Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №11**

**«ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ»**

Выполнил:

Cтудент 3 курса 1 группы

Парибок И. А.

Вариант 5

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию и геометрическому представлению 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**

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.

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

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.

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 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 (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 относительно 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.

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. Например, точка 25*P* может быть представлена как 25*P* = = 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 соответствии с правилами:

где

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.

*ЭК над конечными полями*

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*):

далее для упрощения используем знак простого неравенства:

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.

**Практическое задание**

**Задание 1**

Приложение написано на языке программирования C# и позволяет найти точки ЭК для значений х в диапазоне [141, 175]. Также приложение реализиует следующие операции над точками эллиптической кривой:

* kP;
* P + Q;
* kP + lQ – R;
* P – Q + R.

## 2. Методика выполнения поставленных задач

В основе задания – ЭК вида y2 = x3 + ax + b (mod 751): a = –1, b = 1, p = 751, т.е. E751(–1, 1).

Указанные точки P (59, 386), Q (70, 195), R (72, 254). За числовые коэффициенты примем k = 11, l - 5.

Для реализации первой части задания применим указанную выше формулу ЭК для вычисления ординат, соответствующих абсциссам из диапазона [716; 750]. Реализация данной задачи продемонстрирована на рисунке 1.

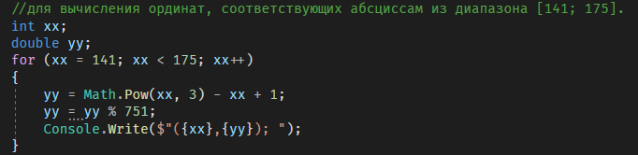


Рис. 1 – Вычисление ординат

Результат выше изложенных вычислений приведен на рисунке 2.

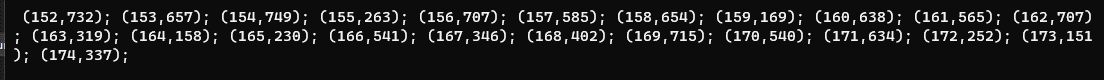


Рис. 2 – Результат вычисления точек

Далее проведем указанные в задании операции. Все выражения состоят из простейших алгебраических операций над точками эллиптической кривой: умножения на коэффициент, сложения точек, вычисление обратной точки.

Рассмотрим сложение точек. Первоначально необходимо проверить, выполняется ли для данной эллиптической кривой неравенство: 4a3+27b2 ≠ 0, где a = –1, b = 1.

Далее необходимо найти λ - угловой коэффициент секущей, проведенной через точки P, Q. Он равен:

λ = ( у2 – у1)/( х2 – х1), если P≠Q,

λ = (3(х1) 2+а)/2 у1, если P=Q.

Программная реализация нахождения λ продемонстрирована на рисунке 3.

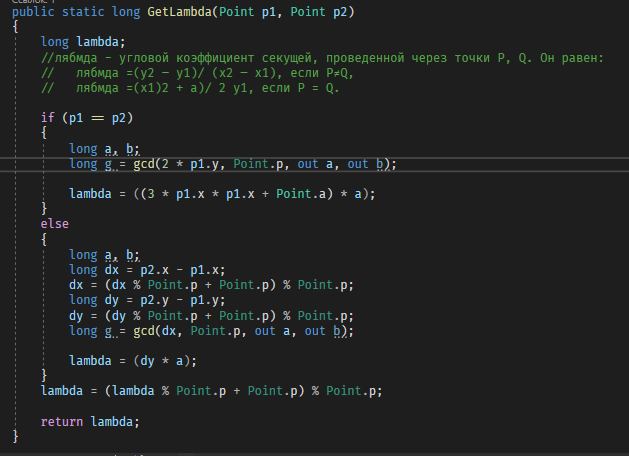


Рис. 3 – Нахождение λ

Далее предположим, что точка P имеет координаты (x1, y1), тогда Q (x2,y2), R(x3, y3) – сумма точек P и Q. Тогда координаты точки R вычисляются по формулам:

x3= λ 2 – х1 – х2

у3= λ (х1–х3 ) – у1

Программная реализация сложения двух точек ЭК продемонстрирована на рисунке 4.

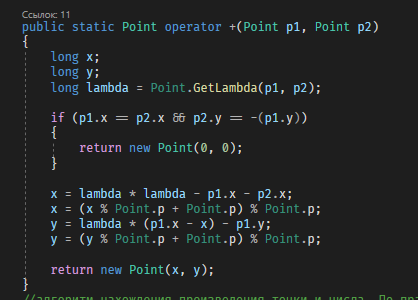


Рис. 4 – Сложение точек ЭК

Далее рассмотрим алгоритм нахождения произведения точки и числа. По правилу умножения точки ЭК, для умножения Pz необходимо точку Р сложить саму с собой z раз. Программная реализация данной операции приведена на рисунке 5.

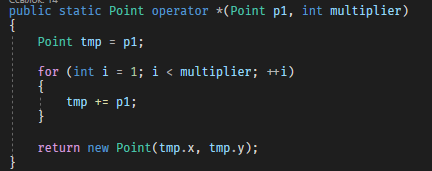


Рис. 5 – Умножение точки на число

Также в указанных вычислениях необходимо было применять сложение с инверсией: инверсией по отношению к точке (x,y) является точка (x,-y) на ЭК.

Результаты вычислений указанных в задании выражений по выше упомянутым формулам, представлен на рисунке 6.

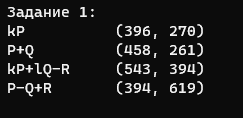


Рис. 6 – Результаты вычислений\

**Задание 2**

Генерирующая точка G = (0,1). Тайный ключ d = 50. Параметр k = 11.

Также примем к сведению, что шифруемым блоком является один символ сообщения, координаты которого представлены в таблице 1.

Таблица 1 – Координаты символа

|  |  |
| --- | --- |
| Ш | (198, 224) |
| А | (200, 721) |
| Г | (227, 452) |

Для реализации зашифрования и расшифрования применим алгоритм Эль-Гамаля. 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.

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.

Программная реализации процесса зашифрования представлена на рисунке 7.

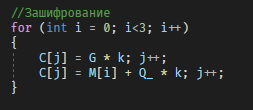


Рис. 7 – Зашифрование в ЭК

Получатель для расшифрования сообщения вычисляет:

P = С2 – dC1.

Программная реализация расшифрования представлена на рисунке 8.

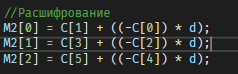


Рис. 8 – Расшифрование в ЭК

Результаты проделанных выше операций представлены на рисунке 9.

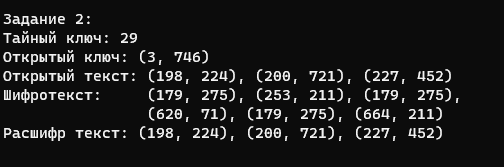


Рис. 9 – Результат зашифрования/расшифрования

Открытый ключ Q = G\*d, где G – генерирующая точка, d – тайный ключ. Как упоминалось ранее, на рисунке видно, что одному символу исходного открытого текста соответствует два символа шифротекста. Именно поэтому их количество – 6.

Как видно из рисунка 9, открытый и расшифрованный тексты совпадает, что говорит о корректной работе разработанного приложения.

**Задание 3**

Приложение написано на языке программирования C# и реализует следующие операции:

* генерация ЭЦП на основе алгоритма ECDSA;
* верификация ЭЦП на основе алгоритма ECDSA.

## Методика выполнения поставленных задач

Примем следующие значения: ЭК Е751(–1, 1) c генерирующей точкой G = (416, 55); порядок точки q = 13. Тайный ключ d = 29.

Вычислим самостоятельно открытый ключ Q по формуле: Q = dG (mod 751).

Хешем подписываемого сообщения, (Н(М)), является модуль по основанию 13 координаты х точки ЭК, соответствующей первому символу собственной фамилии. Т.е., для фамилии «ПАРИБОК» хэшу сообщения будет соответствовать абсцисса по модулю 13 точки «П» (205, 379): x = 205, тогда 205 mod 13 = 10.

## 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).

Программная реализация алгоритма генерации ЭЦП представлена на рисунке 10.

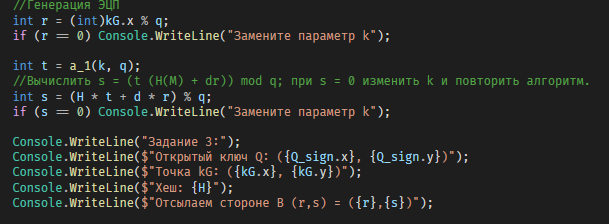


Рис 10– Генерация ЭЦП

## 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.

Программная реализация верификации ЭЦП представлена на рисунке 11.

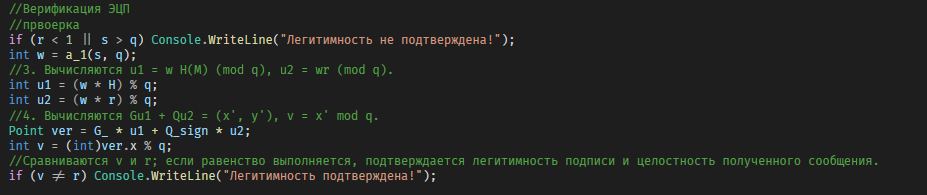


Рис. 11 – Верификация ЭЦП

Результат генерации и верификации ЭЦП представлен на рисунке 12.

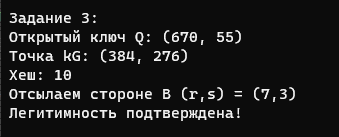


Рис. 12 – Результат генерации/верификации ЭЦП

Как видно из рисунка, легитимность подписи и целостность полученного сообщения подтверждены.

**Вывод** Исследование показало, что криптографические алгоритмы на основе эллиптических кривых обеспечивают высокий уровень безопасности при низкой вычислительной сложности. Применение эллиптических кривых в криптографии предоставляет эффективный способ обеспечения целостности и аутентификации данных через эллиптический цифровой подпись (ECDSA) и безопасный обмен секретными ключами через эллиптический диффициальный обмен ключами (ECDH). Важным аспектом обеспечения безопасности системы является правильный выбор алгоритмов и параметров эллиптических кривых, а также внимательное изучение и понимание их математических основ и рекомендаций по безопасности. В результате, исследование криптографических алгоритмов на основе эллиптических кривых может привести к созданию надежных систем защиты информации с высоким уровнем безопасности и эффективностью.

**Контрольные 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).

y^2= x^3+ax+b

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

Сложение точек: Сложение двух точек на эллиптической кривой определяется следующим образом: сначала проводится линия, проходящая через две точки, затем она пересекает кривую в третьей точке, и результатом сложения является эта третья точка.

Пример: P1 = (1,2) P2 = (2,3) P3 = P1 + P2

Для нахождения P3 проводится линия, проходящая через точки P1 и P2, которая пересекает кривую в третьей точке. Результатом будет новая точка на кривой: P3 = (3, -1)

Удвоение точки: Удвоение точки на эллиптической кривой определяется следующим образом: проводится касательная к кривой в данной точке, и она пересекает кривую во второй точке. Результатом удвоения является эта вторая точка.

Пример: P1 = (1,2) P2 = 2P1

Для нахождения P2 проводится касательная к кривой в точке P1, которая пересекает кривую во второй точке. Результатом будет новая точка на кривой: P2 = (1, -2)

Умножение точки на число: Умножение точки на число на эллиптической кривой определяется как последовательное сложение точки с самой собой определенное количество раз. Например, для умножения точки на число 3, необходимо выполнить сложение точки с самой собой три раза. Пример: P1 = (1,2) P2 = 3P1

Для нахождения P2 нужно выполнить сложение точки P1 с самой собой три раза: P2 = P1 + P1 + P1 = (1,2) + (1,2) + (1,2) = (2,1) + (1,2) = (2,-1)

Результатом является новая точка на кривой.

4. Что такое «рациональная точка»?

В математике, особенно в геометрии, "рациональная точка" - это точка, координаты которой могут быть выражены рациональными числами, т.е. числами, которые могут быть представлены в виде дробей с целыми числителем и знаменателем. Другими словами, если точка на графике может быть определена парой рациональных чисел (x, y), то эта точка является рациональной.

5. Как производится умножение точки ЭК?

Берется точка P, и после этого смотрим коэффициент, на который будем умножать. Далее представляем этот коэффициент в виде степеней двойки: например, 78P = 64P + 8P + 4P + 2P. А дальше выполняем операции сложения точек, где P = Q и где P ≠ Q.

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

2P = P + P.

5P = 4P + P

11P = 8P + 2P + P

20P = 16P + 4P

32P

100P = 64P + 32P + 4P

256P

751P = 512P + 128P + 64P + 32P + 8P + 4P + 2P + P

1024P

А дальше выполняем операции сложения точек, где P = Q и где P ≠ Q

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

Алгоритм многократного сложения точки ЭК заключается в следующих шагах:

1) Инициализация результирующей точки как точки на бесконечности

2) Представление множителя в двоичном виде

3) Перебор битов множителя справа налево

4) Если текущий бит множителя равен 1, добавить текущую точку к результирующей точке

5) Удвоить текущую точку на каждой итерации

6) Повторять шаги 4-5 для каждого бита множителя

7) Вернуть результирующую точку

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

Для точки Q, где d = 4 и G = (2, 22) на кривой Е67(2, 3), используем формулу для умножения точки на число: Q = dG = 4G = 2G + 2G = (35, 1) + (35, 1) + (35, 1) + (35, 1) = (13, 45)

Теперь, если точка Р = (24, 26) и k = 2, то используем формулы для шифрования и расшифрования:

Шифрование: С1 = kG = 2G = (35, 1) C2 = P + kQ = (24, 26) + 2(13, 45) = (24, 26) + (12, 23) = (21, 44)

Таким образом, шифртекст состоит из двух точек: С1 = (35, 1), С2 = (21, 44).

Расшифрование: Сначала сторона В вычисляет dC1 = 4C1 = 4(35, 1) = (23, 25) Затем инвертирует точку (23, 25) и находит (23, 42), поскольку -25 mod 67 = 42. Наконец, выполняет сложение точки С2 и (23, 42) в соответствии с (11.10): C2 + (23, 42) = (21, 44) + (23, 42) = (24, 26), что соответствует исходной точке Р, т.е. сообщению М.

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

Да. Операции над точками на эллиптических кривых над конечными полями используются для решения задач криптографии, в то время как операции над точками на эллиптических кривых над действительными числами используются в геометрии.

Основная разница между ними заключается в том, что в криптографии операции над точками ЭК над конечными полями производятся в модульной арифметике, в то время как в геометрии операции над точками производятся в вещественной арифметике.

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

y^2= x^3+ax+b (mod p)

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

q = 11 + 1 - t,

где t – порядок кривой. След кривой определяется как сумма координат точек на кривой (включая бесконечно удаленную точку).

Для вычисления следа кривой необходимо решить уравнение:

t^2 - 4q = -35,

где q = 11 + 1 - t.

Решая данное уравнение, получим:

t = 7, q = 3.

Следовательно, количество точек на кривой E11(6, -9) равно 3.

Точки на кривой могут быть найдены путем решения уравнения кривой:

y^2 = x^3 + 6x - 9

для всех возможных значений x в поле GF(11). Некоторые из точек на кривой имеют координаты:

(2, 5), (2, 6), (6, 7)

12. Найти все точки ЭК Е11(1, 2).

y^2 = x^3 + x + 2 (mod 11)

Для нахождения всех точек ЭК можно использовать переборный метод, подставляя значения x и вычисляя соответствующие значения y.

Применяя переборный метод, можно получить следующие точки:

(0, 4), (0, 7), (1, 2), (1, 9), (4, 0), (4, 11), (5, 3), (5, 8), (9, 1), (9, 10), (10, 1), (10, 10).

Здесь 11 - порядок поля, а точки записываются в виде (x, y).

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

Криптостойкость систем на основе эллиптических кривых основана на трудности решения задачи дискретного логарифмирования в конечных полях, которая является аналогом задачи факторизации больших чисел в RSA. Для ЭК задача дискретного логарифмирования заключается в нахождении значения x в уравнении P = x \* G, где P и G - точки на кривой, а x - целое число. Для большинства кривых ЭК эта задача является вычислительно сложной и не решаемой за разумное время на современных компьютерах.

Области применения эллиптических кривых в криптографии включают в себя:

- Алгоритмы электронной подписи (ECDSA, EdDSA)

- Схемы обмена ключами (ECDH)

- Криптография на основе идентификации (ECIES)

- Протоколы аутентификации и анонимного обмена сообщениями (ECKAS и др.)

- Различные применения в защите данных и авторизации в Интернете в рамках стандартов SSL/TLS, SSH, IPSec и др.

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

Порядок точки на эллиптической кривой (ЭК) – это количество точек, которые можно получить, последовательно складывая заданную точку с самой собой, пока не будет получена точка в бесконечности. Формально, порядок точки P на ЭК определяется как минимальное число n, такое что nP = O (где O – точка в бесконечности).

Порядок точки играет важную роль в криптографии на основе ЭК, так как он определяет сложность вычислений для нахождения дискретного логарифма. Например, если порядок точки на ЭК большой простой чисел, то вычисление дискретного логарифма становится вычислительно сложной задачей, что делает систему на основе ЭК криптостойкой. Также порядок точки используется для определения размера ключа в системах шифрования на основе ЭК.

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

Базовая точка (или точка генерации) на эллиптической кривой (ЭК) - это фиксированная точка, которая используется для генерации всех других точек на кривой. Обозначается символом G.

Роль базовой точки в криптографии на основе ЭК заключается в том, что она позволяет генерировать случайные ключи шифрования и подписи. В частности, для генерации ключей шифрования используется операция умножения точки на случайное число (секретный ключ), которое приводит к получению другой точки на кривой. Для генерации цифровых подписей также используется умножение точки на число, но уже соответствующее хэшу сообщения.

16. Объяснить порядок формирования ключевой информации на основе ЭК.

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 *РА* = *kA* *Q* и отправляет ее получателю *B*. B действует аналогично: он случайным образом выбирает число *kB*, вычисляет случайное число *kA*, вычисляет точку *РВ* = *kВQ* и отправляет результат стороне *A*.

Общий ключ *P* = *kAkBQ*. Отправитель *A* вычисляет *P* путем умножения числа *РВ*, полученного от получателя *B*, на его секретное число *kA*. Похожим образом действует другая сторона.

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

Допустим, базовая точка на кривой Е11(1, 2) имеет координаты G = (3, 2), а ее порядок равен n = 19.

1) Выберем случайное число k = 10.

2) Вычислим точку Q = k \* G: Q = 10 \* G = G + G + G + G + G + G + G + G + G + G = = (3, 2) + (3, 2) + (3, 2) + (3, 2) + (3, 2) + + (3, 2) + (3, 2) + (3, 2) + (3, 2) + (3, 2) = = (6, 15)

3) Открытый ключ: (x\_Q, y\_Q) = (6, 15).

4) Закрытый ключ: k = 10.