Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Исследование криптографических алгоритмов на основе эллиптических кривых»

Выполнила:

студентки 3 курса 5 группы

специальности ПОИТ

Кубик Е.В.

Минск 2021

1. **Теоретические сведения**

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 = х^3 + aх + b, (1.1)

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

4a^3 + 27b^2 ≠ 0. (1.2)

Нетрудно понять, что вид ЭК (1.1) также задается парой чисел: a и b.

Формула (1.1) называется уравнением Вейерштрасса, а условие (1.2) исключает из рассмотрения кривые с особыми точками или особые кривые.

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

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 - непустое множество, элементы которого 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 прямой, которая не пересекает ЭК ни в какой третьей точке; если R = (х, – у), то R + (х, у) = О. Точка (х, у) является отрицательным значением точки R и обозначается –R. Таким образом, по определению R + (–R) = О;
* P + Q = R: пусть P и Q – две различные точки ЭК 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 относительно оси Х в точку R, равную сумме точек P и Q: P + Q = R;

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

x3= λ^2 – х1 – х2; (1.3)

у3= λ(х1 – х3) – у1, (1.4)

где

λ = (у2 – у1)/(х2 – х1), если Р ≠ Q и λ= (3(х1)^2+а)/2у1, если Р = Q. (1.5)

Из этого следует, что число λ – угловой коэффициент секущей, проведенной через точки Р = (х1, у1) и Q = (х2, у2). При Р = Q секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления λ.

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.

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 Fp. Здесь операции сложения и умножения работают как в модулярной арифметике.

Например, поле F13 (р = 13) состоит из чисел: 0, 1, …, 12.

Определение 7. Эллиптическая кривая над полем Fp задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю р (mod p), нп.:

y^2 ≡ х^3 + aх + b (mod p), (1.6)

далее для упрощения знак «≡» будем заменять простым неравенством:

4a^3+27b^2 ≠ 0 (mod p) (1.7)

и т.д.

Формально ЭК над полем задается так: Ер(а, b).

Важно отметить, что, как и ранее, существует точка (бесконечно удаленная) О; а 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.

Пусть ЭК формально задается записью Е13(6, –9). Проверяем выполнение условия (1.7). Исходя из этого, координаты расположения точек должны быть ограничены квадратом некоторых чисел по модулю 13 (левая часть основного уравнения – у^2). Здесь стоит отметить известную нам цикличность в вычислениях на основе модулярной арифметики.

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. Рассмотрим ситуацию для х = 0. Подставим это значение в правую часть уравнения (1.6), имея в виду ЭК Е13(6, –9):

y^2 = 0 3 + 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.

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 (х и у) являются целыми числами.

Можно также сказать, что три точки находятся на одной прямой, если существует прямая, соединяющая их.

Если требует, например, точку Р сложить саму с собой z раз, то это означает, что нужно выполнить вычисление zР. 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.

Определение 8. Если мы складываем два значения, кратных Р, то получаем 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 неравенству:

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 дискретного логарифмирования для эллиптических кривых

Эта задача аналогична задаче дискретного логарифмирования, используемой в других криптосистемах, таких как алгоритм DSA, протокол ДиффиХеллмана 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; 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 РБ параметром l, называемым уровнем стойкости и принимающим значения (рекомендуется) из {128, 192, 256}. При этом для взлома ключа злоумышленнику нужно выполнить 2l 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, удовлетворяющее условию 2^(2l-1) < р < 2^(2l), р = 3 mod 4, 0 < a < p. Можно использовать некоторое простое число р = 22l – с, где с – небольшое натуральное число.
  2. Выбирается число b, такое, что 0 < b < p. Таким образом, задана ЭК: Ер(а, b).
  3. Выбираются порядок q (простое число) и генерирующая точка G, которая задается двумя координатами, например, G = (0, уG).

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

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}.
  3. Вычисляется открытый ключ – точка Q:

Q = dG, (1.8)

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

**Использование ЭК в криптографии**

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 (передача) ключевой информации (на основе 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 Eр – это ЭК над Fр, а Q – заранее определенная и согласованная сторонами А и В точка на E.

Отправитель A выбирает тайное случайное число Ka, вычисляет точку Рa = Ka\*Q и отправляет ее получателю B. B действует аналогично: он случайным образом выбирает число Kb, вычисляет случайное число Ka, вычисляет точку Рb = Kb \*Q и отправляет результат стороне A.

Общий ключ **P = Ka\*Kb\*Q.** Отправитель A вычисляет P путем умножения числа Рb, полученного от получателя B, на его секретное число Ka. Похожим образом действует другая сторона.

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

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

Вспомним, что зашифрованное сообщение М или каждый зашифрованный блок (mi) этого сообщения состоят из двух чисел. Вспомним лабораторную работу № 8, где блок шифртекста (ci) в соответствии с (8.9) и (8.10) мы обозначали двумя символами аi и bi и вычисляли как

аi = g^k mod p, bi = (y^k\*mi) mod p.

Поскольку символы а и b мы зарезервировали в текущей работе для обозначения параметров ЭК, то блок шифртекста сейчас будем обозначать соответственно символами Сi1 и Ci2.

При использовании ЭК зашифрование предполагает представление сообщения в виде точки Р (или представления каждого блока сообщения в виде разных точек Рi) ЭК с известной точкой G и известным Q. Соответственно шифротекст – это две точки на той же ЭК: С1 и C2 или Сi1 и Ci2.

Предположим, что шифруемое сообщение М – это точка Р на ЭК.

Сторона А выбирает некоторое случайное число k и далее выполняет вычисления с использованием открытого ключа стороны В:

С1 = kG, С2 = P + kQ. (1.9)

Получатель для расшифрования сообщения вычисляет:

P = С2 – dC1. (1.10)

Знак «–» в (1.10) означает сложение с инверсией: инверсией по отношению к точке (х, у) является точка (х, –у) на ЭК.

**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 внимание должен приниматься еще один известный параметр ЭК: порядок точки G, т. е. число q.

Краткая характеристика алгоритма генерации и верификации ЭЦП. Полагаем, 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.
  3. Вычислить t = k^-1mod q (например, на основе расширенного алгоритма Евклида).
  4. 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 отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над М 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 Н(М) и w = s^-1 mod q.
  3. Вычисляются u1 = w Н(М) (mod q), u2 = wr (mod q).
  4. Вычисляются Gu1 + Qu2 = (x', y'), **v = x' mod q**.
  5. Сравниваются v и r; если равенство выполняется, подтверждается легитимность подписи и целостность полученного сообщения.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать пользовательское приложение, которое должно реализовывать следующие операции:

1. Найти точки эллиптической кривой для значений х, указанных в таблице согласно варианту.
2. Разработать приложение для выполнения операций над точками кривой:

* k\*P;
* P+Q;
* k\*P+l\*Q-R;
* P-Q;

Для выполнения первого задания было разработано приложение, которое согласно введенным коэффициентам A и B, а также ограничивающему коэффициенту Field рисует график функции по формуле 1.6.

При вводе x координат точек P и Q рассчитываются их y координаты согласно графику, а при заполнении всех полей этих двух точек по формулам 1.3 – 1.5 рассчитываются координаты точки R. Соответствующие точки проставляются на графике.

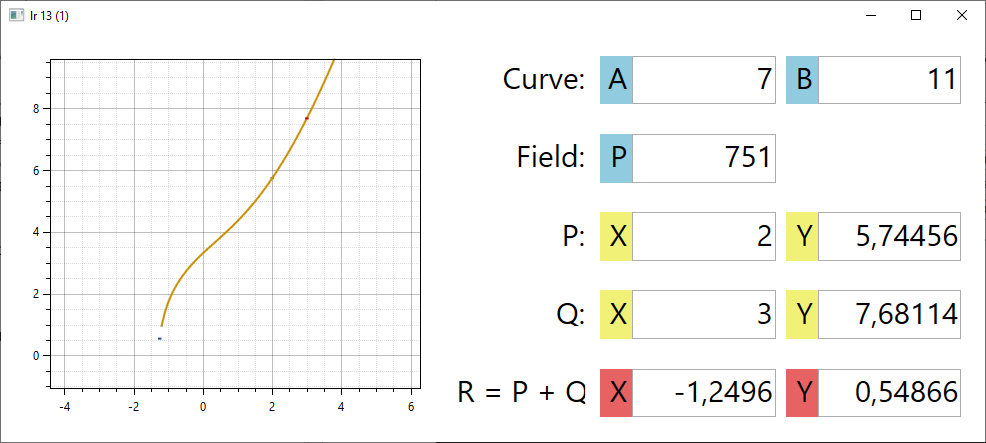


Рисунок 13.1 – Расчет координат точки R (приложение)

Проверим работоспособность приложения, используя источник, данный в лабораторной работе:

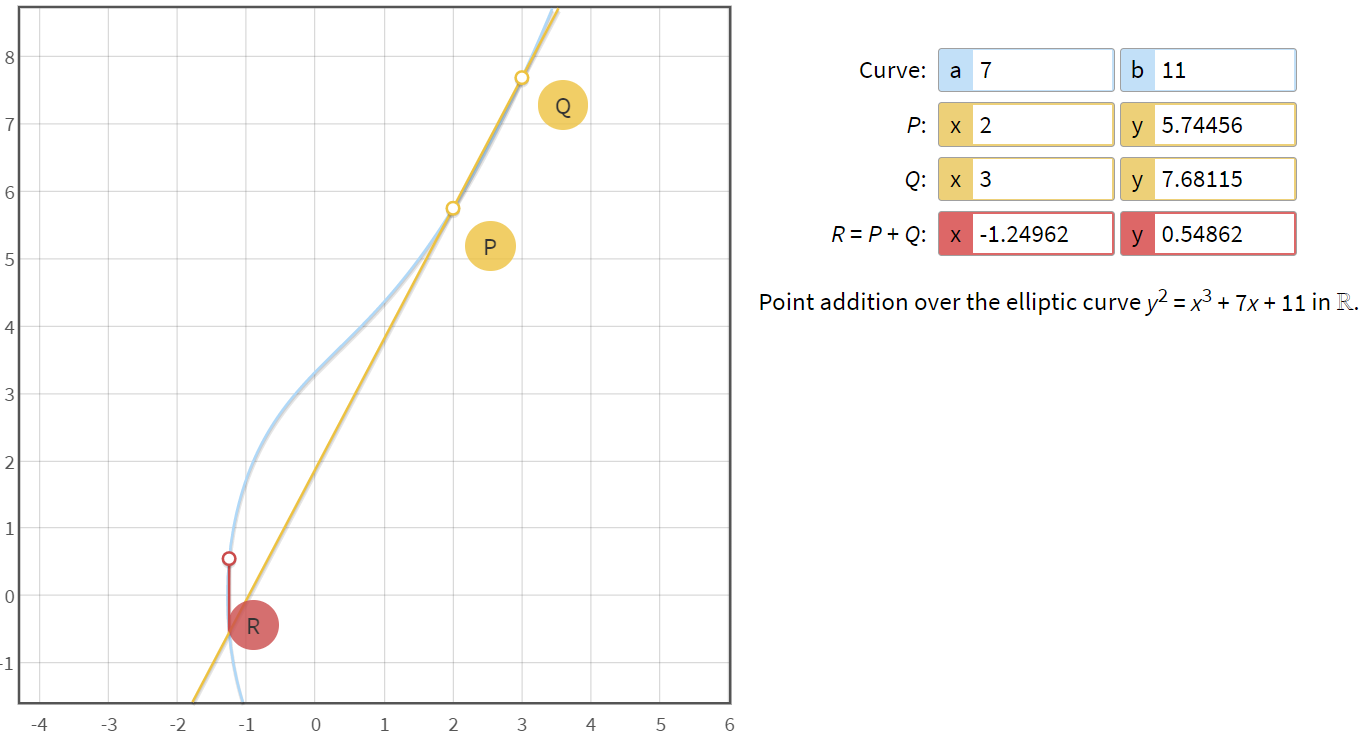


Рисунок 13.2 – Расчет координат точки R (источник)

Для выполнения второго задания было разработано приложение, которое позволяет производить операции арифметического суммирования и скалярного умножения точек. Для этого было написано 2 функции – функция sum, которая принимает на вход координаты 2 точек и возвращает координаты новой точки, и функция duplicate, которая позволяет получить координаты дублированной точки.

Вычислим координаты новой точки, равной k\*P:

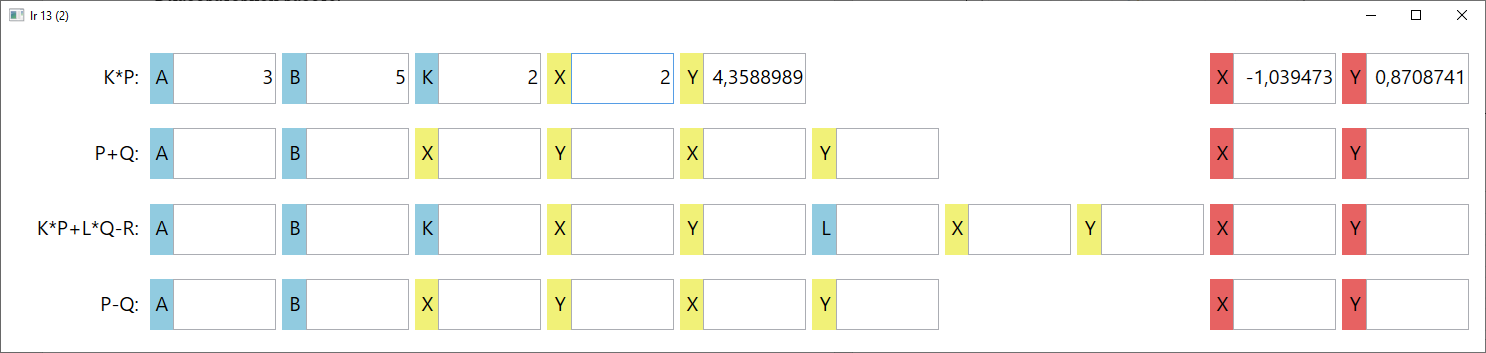


Рисунок 13.3 – Вычисление k\*P (приложение)

Проверим работоспособность приложения, используя источник, данный в лабораторной работе:

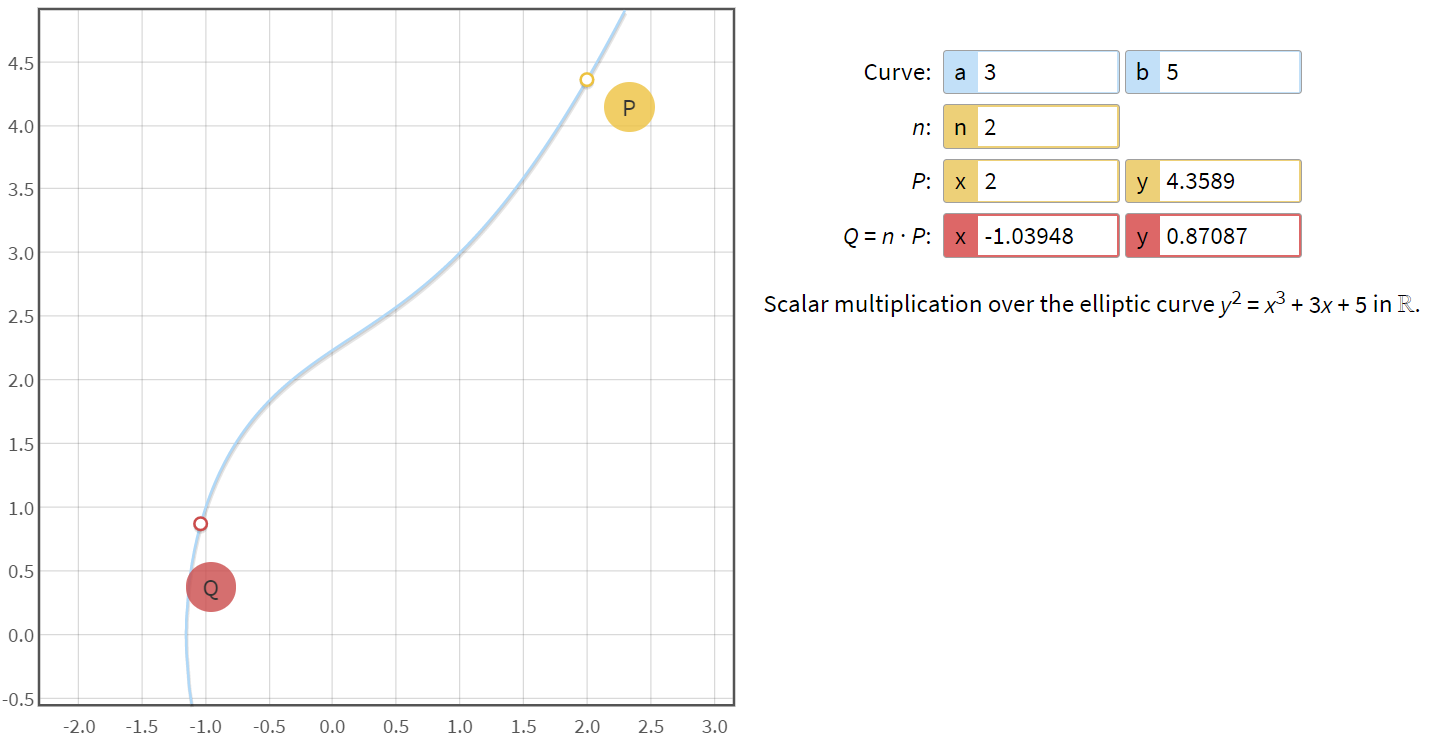


Рисунок 13.4 – Вычисление k\*P (источник)

Таким же образом рассчитаем P + Q:

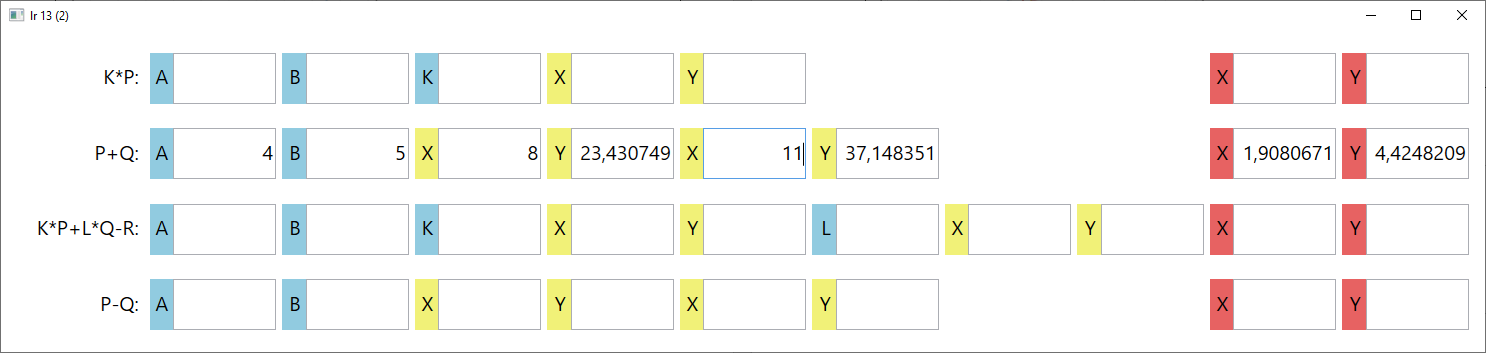


Рисунок 13.5 – Вычисление P+Q (приложение)

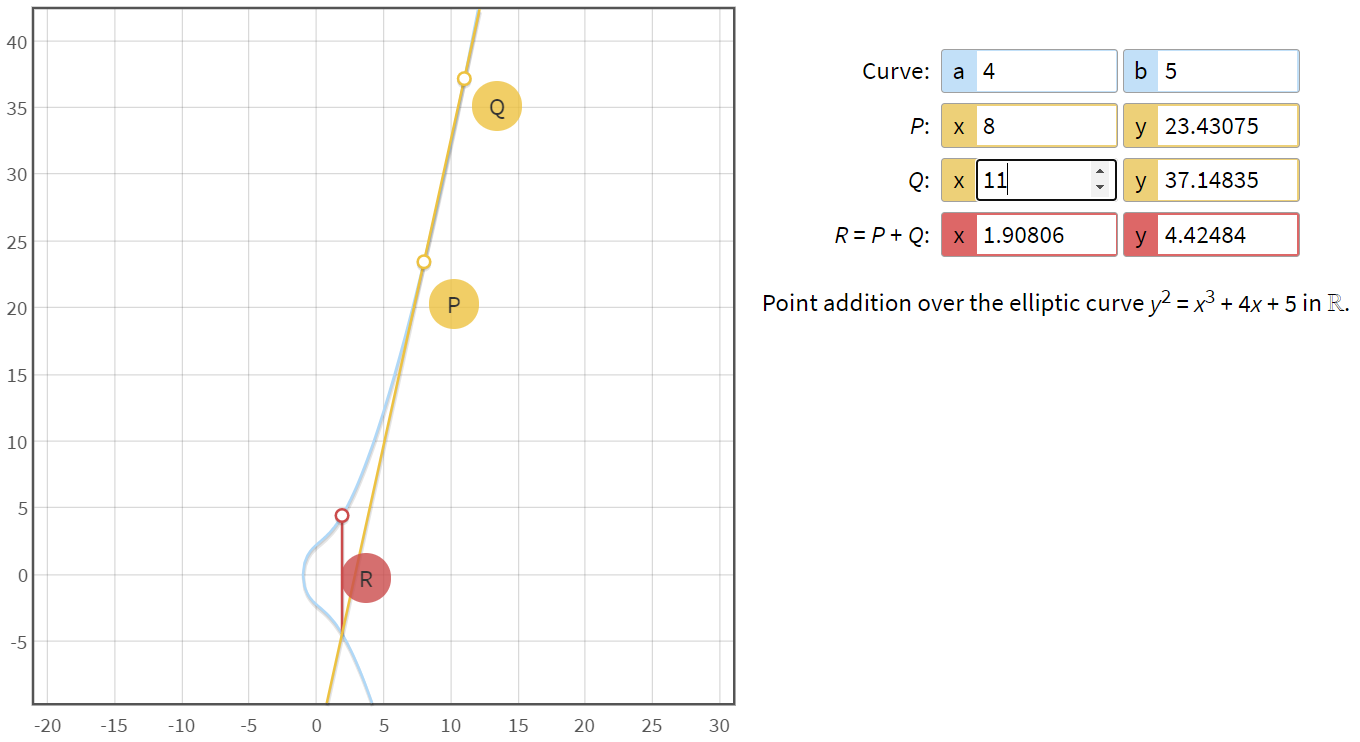


Рисунок 13.6 – Вычисление P+Q (источник)

Вычислим k\*P + l\*Q - R:

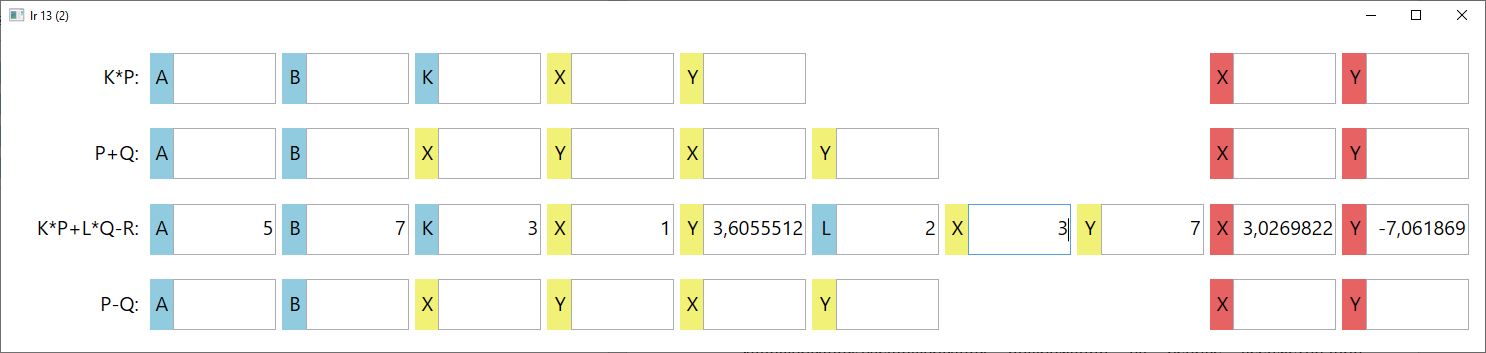


Рисунок 13.7 – Вычисление k\*P+l\*Q-R (приложение)

А также P-Q:

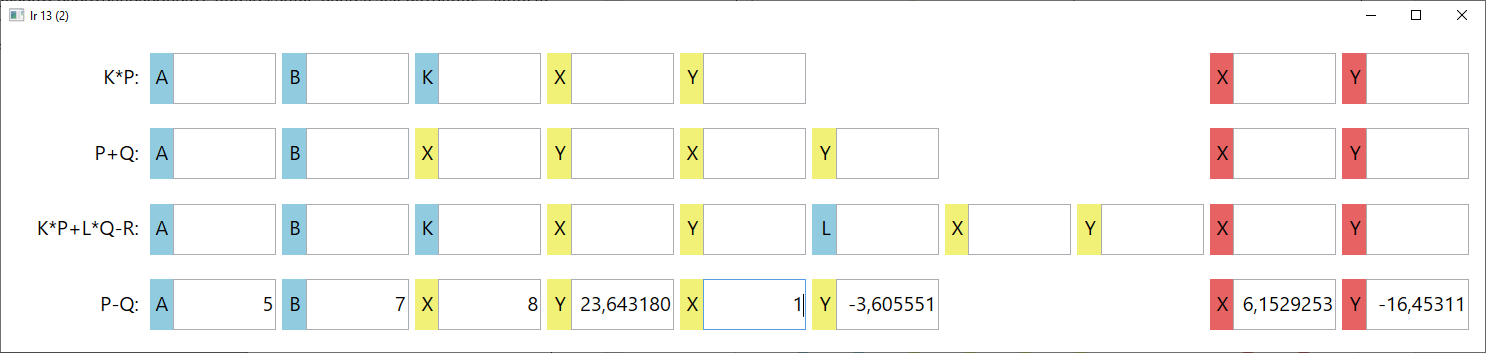


Рисунок 13.8 – Вычисление P-Q (приложение)

**Вывод**

В данной лабораторной работе я закрепила теоретические знания по алгебраическому описанию и геометрическому представлению операций над эллиптическими кривыми: по алгоритмам согласования ключевой информации на основе эллиптических кривых, алгоритмам зашифрования/расшифрования информации на основе ассиметричной криптографии и эллиптических кривых, алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и эллиптических кривых, оценке криптостойкости систем на основе эллиптических кривых. А также разработала собственное приложение для реализации указанных преподавателем методов криптопреобразований на основе эллиптических кривых.