Министерство образования Республики Беларусь

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Исследование криптографических алгоритмов на основе эллиптических кривых»

Выполнил:

студент 3 курса 5 группы ФИТ

Храмых Владислав Олегович

Преподаватель:

Блинова Е.А.

Минск 2020

1. **Теоретические сведения**

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

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

*у*2 = *х*3 + *aх* + *b*

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

4*a3+*27*b2 ≠ 0*.

Формула называется *уравнением Вейерштрасса*, а условие

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 [2]).

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

2. *Группа* – непустое [множество](https://dic.academic.ru/dic.nsf/ruwiki/4759) с определенной на нем [бинарной 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.

3. *Группа для ЭК* есть непустое множество, элементы которого являются точками ЭК



Рисунок 1.1 – 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 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(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*

## 1.1 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 (*р* = 13) состоит из чисел: 0, 1, … , 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 *р* (mod *p*),

Формально ЭК над полем задается так: *Е*р(*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 ко- торой будут рассчитываться точки кривой, и функция кривой.

Рассмотрим конкретный пример.

*Пример* 4. Пусть ЭК формально задается записью *Е*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 – *у*2). Здесь стоит отметить известную нам цикличность в вычислениях на основе модулярной арифметики. Это видно для нашего случая из табл. 11.1.

**Таблица 1.1 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, рассмотрим ситуацию для *х* = 0. Подставим это значение в правую часть уравнения (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 рассматриваемой ЭК нет ни одной точки, координата *х* которой равна 3.

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

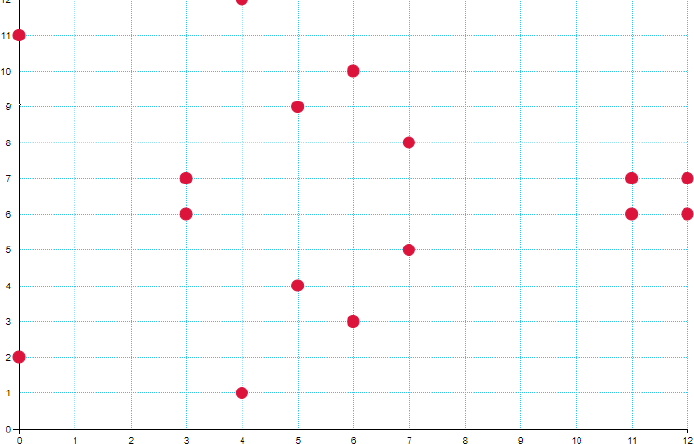


Рисунок 1.2 – Точки ЭК *Е*13(6, –9)

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* существует максимум две точки. Отметим также симметрию в расположении точек относительно *y = p/2*.

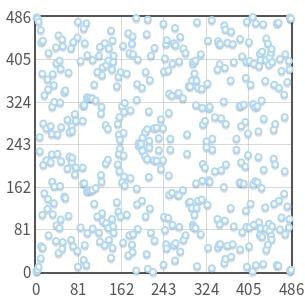
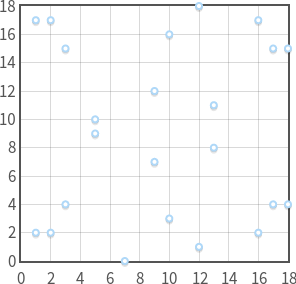


Рисунок 11.4 – Отображение точек ЭК *у*2 = *х*3 – 7*х* + *10* (mod *p*)

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

ми числами.

*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:

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-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 [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*.*

## 1.2 Основные этапы генерации ключевой информации на основе ЭК

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

Входными параметрами являются: число *l*, число *р*, удовлетворяющее условию 22*l-*1 < *р* < 22*l*, *р* = 3 mod 4, 0 < *a* < *p*. Можно использовать некоторое простое число *р* = 22*l* – *с*, где с – небольшое натуральное число.

Выбирается число *b*, такое, что 0 < *b* < *p*. Таким образом, задана ЭК: *Е*р(*а*, *b*).

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

*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

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 (передача) ключевой информации (на основе идеи Диффи-Хеллмана),

в алгоритмах асимметричного шифрования/дешифрования сообщений

в алгоритмах генерации/верификации ЭЦП.

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 случайным 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 сторона.

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 (*m*i) этого сообщения состоят из двух чисел. Вспомним лабораторную 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

Поскольку символы *а* и *b* мы зарезервировали в текущей работе для обозначения параметров ЭК, то блок шифртекста сейчас будем обозначать соответственно символами *С*i1 и *C*i2.

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 шифртекст – это две точки на той же ЭК: *С*1 и *C*2 или *С*i1 и *C*i2.

**2 Практическая часть**

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).

2.1 Найти точки ЭК для значений *х*

2.2. Разработать приложение для выполнения операций над точками кривой:

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

2,3 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.

2,4 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.

2,5 Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA:

Параметры *k* – по собственному усмотрению.

2,6 Хешем подписываемого сообщения, (*Н*(*М*)), является модуль по основанию 13 координаты *х* точки ЭК, соответствующей первому символу собственной 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.

На рисунке приведен общий интерфейс программы (Рисунок 2.1)

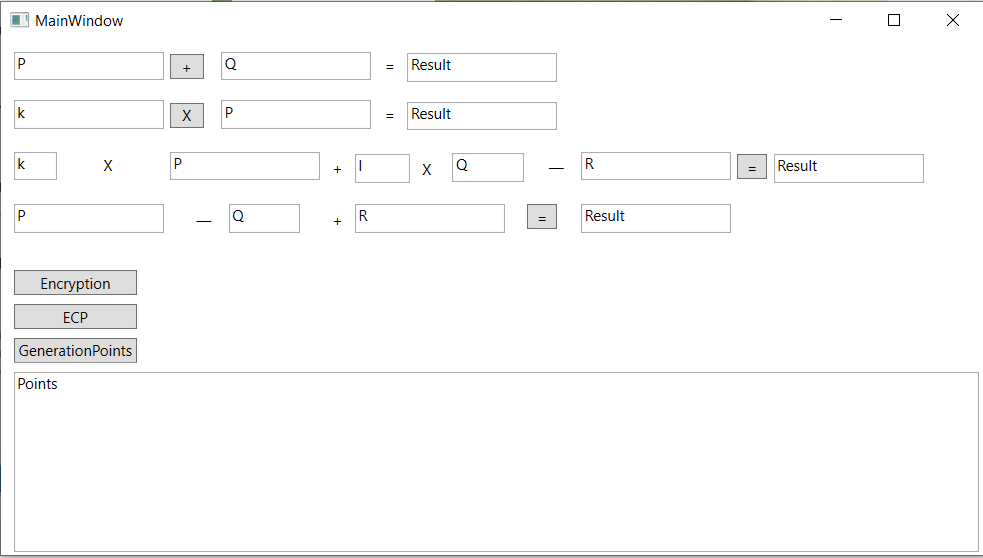


Рисунок 2.1 – Общий интерфейс программы

Далее приведен скриншот выполнения 1 и 2 заданий согласно варианту №2 (Рисунок 2.2)

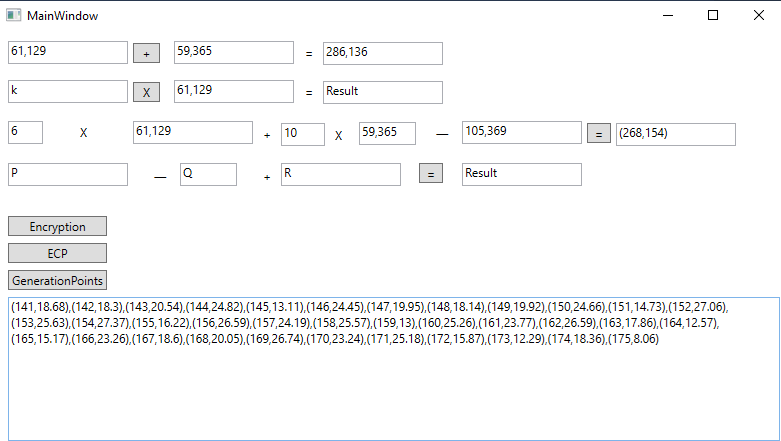


Рисунок 2.2 – Вычисление значений

Далее приведен скриншот выполнения задания №3 и шифрование расшифрование своей фамилии (Рисунок 2.3)

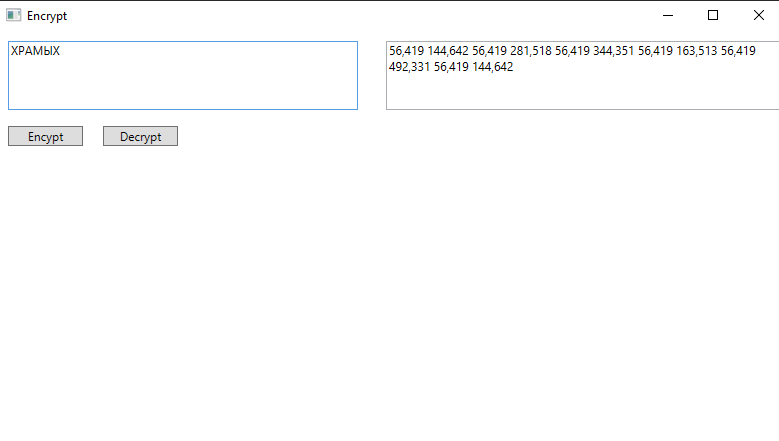


Рисунок 2.3 – Шифрование/Дешифрование Фамилии на основе ЭК

В следующем задании необходимо было реализовать генерацию и верификацию ЭЦП на основе алгоритма ECDSA. Вычислить самостоятельно значение открытого ключа, *Q*. ЭК *Е*751(–1, 1) c генерирующей точкой *G* = (416, 55); порядок точки *q* = 13. Тайный ключ равен 44. В итоге имеем приложение, которое отображает получившийся открытые ключ и выводит булевское значение, отражающее подлинность ЭЦП (рис. 2.4):

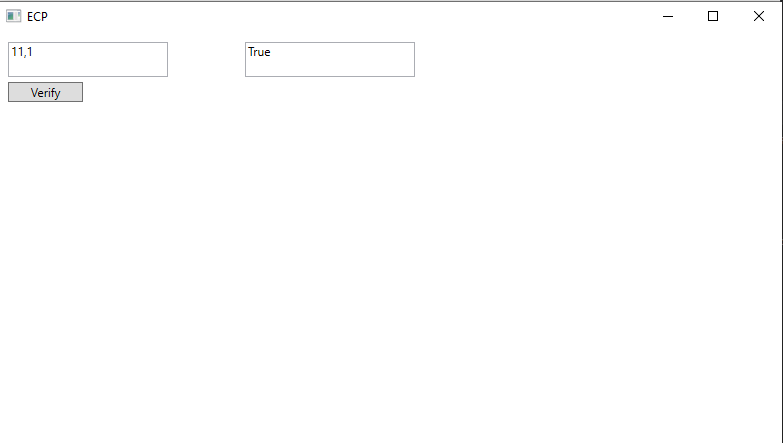


Рисунок 2.4 – ЭЦП

И генерация (Рисунок 2.5)

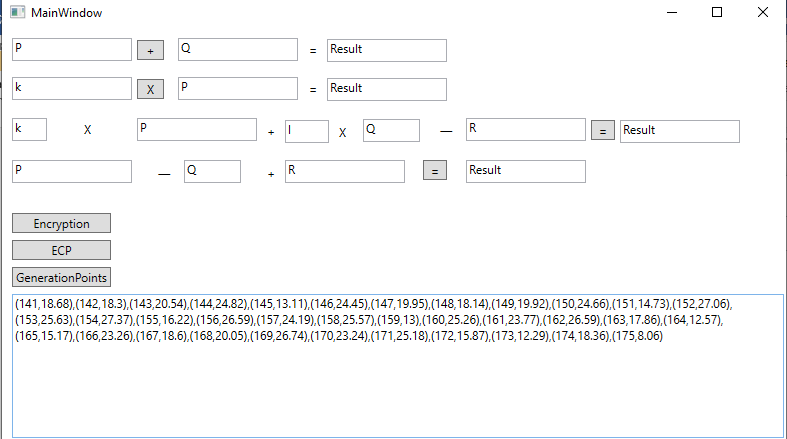


Рисунок 2.5 – Генерация

**Вывод:** в результате лабораторной работы была изучена теория по Эллиптическим кривым, а также основная информация по методам нахождения и вычисления. Также была разработана программа, реализующая требуемые в условии задания