут: (0, 2) и (0, 11); здесь мы приняли во внимание то, что значение некоторого целого отрицательного числа (–*k*) по модулю (*р*) вычисляется следующим образом:

(–*k*) mod *р* = – (*k* mod *р*) + *p*.

Следуя приведенной логике рассуждений, определим, например, точки при *х* = 3: *у*2 = 33 + 6\*3 – 9 (mod 13) = 36 (mod 13) = 10. Обращаем внимание на 7 и 8 строки левого столбца табл. 11.1 и устанавливаем координаты еще 2- х точек ЭК: (3, 6), (3, 7).

Теперь вернемся к *х* = 1: *у*2 = 13 + 6\*1 – 9 (mod 13) = –2 (mod 13) = 11. В табл. 11.1 не найдено ни одного соответствия. Это означает, что на рассмат- риваемой ЭК нет ни одной точки, координата *х* которой равна 3.

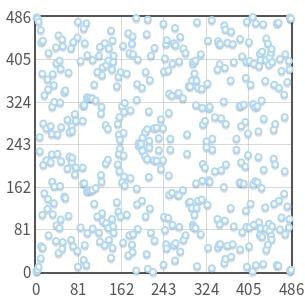
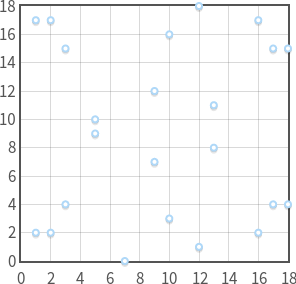
На рис. 11.3 представлены все точки для ЭК *Е*13(6, –9).



**Рисунок 11.3 Точки ЭК *Е*13(6, –9)**

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

Из приведенных примеров можно заметить, что для каждого *x* существу- ет максимум две точки. Отметим также симметрию в расположении точек относительно *y = p/2*.



Источник: https://habr.com/ru/post/335906/

а) б)

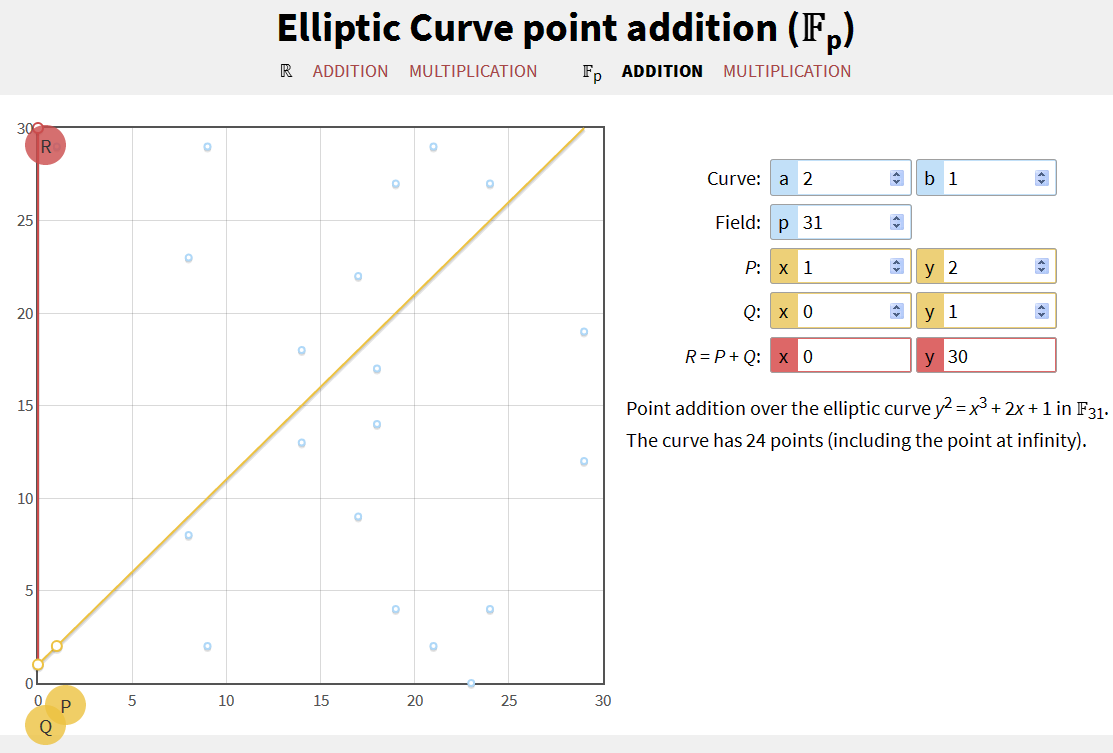
**Рисунок 11.4 Отображение точек ЭК *у*2 = *х*3 – 7*х* + *10* (mod *p*)**

То, что раньше было непрерывной кривой, теперь стало множеством от- дельных точек на плоскости XY, координаты которых (*х* и *у*) являются целы-

ми числами.

Можно также сказать, что три точки находятся на одной прямой, если существует прямая, соединяющая их.Рисунки 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 суммиро- вания двух точек с параметрами, примерно соответствующими рисунку 11.2 (не для любых параметров выполняется операция).



**Рисунок 11.5 Геометрическое отображение операции суммирования двух точек ЭК с параметрами, расположенными в правой части экрана**

Рассмотрим пример.

*Пример* 5. Пусть *р* = 23. Рассмотрим ЭК *y*2 = *x*3+ *x* + 1(mod 23): *Е*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 так- же точка *О*.

Пусть *Р* = (3,10) и *Q* = (9,7). Найдем *Р + Q* и 2*Р*. Пусть *Р + Q* = (*х*3, *у*3), тогда при

       (mod 23)   (mod 23)

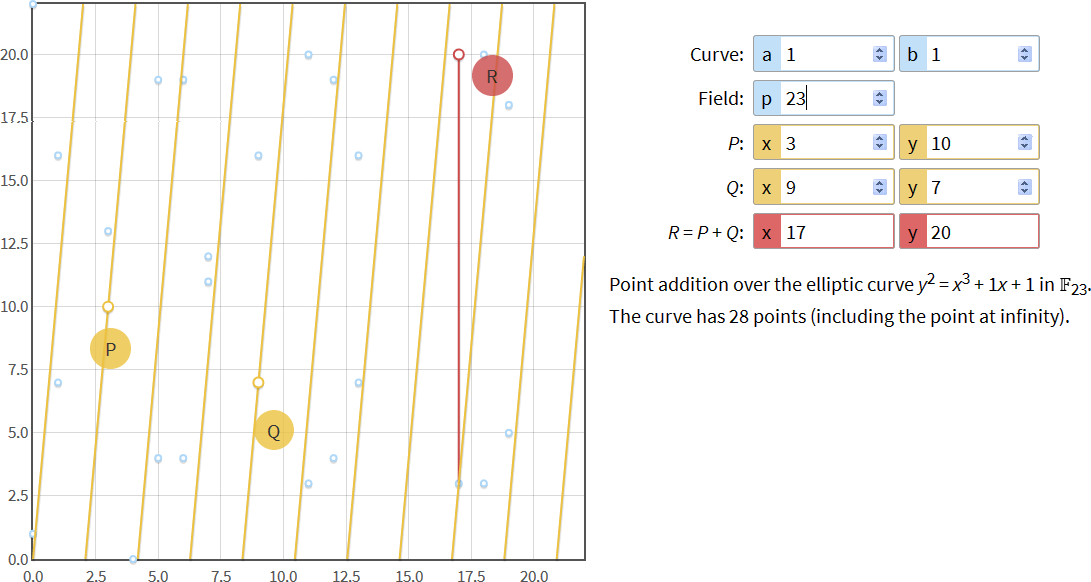
имеем:

*х*3 = 121–3–9 (mod 23) =109 (mod 23) = 17,

*у*3 = 11(3 + 6) – 10 (mod 23) = 89 (mod 23) = 20.

Таким образом, *Р + Q* = (17, 20).

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



**Рисунок 11.6 Окно приложения с результатами выполнения операции сложения двух точек из примера 2**

Найдем теперь точку 2*Р* = *Р + Р* = (*х*3, *у*3) – с формальной точки зрения это также будет третья точка.

Для этого случая

λ = (3\*9 + 1) (mod 23) = 6 (mod 23)

и с учетом последнего для вычисления координаты *у*3: *x*3 = 36 – 6 (mod 23) = 30 (mod 23) = 7 (mod 23);

*у3* = 6\*(3– 7)– 10 (mod 23) = –34 (mod 23) = 12 (mod 23).

Таким образом, 2*Р* = (7,12).

При последовательном выполнении сложения *nP* = *P + P + P + … + P* на каждом шаге будет получаться точка, которая также должна принадлежать Ep(*a*, *b*). В силу того, что эллиптическая группа содержит конечное множество точек, и наступит такой момент, что для некоторых результатов вычислений будет выполняться равенство *qР* = *О* (см. пример 5.12 из [2], где 5A= *O*, т.е. здесь *q* = 5).

*Пример* 6. Для точки *Р* = (4, 2) ЭК вида *Е*7 (4,1), например, справедливы сле- дующие соотношения:

2*Р* = (4, 2) + (4, 2) = (0, 1),

3*Р* = (0, 1) + (4, 2) = (0, 6),

4*Р* = 2(0, 1) = (4, 5),

5*Р* = (0, 1) + (0, 6) = *О* .

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 *Е*5(0,1).

**Таблица 11.2 Результаты выполнения операции Р+ …+Р для кривой *Е*5(0,1)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **+** | **(0,1)** | **(0,4)** | **(2,2)** | **(2,3)** | **(4,0)** |
| ***Р*** | (0,1) | (0,4) | (2,2) | (2,3) | (4,0) |
| ***2Р*** | (0,4) | (0,1) | (0,4) | (0.1) | *О* |
| ***3Р*** | *О* | *О* | (4.0) | (4.0) | (4,0) |
| ***4Р*** | (0,1) | (0,4) | (0.1) | (0,4) | *О* |
| ***5Р*** | (0,4) | (0,1) | (2.3) | (2.2) | (0.4) |
| ***6Р*** | *О* | *О* | *О* | *О* | *О* |

Данные приведенной таблицы подтверждают наши выводы.

Если требует, например, точку *Р* сложить саму с собой *z* раз, то это означа- ет, что нужно выполнить вычисление z*Р*. Для реализации этой операции суще- ствует простой метод на основе операции сложения точек. Число *z* представля- ется в двоичном виде. И далее вычисляются необходимые составляющие общей суммы на основе весовых (единичных) разрядов двоичного числа *z.* Рассмотрим это на примере.

*Пример* 7. Пусть *z* = 171. Это число в двоичном виде выглядит так: 10101011. В соответствии с весом «1» мы должны сложить следующие состав- ляющие (слагаемые) общей суммы: 171*P* = *Р* + 2*Р* + 8*Р* + 32*Р* + 128*Р*.

Первое из приведенных слагаемых известно. Второе слагаемое: 2*Р* = *Р* + *Р*, промежуточное вычисление: 4*Р* = 2*Р* + 2Р, третье слагаемое: 8*Р* = 4*Р* + 4*Р*, про- межуточное вычисление: 16*Р* = 8*Р* + 8*Р*, промежуточное вычисление: 16*Р* = 8*Р*

+ 8*Р*, четвертое слагаемое: 32*Р* = 16*Р* + 16*Р*, промежуточное вычисление: 64*Р* = 32*Р* + 32*Р*, последнее слагаемое: 128*Р* = 64*Р* + 64*Р*.

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

*Определение* 9. Наименьшее значение числа *q*, для которого выполняется равенство *qР* = *О*, называется *порядком точки Р*.

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

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

Порядок точки *Р* 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 Ер(*а*, *b*) порядок *m* группы точек должен удовлетворять неравен- ству:

*p* + 1 – 2(*p*)½ ≤ *m* ≤ *p* + 1 + 2(*p*)½ .

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 дис- кретного логарифмирования* для эллиптических кривых.

Эта задача аналогична задаче дискретного логарифмирования, использу- емой в других криптосистемах, таких как алгоритм DSA, протокол Диффи- Хеллмана и схема Эль-Гамаля.

В криптографии на основе ЭК тайный ключ – это случайное целое *d* , выбранное из множества {1, 2, ..., *q*–1}, где *q* – порядок подгруппы; *откры- тый 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 РБ [50] параметром *l*, называемым *уровнем стойкости* и принимающим значения (рекомендуется) из {128, 192, 256}. При этом для взлома ключа злоумышленнику нужно выполнить 2*l* операций*.*

## *Основные этапы генерации ключевой информации* на основе ЭК

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

* 1. Входными параметрами являются: число *l*, число *р*, удовлетворяю- щее условию 22*l-*1 < *р* < 22*l*, *р* = 3 mod 4, 0 < *a* < *p*. Можно использовать неко- торое простое число *р* = 22*l* – *с*, где с – небольшое натуральное число.
  2. Выбирается число *b*, такое, что 0 < *b* < *p*. Таким образом, задана ЭК: *Е*р(*а*, *b*).
  3. Выбираются порядок *q* (простое число) и генерирующая точка *G*, ко- торая задается двумя координатами, например, *G =* (0, *у*G).

Дополнительно к рассмотренным действиям стандарт [50] предусматри- вает использование вспомогательного параметра (*s*, *seed*) – произвольное 64- битное число.

Для примера в нижеследующей иллюстрации (рис. 11.7) [50] приведены параметры ЭК для двух значений *l*.(на иллюстрации это – Таблица Б.1 и Таб- лица Б.2). Здесь нижние индексе в левом столбце обозначают битовую длину чмсла.

Второй этап. *Генерация ключевой информации*.

* 1. Входными параметрами являются: *р*, *а*, *b*, *q* и *G*.
  2. Генерируется тайный ключ – число *d*, выбранное из множества {1, 2,

…, *q*–1}.

* 1. Вычисляется открытый ключ – точка *Q:*

*Q* = *dG*, (11.8)

к открытому ключу также относятся *р*, *а*, *b*, *q*.

Отметим также, что сгенерировать ключевую информацию на основе ЭК

можно воспользовавшись известной нам библиотекой *OpenSSL*. Например, если воспользоваться версией *OpenSSL* 1.1.1*L* в системе *Debian* 9 (с помощью команды с двумя разными псевдонимами (выделены жирным):

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

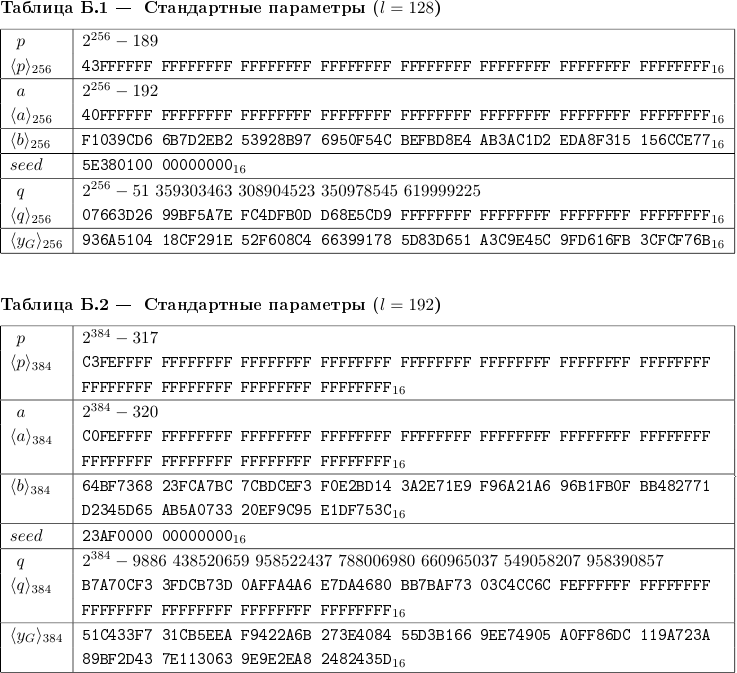
*openssl ecparam –name secp521r1 –genkey –out* ***secp521r1***,

то получим тайные ключи соответственно следующего содержания:

MFwCAQEEGLDsGwgZq/Kq4suR74ftkipbKMRmoWDtlqAHBgUrgQQAH6E0AzIABPfKAz FU+QKsh+I7a6K5taNUe3TZAdLMp92RpYoT0PIrmGD3QVRcqAmqZSba6kanKg==

MIHcAgEBBEIAvv7P//lWx3QQis5Hb25eN/UY5isVJk+s56ZDSTleUcrqj2mNH4Y3 xWLXGMtpmDJRiHalCv3MDt/T5h67daHaViagBwYFK4EEACOhgYkDgYYABABgOPla 5ygHB/j79g0R2N12/tv4YlIj6ZA+t2FhtvEMPvj9QHMg5sN45yjGKmLlIwEMP2YW xjPj3YL0Z0uLO9BBYwBUGVCPEWKylC8x5qGL1ypG6shCPTUcXQxLuFMmKv+AaDH2

4TCdBvl9nYANhlxZKv96Pb/lari3OKZkmO5zgVWKCw==



**Рисунок 11.7 Стандартные параметры ЭК**

Полезные рекомендации по выбору параметров ЭК можно найти, например, в [51].

## *Использование ЭК в криптографии*

Отметим еще раз, что ЭК в криптографических приложениях обычно ис- пользуется на этапе генерации либо согласования ключевой информации. Таким образом, можно отметить 3 направления использования ЭК в крипто- графии:

* в алгоритмах согласования (передача) ключевой информации (на осно- ве идеи Диффи-Хеллмана),
* в алгоритмах асимметричного шифрования/дешифрования сообщений,
* в алгоритмах генерации/верификации ЭЦП.

## *Реализация алгоритма Диффи-Хеллмана на основе ЭК*

Рассмотрим наиболее общий случай. Предположим, что *E*р – это ЭК над

*F*р, а *Q* – заранее определенная и согласованная сторонами **А** и **В** точка на *E*. Отправитель **A** выбирает тайное случайное число *k*A, вычисляет точку *Р*А

= *k*A\*Q и отправляет ее получателю **B**. **B** действует аналогично: он случай- ным образом выбирает число *k*B, вычисляет случайное число *k*A, вычисляет точку *Р*В = *k*В\*Q и отправляет результат стороне **A**.

Общий ключ *P* = *k*A\**k*B\**Q*. Отправитель **A** вычисляет *P* путем умножения числа *Р*В, полученного от получателя **B**, на его секретное число *k*A. Похожим образом действует другая строна.

## *Реализация алгоритма зашифрования/расшифрования* на основе ЭК

Вспомним, что процедура предусматривает использование ключей полу- чателя (стороны **В**). Рассмотрим это на примере алгоритма Эль-Гамаля.

Вспомним, что зашифрованное сообщение *М* или каждый зашифрован- ный блок (*m*i) этого сообщения состоят из двух чисел. Вспомним лаборатор- ную работу № 8, где блок шифртекста (*c*i) в соответствии с (8.9) и (8.10) мы обозначали двумя символами *а*i и *b*i и вычисляли как

*а*i = *g*k mod *p*, *b*i = (*y*k•*m*i) mod *p*.

Поскольку символы *а* и *b* мы зарезервировали в текущей работе для обо- значения параметров ЭК, то блок шифртекста сейчас будем обозначать соот- ветственно символами *С*i1 и *C*i2.

При использовании ЭК зашифрование предполагает представление сооб- щения в виде точки *Р* (или представления каждого блока сообщения в виде разных точек *Рi*) ЭК с известной точкой *G* и известным *Q*. Соответственно шифртекст – это две точки на той же ЭК: *С*1 и *C*2 или *С*i1 и *C*i2.

Предположим, что шифруемое сообщение *М* – это точка *Р* на ЭК. Сторона **А** выбирает некоторое случайное число *k* и далее выполняет вы-

числения с использованием открытого ключа стороны **В**:

*С*1 = *kG*, *С*2 = *P* + *kQ*. (11.9)

Получатель для расшифрования сообщения вычисляет:

*P* = *С*2 – *dC*1. (11.10)

Знак «–» в (11.10) означает сложение с инверсией: инверсией по отно- шению к точке (*х*, *у*) является точка (*х*, –*у*) на ЭК.

Рассмотрим пример.

*Пример* 8. Пусть сторона **В** использует ЭК вида *Е*67(2, 3), *G* = (2, 22) и *d*

= 4. Тогда *Q* = *dG* = 4*G =* (13, 45); здесь расчеты, которые проводились на ос- нове (11.3)–(11.5), опускаются.

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

*С*1 = *2G* = 2\*(2, 22) = (35, 1), *С*2 = *P* + *kQ* = (24, 26) + 2\*(13, 45) = (21, 44).

Таким образом, сообщению соответствует шифртекст из двух точек: *С*1 = (35, 1), *С*2 = (21,44).

Для расшифрования сторона **В** вычисляет последовательно:

*dC*1 = 4\*(35, 1) = (23, 25),

далее инвертирует точку (23, 25): (23, 42), поскольку –25 mod 67 = 42, и,

наконец, выполняется сложение в соответствии с (11.10): *С*2 + (23, 42) = (24, 26), что соответствует исходной точке *Р*, т.е. сообщению *М*.

Сравнительная оценка влияния размера ключа (в битах) для классиче- ской асимметричной системы шифрования (RSA) и асимметричной системы на основе ЭК дана американским институтом стандартов NIST, которую мы приводим ниже в виде табл. 11.3.

**Таблица 11.3 Размер ключей, обеспечивающих примерно одинаковый уровень крип- тостойкости**

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

## *Реализация ЭЦП на основе ЭК*

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

Краткая характеристика алгоритма генерации и верификации ЭЦП. По-

лагаем, что отправитель подписывает хеш *Н*(*М*) сообщения *М*. Генерация ЭЦП.

1. Выбрать число *k* (1 < *k* < *q*), *q* – порядок точки *G*.
2. Вычислить точку *kG* = (*х*, *у*), вычислить *r* = *x* mod *q*; при *r* = 0 изменить

*k* и повторить шаг 2.

1. Вычислить *t* = *k*-1mod *q* (например, на основе расширенного алгоритма Евклида).
2. Вычислить *s* = (*t* (*H*(*M*) + *dr*)) mod *q*; при *s* = 0 изменить *k* и повторить алгоритм.

Стороне **В** отсылаются сообщение *М* и ЭЦП (числа *r* и *s*). Верификация ЭЦП.

Получатель знает алгоритм хеширования, который использовался отпра- вителем, открытый ключ отправителя, с помощью чего выполняет следую- щие операции над *М* и полученной ЭЦП (обозначения чисел оставим без из- менений).

1. Проверить выполнение условия: 1 < *r*, *s* < *q*; если условие не выполня- ется, то легитимность подписи не подтверждается, в противном случае – вы- полняются дальнейшие шаги.
2. Вычисляются *Н*(*М*) и *w* = *s*–1 mod *q*.
3. Вычисляются *u*1 = *w Н*(*М*) (mod *q*), *u*2 = *wr* (mod *q*).
4. Вычисляются *Gu*1 + *Qu*2 = (*x'*, *y'*), *v* = *x'* mod *q*.
5. Сравниваются *v* и *r*; если равенство выполняется, подтверждается ле- гитимность подписи и целостность полученного сообщения.

*Пример* 9. Полагаем, что *Н*(*М*) = 12. Используется ЭК *Е*751(–1, 1) с гене- рирующей 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. *х* = 596, вычис- ляется *r* = *x* mod *q* = 596 mod 13 = 11.

3. Вычисляется *t* = *k*-1mod *q* = 3–1 mod 13 = 9, ((9\*3) mod 13 = 1).

4. Вычисляется *s* = (*t* (*H*(*M*) + *dr*)) mod *q* = (9 \* (12 + 12\*11) mod 13 = 9. Стороне **В** отсылаются сообщение *М* и ЭЦП (числа *r* = 11 и *s* = 9).

Верификация ЭЦП.

Получатель знает алгоритм хеширования, который использовался отпра- вителем, открытый ключ отправителя, с помощью чего выполняет следую- щие операции над *М* и полученной ЭЦП (числа *r* = 11 и *s* = 9).

1. Подтверждается выполнение условия 1 < *r*, *s* < *q*.
2. Вычисляется *Н*(*М*) – положим, что в результате хеширования полу- ченного сообщения М его хеш не изменился: *Н*(*М*) = 12; далее вычисляется *w* = *s*–1 mod *q* = 9–1 mod 13 = 3.
3. Вычисляются *u*1 = *w Н*(*М*) (mod *q*) = 3\*12 (mod 13) = 10 и *u*2 = *wr* (mod

*q*) = 3\*11 (mod 13) = 7.

4. Вычисляются *Gu*1 + *Qu*2 = 10(384, 475) + 7(384, 276) = (596, 318) = (*x'*,

*y'*); *v* = *x'* mod *q* = 596 mod 13 = 11.

5. Сравниваются *v* = 11 и *r* = 11: равенство выполняется – подтверждает- ся легитимность подписи и целостность полученного сообщения *М*.

# 11.2 Практическое задание

В основе задания – ЭК вида *у*2 = *х*3 – х + 1 (mod 751): *а* = –1, *b* = 1, р = 751, т. е. *Е*751(–1, 1).

Задание **I** (рассчитано на 2 часа аудиторных занятий).

1.1 Найти точки ЭК для значений *х*, указанных в табл. 11.4

**Таблица 11.4 Диапазоны изменения координаты х для поиска точек ЭК**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вар-т  Парам. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| *х*мин | 0 | 36 | 71 | 106 | 141 | 176 | 201 | 481 | 516 | 551 | 586 | 621 | 656 | 691 | 716 |
| *х*макс | 35 | 70 | 105 | 140 | 175 | 200 | 235 | 515 | 550 | 585 | 620 | 655 | 690 | 715 | 750 |

1.2. Разработать приложение для выполнения операций над точками кри-

вой:

*а) kР,* б) *Р + Q*, в) *kР* + *lQ – R*, г) Р – *Q* + *R*.

Варианты коэффициентов приведены в табл. 11.5.

В табл. 11.6 указаны координаты точек, над которыми выполняются опе- рации.

Результаты выполнения операций представить в табличной форме.

**Таблица 11.5 Числовые значения коэффициентов для операций над точками**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вар-т  Парам. | 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 |

Задание **II** (рассчитано на 2 часа аудиторных занятий).

* 1. Создать оконное приложение для зашифрования/расшифрования собственной фамилии (или имени – по выбору) на основе ЭК, указанной в задании **I**, для генерирующей точки *G* = (0, 1). Тайный ключ – в соответствии с вариантом из табл. 11.7.
  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 mod 751; см. также пример 5 (вычисление 2*Р*) и пример 7.

Принять, что шифруемым блоком является один символ сообщения, ко- ординаты которого на ЭК соответствуют табл. 11.8 (может быть принята за основу и иная таблица).

Параметры *k* – по собственному усмотрению.

**Таблица 11.6 Координаты точек ЭК**



**Таблица 11.7 Варианты численных значений тайного ключа**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вар-т  Парам. | 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 **III** (рассчитано на 2 часа аудиторных занятий).

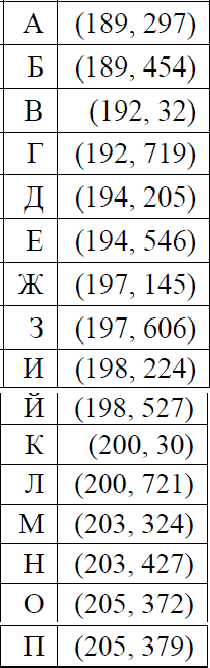
* 1. Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA: ЭК *Е*751(–1, 1) c генерирующей точкой *G* = (416, 55); порядок точки *q* = 13. Тайный ключ – в соответствии с вариантом из табл. 11.7. Тайный ключ – в соответствии с табл. 11.9.
  2. Вычислить самостоятельно значение 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 mod 751; см. также пример 5 (вычисление 2*Р*) и пример 7.

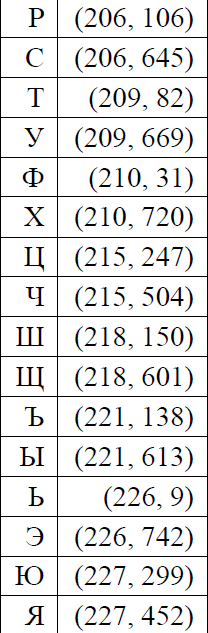
Параметры *k* – по собственному усмотрению.

* 1. Хешем подписываемого сообщения, (*Н*(*М*)), является модуль по ос- нованию 13 координаты *х* точки ЭК, соответствующей первому символу соб- ственной фамилии, из табл. 11.8. Например, фамилия начинается на букву

«Я»: *х* = 227, тогда 227 mod 13 = 6, значит в данном конкретном случае *Н*(*М*)

= 6.

**Таблица 11.8 Координаты точек ЭК, соответствующие символам алфавита**



**Таблица 11.9 Варианты численных значений тайного ключа**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вар-т  Парам. | 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 разработан- ного 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 крипто- графии, ЕСС).
3. Объяснить и показать на примере правила выполнения основных опе- раций над точками ЭК.
4. Что такое «рациональная точка»?
5. Как производится умножение точки ЭК?
6. Как производится умножение точки *Р* 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.

1. Привести расчеты для точки Q при известных d и G из примера 7.
2. Есть ли отличия в применении операций над точками ЭК над конеч- ными полями и над действительными числами?
3. Записать уравнение ЭК при формальном ее представлении в следую- щем виде: Ер(а, b).
4. Из какого числа точек состоит ЭК Е11(6, –9)? Дать их координаты.
5. Найти все точки ЭК Е11 (1, 2).
6. На чем основа криптостойкость систем на основе ЭК? Области при- менения ЭК в криптографии.
7. Что такое «порядок точки» ЭК? Показать на примере. Какую роль этот параметр играет в криптографии на основе ЭК?
8. Что такое «базовая точка» ЭК? Какую роль этот параметр играет в криптографии на основе ЭК?
9. Объяснить порядок формирования ключевой информации на основе

ЭК.

1. Сгенерировать ключевую информацию на основе кривой *Е*11 (1, 2).

К списку литературы

51. Standards for Efficient Cryptography. SEC 2: Recommended Elliptic Curve Domain Parameters [Электронный ресурс] [https://www.secg.org/SEC2-Ver- 1.0.pdf](https://www.secg.org/SEC2-Ver-1.0.pdf)