Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информатики и веб-дизайна**

**Лабораторная работа № 13**

Исследование криптографических алгоритмов

на основе эллиптических кривых

Выполнил:

Студент 3 курса 6 группы ФИТ

Дикун Игорь Вячеславович

**2023 г.**

1. **Теоретические сведения**

Криптография базируется на задачах факторизации, дискретного логарифмирования и операциях над точками эллиптичекой кривой (Elliptic Curve, ЕС; ЕС Cryptography, ЕСС). Последние являются предметом исследования в данной работе.

**Определение 1**.*Эллиптические кривые*–математическийобъект, который может быть определен над любым полем.

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

|  |  |
| --- | --- |
| *у*2= *х*3+ *aх* + *b*, | (1.1) |

при этом константы (*а* и *b –* вещественные числа) должны удовле-творять условию

4*a*3 *+* 27*b*2 ≠ 0. (1.2)

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

Формула (1.1) называется уравнением *Вейерштрасса*, 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 обозна-чим символом *О*.

**Определение 4**.*Группа*–непустое множество с определеннойна нем бинарной операцией, называемой сложением и удовлетво-ряющей нескольким аксиомам.

На основе последнего определения мы можем определить группу для ЭК.

**Определение 5**.*Группа для ЭК*есть непустое множество,эле-менты которого являются точками ЭК, обладающими следующими свойствами:

*единичный элемент* –это бесконечно удаленная точка *О*;

*обратная величина точки R* –это точка,симметричная отно-сительно оси *Х*;

*сложение* задается следующим правилом:сумма трех нену-левых 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 вертикаль-ной 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(рис. 11.1), *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* = 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* – это сумма *n* точек *Р*: *nP* = *P + P + P + … + P*.

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

Если *Р* *=* (*х*1, *у*1) и *Q* = (*х*2, *у*2), то *Р* *+ Q =* (*х*3, *у*3) определяется в соответствии с правилами:

|  |  |
| --- | --- |
| *x*3*=* λ2 *– х*1 *– х*2; | (1.3) |
| *у*3*=* λ(*х*1 *– х*3) – *у*1, | (1.4) |

где

= (*у*2 *–* *у*1)*/*(*х*2 *–* *х*1) при *Р* *≠* *Q* и λ = (3(*х*1)2*+а*)/2*у*1 при *Р* *= Q.* (11.5)

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 фор-мул для вычисления λ.

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

**Определение 7**.*Эллиптическая кривая над полем**F**p*задаетсятеми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю *р* (mod *p*):

|  |  |
| --- | --- |
| *у*2≡ *х*3+ *aх* + *b* (mod *p*), | (11.6) |

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

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.

**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 котороговыполняется равенство *qР* = *О*, называется *порядком точки Р*.

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

**Определение 11*.*** Точка*Р*называется*генератором*или*базо-вой точкой* циклической подгруппы(такую точку во многих доку-ментах обозначают символом *G*).

Порядок точки *Р* связан с порядком *m* ЭК *теоремой Лагранжа*, согласно которой *порядок подгруппы* *–* *это делитель порядка ис-ходной группы*.Иными словами,если ЭК содержит *m* точек,а однаиз подгрупп содержит *q*, то *q* является делителем *m*.

Для ЭК *Ер*(*а*, *b*) порядок *m* группы точек должен удовлетворять неравенству *p* + 1 – 2*p*1/2≤ *m* ≤ *p* + 1 + 2*p*1/2.

*Генерация ключевой информации на основе ЭК*.Обычно он основан на выполнении следующих условий и операций.

1.1. 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.

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

Таким образом, задана ЭК: *Ер*(*а*, *b*).

1.3. Выбираются порядок *q* (простое число) и генерирующая точка *G*, которая задается двумя координатами

Второй этап: генерация ключевой информации.

2.1. Входными параметрами являются: *р*, *а*, *b*, *q* и *G*.

2.2. Генерируется тайный ключ – число *d*, выбранное из мно-жества {1, 2, …, *q* – 1}.

2.3. Вычисляется открытый ключ – точка *Q:*

|  |  |
| --- | --- |
| *Q* = *dG*, | (11.8) |

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

*Шифрование/расшифрование на основе ЭК.*

Зашифрованное сообщение или каждый зашифрованный блок (*mi*) этого сообщения состоят из двух чисел. Обратимся к лабораторной работе № 8, где блок шифртекста (*ci*) в соответствии с выражениями (8.9) и (8.10) мы обозначали двумя символами *аi* и *bi* и вычисляли как

*аi* ≡ *gk* mod *p*, *bi* ≡(*ykmi*) mod *p*.

Поскольку символы *а* и *b* мы зарезервировали в текущей работе для обозначения параметров ЭК, то блок шифртекста сейчас будем обозначать соответственно символами *Сi*1 и *Ci*2.

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 *Сi*1 и *Ci*2.

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**:

|  |  |
| --- | --- |
| *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 отношению к точке (*х*, *у)*

*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 *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 легитимность подписи и целостность полученного сообщения.

**2 Практическая часть**

**Задание 1**

1.1 Найти точки ЭК для значений *хmin = 36, хmax = 70.*

1.2 Разработать приложение для выполнения операций над точками кривой:

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

при *k=6, l=10.*

**Задание 2**

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).

**Задание 3**

Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ЕС DSA: ЭК *Е*751(–1, 1) c генерирующей точкой *G* = (416, 55); порядок точки *q* = 13

Интерфейс программы представлен на рисунке 2.1.

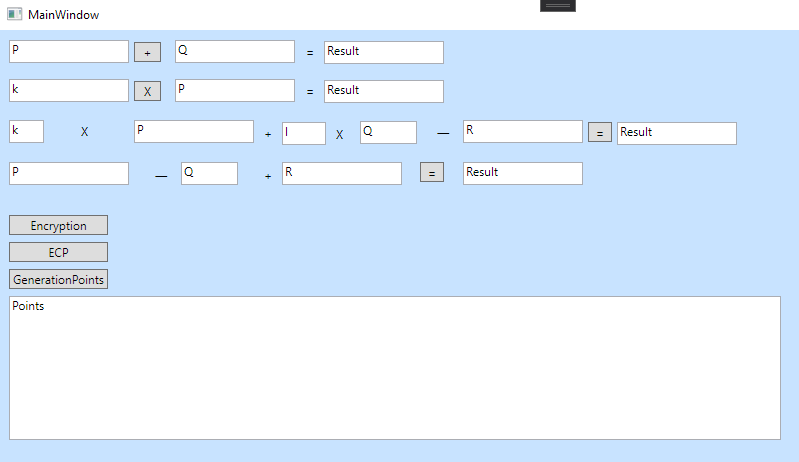


Рисунок 2.1 – Общий интерфейс программы

На рисунке 2.2 отображено решение первого пункта задания № 1, где необходимо было вычислить все точки ЭК для значений от *хmin = 36 до хmax = 70.*

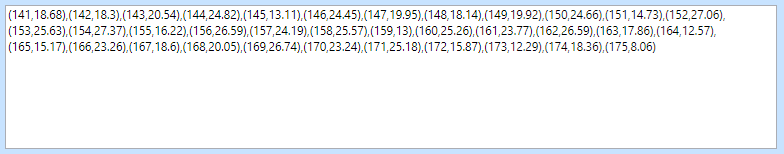


Рисунок 2.2 – Точки ЭК

Пример выполнения второй части задания № 1 представлен на рисунке 2.3, где производятся различные операции над точками ЭК.

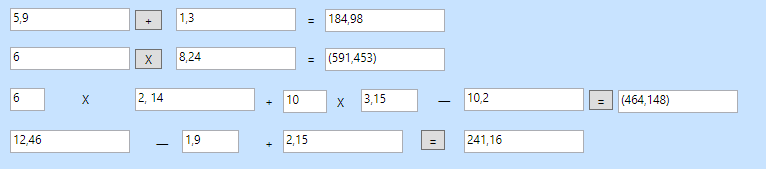


Рисунок 2.3 – Операции над точками ЭК

Далее, на рисунке 2.4, приведен скриншот выполнения задания № 2 с шифрованием и расшифрованием своей фамилии.

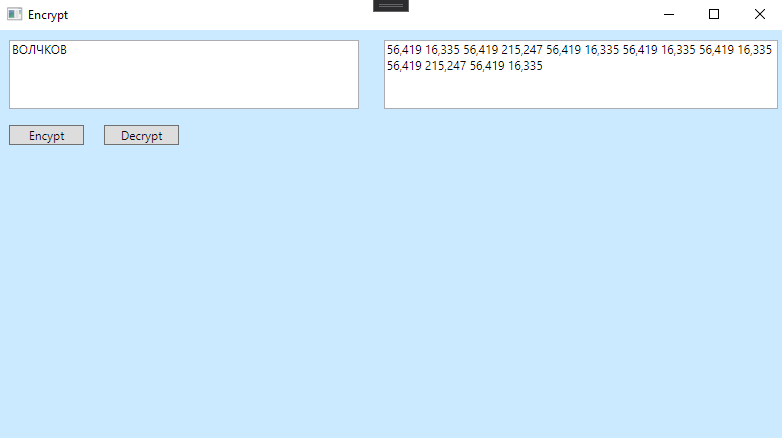


Рисунок 2.4 – Шифрование/дешифрование фамилии на основе ЭК

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 12. Полученное приложение, проверяющее подлинность ЭЦП, представлено на рисунке 2.5.

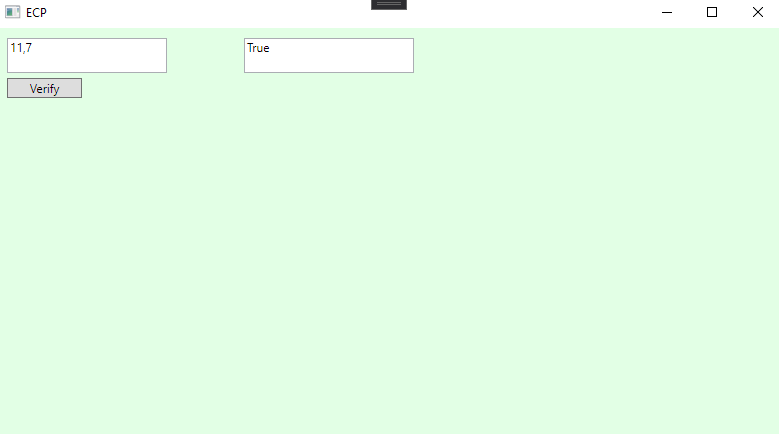


Рисунок 2.4 – Проверка подлинности ЭЦП

**Вывод**: таким образом, в ходе лабораторной работы была изучена теория по Эллиптическим кривым, а также основная информация по методам нахождения и вычисления. Также было разработано приложение, реализующее требуемые в условии задания