МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №11 НА ТЕМУ:

Исследование криптографических алгоритмов на основе эллиптических кривых

Выполнила:

Студентка 3 курса 1 группы ФИТ

Шимчёнок Елизавета Константиновна

**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 алгоритмам реализации 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.

**Теоретические сведения**

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

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

*у2 = х3 + aх + b*,

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

*4a3 + 27b2 ≠ 0*.

Условие исключает из рассмотрения кривые с особыми точками или особые кривые.

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

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

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

– единичный элемент – это бесконечно удаленная 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.

Принцип умножения точки Р на целое положительное число n – это сумма n точек Р:

nP = P + P + 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 соответствии с правилами:

x3= λ2 – х1 – х2;

у3= λ(х1 – х3) – у1,

где

λ = (у2 – у1)/(х2 – х1) при Р ≠ Q и λ = (3(х1)2 +а)/2у1 при Р = Q

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.

**Ход работы (вариант 12)**

В основе задания – ЭК вида у2 = х3 – х + 1 (mod 751):

а = –1, b = 1, р = 751, т. е. Е751(–1, 1).

**Задание 1**

**1.1 Найти точки ЭК для значений х: x­min=621 и xmax=655.**

Координаты расположения точек должны быть ограничены квадратом некоторых чисел по модулю 751. С ограничением определяем цикличность в вычислениях на основе модулярной арифметики (рисунок 1).

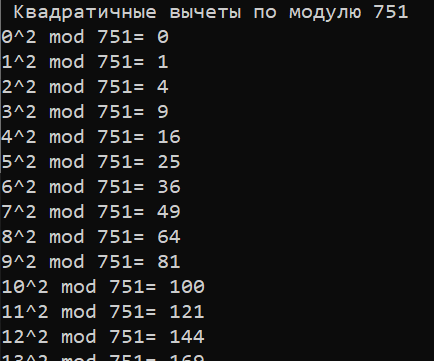


Рисунок 1 – Программное вычисление квадратичных вычетов

Найдем y для x = 621 (проверка с использованием онлайн калькулятора https://planetcalc.ru/8326/ на рисунке 2).

у2 = 6213 – 621 + 1 (mod 751) = 557.

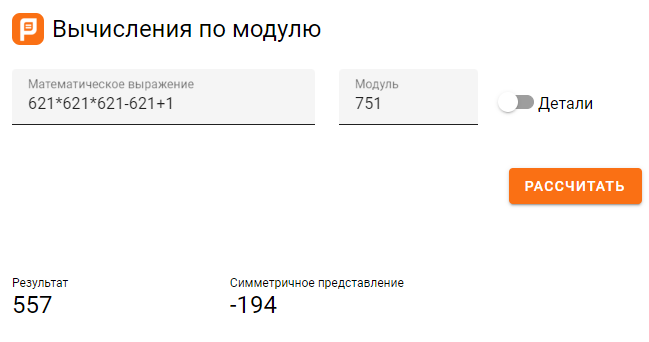


Рисунок 2 – Проверка вычисления

Вычислим *y*2 для всех *x* в диапазоне [621,655] (рисунок 3).

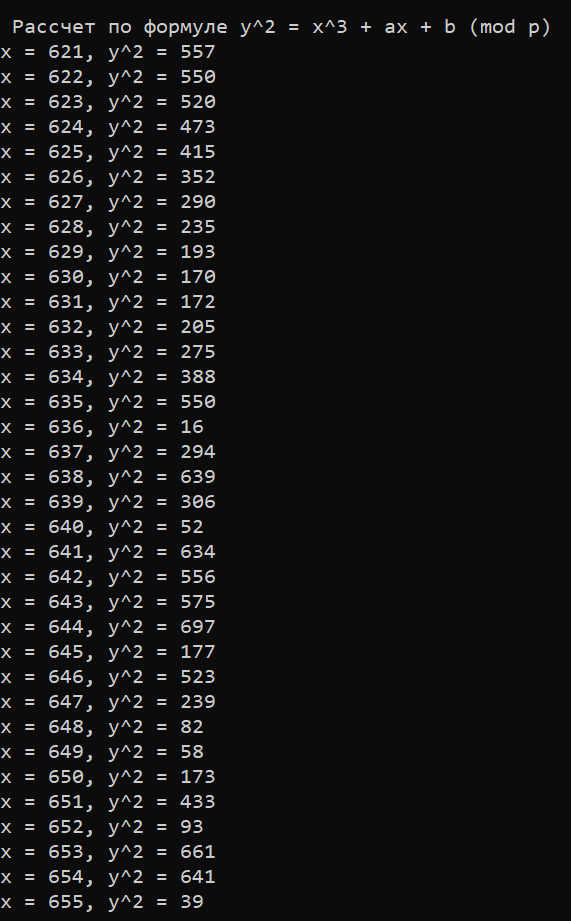


Рисунок 3 – Определение целочисленных координат

Теперь ищем соответствие y2 (в примере это 557) в квадратичных вычетах. Если соответствия нет – нет ни одной точки на ЭК с рассматриваемой координатой x.

Что, собственно, мы и получили в примере с числом 557. Данной рассчитанной сумме вычета нет соответствия => на рассматриваемой кривой нет точки, с координатой x = 621.

В случае, если соответствие было найдено, как в случае с координатой

x = 623, проводятся следующие вычисления:

y2 = 6233 – 623 + 1 (mod 751) = 520.

По таблице квадратов по модулю 751:

1662 mod 751= 520.

Соответственно, точка будет: (623, 166).

Таким образом проверяется каждая переменная x. Результат вычислений точек, принадлежащих ЭК изображен на рисунке 4.

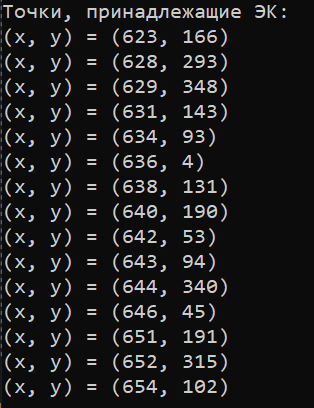


Рисунок 4 – Точки, принадлежащие ЭК

**1.2. Выполнить операции над точками кривой**

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

Исходные значения в соответствии с 12 вариантом:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Параметры | | Координаты точек | | |
| k | l | *P* | *Q* | *R* |
| 6 | 7 | (61, 622) | (61, 622) | (90, 730) |

а) Умножим точку *P* (61, 622) на *k* = 6.

Принцип умножения точки *Р* на целое положительное число *n* – это сумма *n* точек *Р*: *nP* = *P* + *P* + *P* + … + *P*.

6P = 2P + 4P, где

4P = 2P + 2P,

2P = P + P.

Воспользуемся формулами

x3= λ2 – х1 – х2 (mod p);

у3= λ(х1 – х3) – у1 (mod p),

где при *P* != *Q:*

λ = (y2 – y1)/(x2 – x1) (mod p),

при *P* = *Q:*

λ = (3(x1)2 + a)/2y1 (mod p).

* 2*P* = *P* + *P*

λ = (3 · 612 – 1) / 2 · 622 (mod 751) = 242,

*x*3= 2422 – 61 – 61(mod 751) = 615,

*у*3= 242(61 – 615) – 622(mod 751) = 490.

Получаем точку **2*P* (615, 490)**.

* 4*P* = 2*P* + 2*P*

λ = (3 · 6152 – 1) / 2 · 490 (mod 751) = 626,

x3= 6262 – 615 – 615 (mod 751) = 126,

у3= 626 · (615 – 126) – 490 (mod 751) = 718.

Получаем точку **4P (126, 718)**.

* 6*P* = 2*P* + 4*P*

Используем λ = (y2 – y1)/(x2 – x1) (mod p),

λ = (718 – 490) / (126 – 615) (mod 751) = 41,

x3= 412 – 615 – 126 (mod 751) = 189,

у3= 41 · (615 – 189) – 490 (mod 751) = 454.

Получаем точку **6P (189, 454)**.

б) Выполним операцию сложения точек Р + Q = 2P.

в) Найдем результат kР + lQ – R.

**kP = (189, 454)** из предыдущих заданий. **lQ = (623, 585)** найдено аналогичным образом.

Для нахождения kР + lQ – R воспользуемся правилом, что

kР + lQ – R = kР + lQ + (–R).

Найдем (–R). Обратной точкой для точки R (x; y) на эллиптической кривой называют точку – R (x; – y).

R (90, 730).

– y mod p = – 730 mod 751 = 21.

Отсюда -**R (90, 21)**.

В результате по порядку вычислим:

kP + lQ = (33, 396);

kPlQ + (-R) = (405, 747).

г) Аналогично вычисляем P-Q+R.

-Q (61, 129) (для y вычисляем: – y mod p).

P-Q+R = (90, 1481).

Результат программного выполнения задания 1.2 приведен на рисунке 5.

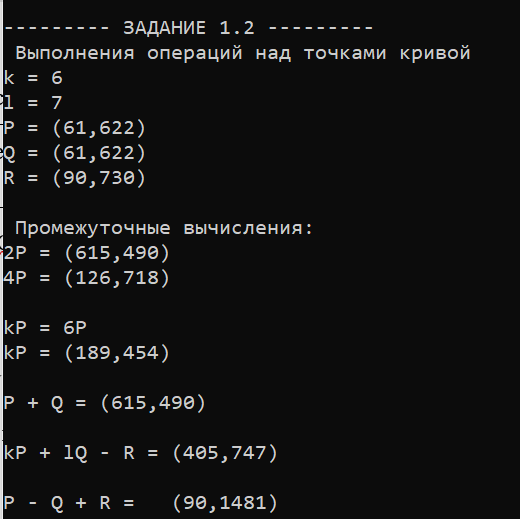


Рисунок 5 – Результат выполнения части программы

Все вычисления были проверены при помощи онлайн калькулятора по адресу: https://andrea.corbellini.name/ecc/interactive/modk-add.html.

**Задание 2**

**2.1. Создать 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.**

Для зашифрования использовалась основная формула:

С1 = kG, С2 = P + kQ.

Использовались следующие входные данные:

|  |  |  |
| --- | --- | --- |
| Параметры | | Генерирующая точка |
| k | d | *G* |
| 6 | 51 | (0,1) |

Шифрование:

Найдем значение открытого ключа Q как Q = dG, где G – базовая точка подгруппы. Получаем значение **Q (120, 147)**. Результат подтверждается рисунком 6.

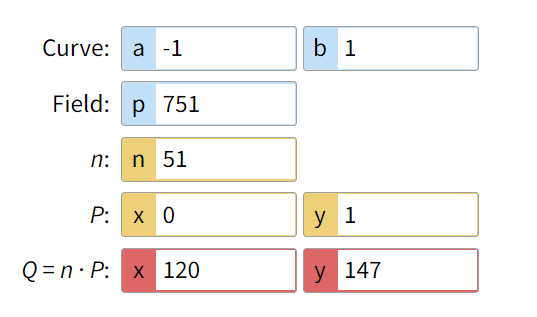


Рисунок 6 – Вычисление открытого ключа

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: С1 и C2 или Сi1 и Ci2.

Вычисление С1 (не зависит от входящего сообщения, будет одинаковым для всех зашифрованных символов):

С1 = kG,

**С1 = (725, 195)**.

Из таблицы 11.10 лабораторного практикума определим координаты точек, соответствующих символам шифруемого сообщения.

Л – P(200, 721); И – P(198, 224); З – P(197, 606); А – P(189, 297).

Теперь можем получить C2 для каждой буквы:

С2 = P + kQ,

kQ = 6 · (120, 147) = (181, 133);

**С2(Л)** = (200, 721) + (181, 133) = **(454, 628)**.

Далее требуется лишь повторить вычисление C2 для каждой буквы текста:

**С2(И)** = (198, 224) + (181, 133) = **(502, 225)**.

**С2(З)** = (197, 606) + (181, 133) = **(405, 4)**.

**С2(А)** = (189, 297) + (181, 133) = **(238, 576)**.

В результате одной букве соответствует шифртекст из двух точек: Л – (725, 195), (454, 225).

Результат программы изображен на рисунке 7.

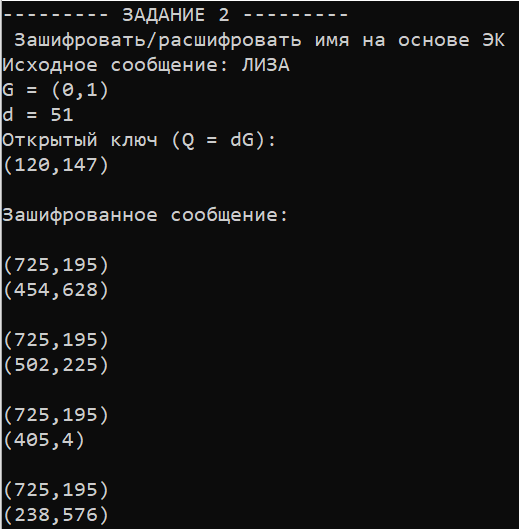


Рисунок 7 – Зашифровка сообщения «ЛИЗА»

Для расшифрования сообщения необходимо вычислить:

P = С2 – dC1;

dC1 = 51 \* (725, 195) = (181, 133).

Найдем -dC1, как точку, обратную dC1:

-133 (mod 751) = 618;

-dC1 = (181, 618);

P(Л) = (454, 628) + (181, 618) = (200, 721).

Далее требуется найти в таблице 11.10 вычисленную точку – это и будет расшифрованный символ (в данном случае: буква «Л»). Остальные буквы по аналогии.

Приложение успешно расшифровывает сообщения.

**Задание 3**

**3.1. Создать приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA: ЭК Е751(–1, 1) c генерирующей точкой G = (416, 55); порядок точки q = 13.**

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



Рисунок 8 – Вычисление хеша сообщения

Генерация ЭЦП:

1. Выбрать число *k* (1 < *k* < *q*), *q* – порядок точки *G*.

Пусть **k = 2**, **d = 11**.

2. Вычислить точку *kG* = (*х*, *у*), вычислить *r* ≡ *x* mod *q* (при *r* = 0 изменить *k* и повторить шаг 2).

kG = 2G = G + G;

λ = (3 · 4162) – 1) / 2 · 55 (mod 751) = 439,

x3= 4392 – 416 – 416 (mod 751) = 384,

у3= 439(416 – 384) – 55 (mod 751) = 475.

Получили точку 2G (384, 475). Отсюда

r = 384 mod 13;

**r = 7**.

3. Вычислить *t* ≡ *k*–1 mod *q* (например, на основе расширенного алгоритма Евклида).

Найдем t ≡ k-1 mod q = 2-1 mod 13.

13 = 2 · 6 + 1;

t = (13 – 6) mod 13 = 6.

4. Вычислить *s* = (*t* (*H*(*M*) + *dr*)) mod *q*; при *s* = 0 изменить *k* и повторить алгоритм. Пусть H(M) = 11, тогда

s = (t (H(M) + dr)) mod q = 6 \* (11 + 9 \* 7) mod 13;

**s = 2**.

Подпись сообщения – (7, 2). Стороне получателя отсылается сообщение *М* и ЭЦП (числа *r* = 11 и *s* = 4).

**3.2. Вычислить самостоятельно значение открытого ключа Q (рисунок 9).**

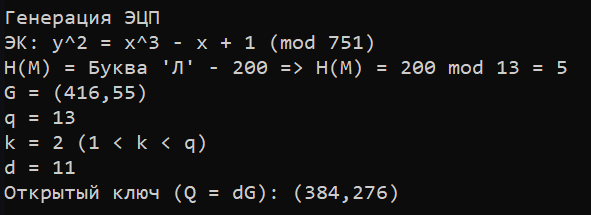


Рисунок 9 – Вычисление открытого ключа Q

Верификация ЭЦП. Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над М и полученной ЭЦП (числа r = 7 и s = 2).

1. Подтверждается выполнение условий 1 < r, s < q.

2. Вычисляется Н(М) – положим, что в результате хеширования полученного сообщения М его хеш не изменился: Н(М) = 5; далее вычисляется

w = s–1mod q = 2–1 mod 13 = 6.

3. Вычисляются

u1 = w Н(М) (mod q) = 6 · 11 (mod 13) = 1,

u2 = wr (mod q) = 6 · 7 (mod 13) = 3.

4. Вычисляются

Gu1 + Qu2 = 1(416, 55) + 3(455, 368) = (416, 55) + (416, 55);

Gu1 + Qu2 = (384, 475) = (x', y');

v = x' mod q = 384 mod 13 = 7.

5. Сравниваются v = 7 и r = 7: равенство выполняется – подтверждается легитимность подписи и целостность полученного сообщения М.

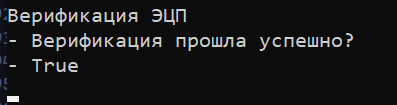


Рисунок 9 – Вычисление открытого ключа Q

**Ответы на вопросы**

1. Дать определение эллиптической кривой.

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

2. Записать уравнение ЭК над вещественными числами (ЭК в криптографии, ЕСС).

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

у2 = х3 + aх + b,

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

4a3 + 27b2 ≠ 0.

3. Объяснить и показать на примере правила выполнения основных операций над точками ЭК.

А) Проверяем, что точка имеет координаты (x, y), которые удовлетворяют уравнению кривой:

Б) Проверяем, что координаты точки лежат в диапазоне, определяемом порядком группы точек на кривой.

Пример: есть кривая ЭК с параметрами a = -7, b = 10, и порядком группы точек на кривой, равным 23. Для двух точек Q = (2,7) и R = (18,13).

4. Что такое «рациональная точка»?

Точка, координаты которой принадлежат заданному полю.

5. Как производится умножение точки ЭК?

Принцип умножения точки Р на целое положительное число n – это сумма n точек Р: nP = P + P + P + … + P.

6. Как производится умножение точки Р на число k, если k принимает значение: 2, 5, 11, 20, 32, 100, 256, 751, 1024?

Для k = 2: 2P = P + P.

Для k = 5: 4P = 2P + 2P, 5P = 4P + P.

Для k = 11: 8P = 4P + 4P, 11P = 8P + 2P + P.

Для k = 20: 16P = 8P + 8P, 20P = 16P + 4P.

Для k = 32: 32P = 16P + 16P.

Для k = 100: 64P = 32P + 32P, 100P = 64P + 32P + 4P.

7. Составить алгоритм многократного сложения точки ЭК (умножения точки на число) на основе примера 7.

* Инициализируем переменную *Q = O*, где *O* – это точка в бесконечности на кривой ЭК.
* Представляем число k в двоичном виде.
* Для каждого бита числа *k* в двоичном представлении, начиная с младшего бита:
* Удваиваем точку *Q: Q = 2Q*.
* Если равен 1, то прибавляем к точке *Q* исходную точку *P*:
* *Q = Q + P.*
* После прохождения всех битов числа *k*, точка *Q* будет равна *kP*.
* Возвращаем точку *Q*.

8. Привести расчеты для точки Q при известных d и G из примера 7.

ЭК вида Е67(2, 3), G = (2, 22) и d = 4. Тогда Q = dG = 4G, 4G = 2G + 2G, 2G = G + G. Воспользуемся формулами:

x3 = λ2 – х1 – х2 (mod p);

у3 = λ(х1 – х3) – у1 (mod p),

где λ = (3(х1)2 +а)/2у1 (mod p) при Р = Q.

Вычисления:

λ = (3 · 22 + 2) / (2 · 22) mod 67 = 46,

x3 = 462 – 2 – 2 (mod 67) = 35,

у3 = 46(2 – 35) – 22 (mod 67) = 1.

Получаем точку 2G (35, 1). Вычислим 4G:

λ = (3 · 352 + 2) / (2 · 1) mod 67 = 63,

x3 = 632 – 35 – 35 (mod 67) = 13,

у3 = 63(35 – 13) – 1 (mod 67) = 45.

Получаем точку Q (13, 45).

9. Есть ли отличия в применении операций над точками ЭК над конечными полями и над действительными числами?

Основное отличие заключается в том, что операции над точками на эллиптических кривых над конечными полями производятся с помощью арифметики в конечных полях (например, полях Галуа), тогда как операции над точками на эллиптических кривых над действительными числами производятся с помощью арифметики действительных чисел.

В арифметике конечных полей умножение и сложение выполняются по модулю простого числа p, которое определяет размер поля. Это позволяет производить вычисления над точками на эллиптических кривых с использованием целочисленной арифметики, что важно для реализации криптографических алгоритмов на компьютерах.

С другой стороны, в арифметике действительных чисел умножение и сложение производятся без ограничений на размер чисел. В этом случае вычисления над точками на эллиптических кривых производятся с помощью вещественной арифметики, что может быть менее эффективным в плане вычислительной сложности.

10. Записать уравнение ЭК при формальном ее представлении в следующем виде: Ер(а, b).

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

у2 = х3 + aх + b (mod p),

4a3 + 27b2 ≠ 0 (mod p),

и т.д.

11. Из какого числа точек состоит ЭК Е11(6, –9)? Дать их координаты.

Для определения числа точек на кривой *E*11(6, –9) необходимо вычислить количество точек на этой кривой в пределах конечного поля *Z*11. Для этого можно воспользоваться теоремой Хассе-Вейля, которая гласит, что количество точек на кривой *Ep* (*a*, *b*) в конечном поле *Fp* примерно равно

*p* + 1 – *t*, где *t* – параметр кривой, называемый порядком кривой.

Для кривой *E*11 (6, –9) порядок *t* можно вычислить, перебрав все точки на кривой и считая их количество. Воспользуемся для этого алгоритмом полного перебора точек, который заключается в последовательном переборе всех возможных значений координат (*x*, *y*) в конечном поле *Z*11 и проверке, является ли точка (*x*, *y*) находится на кривой *E*11 (6, –9).

Результаты перебора показывают, что кривая *E*11(6, –9) состоит из 12 точек, перечисленных в таблице ниже, в которой координаты точек записаны в виде (*x*, *y*):

(0, 3), (0, 8), (1, 2), (1, 9), (6, 0), (6, 11), (7, 2), (7, 9), (8, 3), (8, 8), (9, 4),

(9, 7).

12. Найти все точки ЭК Е11(1, 2).

Для нахождения всех точек на кривой E11(1, 2) в конечном поле Z11 можно воспользоваться алгоритмом полного перебора точек, который заключается в последовательном переборе всех возможных значений координат (x, y) в конечном поле Z11 и проверке, является ли точка (x, y) находится на кривой E11(1, 2).

Применяя этот алгоритм, получим следующие 13 точек на кривой

E11(1, 2) в конечном поле Z11:

(0, 6), (0, 5), (1, 1), (1, 10), (3, 3), (3, 8), (4, 2), (4, 9), (5, 1), (5, 10), (9, 3), (9, 8), (10, 6).

13. На чем основа криптостойкость систем на основе ЭК? Области применения ЭК в криптографии.

Криптостойкость систем на основе эллиптических кривых (ЭК) основана на сложности задачи дискретного логарифмирования на кривых ЭК. В частности, для заданной точки P и числа k, которое является секретным ключом, найти точку Q = kP является вычислительно сложной задачей, к которой пока нет эффективных алгоритмов решения.

Одно из наиболее распространенных применений ЭК в криптографии – это создание криптографических систем на основе ЭК, таких как ECDSA (эллиптическая криптография с открытым ключом) и ECDH (эллиптический протокол Диффи-Хеллмана), которые используются для аутентификации и обмена ключами в интернет-протоколах SSL/TLS.

14. Что такое «порядок точки» ЭК? Показать на примере. Какую роль этот параметр играет в криптографии на основе ЭК?

Порядок точки относительно замкнутой кривой на плоскости – это целое число, представляющее число полных оборотов, которое делает кривая вокруг заданной точки против часовой стрелки.

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.

15. Что такое «базовая точка» ЭК? Какую роль этот параметр играет в криптографии на основе ЭК?

Базовая точка (или точка генератор) на эллиптической кривой – это фиксированная точка P, которая используется в криптографии на основе эллиптических кривых для генерации случайных ключевых значений и подписей.

Роль базовой точки заключается в том, что она позволяет генерировать другие точки на кривой, которые могут быть использованы для создания ключей или подписей. В частности, любую точку Q на кривой можно представить в виде кратной суммы базовой точки P, т.е. Q = kP, где k - целое число. Это свойство позволяет использовать базовую точку для генерации случайных значений k, которые могут быть использованы в криптографии для создания ключей и подписей.

16. Объяснить порядок формирования ключевой информации на основе ЭК.

– Выбор параметров ЭК: выбираются параметры эллиптической кривой, такие как коэффициенты a и b, модуль p и базовая точка P.

– Генерация закрытого ключа: случайным образом выбирается целое число d, которое является закрытым ключом пользователя.

– Вычисление открытого ключа: открытым ключом пользователя является точка Q = dP, т.е. результат умножения базовой точки на закрытый ключ.

– Обмен ключами: для установления защищенного соединения пользователи обмениваются открытыми ключами и с помощью них вычисляют общий секретный ключ.

– Вычисление общего секретного ключа: общий секретный ключ вычисляется путем умножения открытого ключа другого пользователя на закрытый ключ текущего пользователя, т.е. K = dQ = d(kP), где k - закрытый ключ другого пользователя.

17. Сгенерировать ключевую информацию на основе кривой Е11(1, 2).

Для генерации ключевой информации на основе кривой Е11(1, 2), нужно сначала выбрать базовую точку на кривой. Для этой кривой можно выбрать точку (2,7), которая является точкой большого простого порядка.

Шаги алгоритма с выбранной базовой точкой (2,7):

1. Выбрать базовую точку *G* = (2,7).
2. Выбрать случайное секретное число *d*, например, *d* = 3.
3. Вычислить публичный ключ *Q = d*\**G* = 3\*(2, 7) = (4, 1).

**Вывод:** были изучены и приобретены практические навыки разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.