Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и
теории чисел

ЭЛЛИПТИЧЕСКИЕ КРИПТОСИСТЕМЫ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

Студента 4 курса 421 группы
направления 010200 — Математика и компьютерные науки
Механико-математического факультета
Каймашникова Всеволода Александровича

Научный руководитель
доцент, к. ф.-м. н. _____ В. В. Кривобок

Заведующий кафедрой
Профессор, доктор _____ В. Н. Кузнецов

Саратов 2015

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Средства и системы криптографической защиты информации играют важную роль в современных компьютерных информационных системах, используемых в сфере финансовой и коммерческой деятельности. Интерес к ним обусловлен не только возрастающими общественными потребностями в переводе экономических и государственно-правовых отношений на 'электронную основу', но и сильно расширившимися возможностями передачи, обработки и хранения информации в распределенных вычислительных системах. Применение специальных криптографических протоколов и криптосистем позволяет осуществлять многообразные экономические отношения 'дистанционно', исключая необходимость личной встречи участников этих отношений, а также поддерживать при этом должную финансовую и правовую дисциплину.

В 1985 году Нил Коблиц и Виктор Миллер независимо предложили использовать в криптографии некоторые алгебраические свойства эллиптических кривых. С этого момента началось бурное развитие нового направления в криптографии, для которого используется термин криптография на эллиптических кривых (Elliptic Curve Cryptography, сокращенно ECC). Криптосистемы с открытым ключом на эллиптических кривых обеспечивают такую же функциональность, как и алгоритм RSA. Однако их криптостойкость основана на другой проблеме, а именно на проблеме дискретного логарифма в группе точек эллиптической кривой (Elliptic Curve Discrete Logarithm Problem, сокращенно ECDLP). В настоящее время лучшие алгоритмы для решения ECDLP имеют экспоненциальное время работы, в отличие от алгоритмов для решения проблемы простого дискретного логарифма и проблемы факторизации целого числа, которые имеют субэкспоненциальное время ра-

боты.

Эллиптические кривые являются одним из основных объектов изучения в современной теории чисел и криптографии. Эллиптическая криптография образует самостоятельный раздел криптографии, посвященный изучению криптосистем на базе эллиптических кривых.

Данная работа посвящена рассмотрению основных протоколов шифрования на эллиптических кривых. В первой главе будут изложены основные факты из алгебры, теории чисел и теории криптографии. Во второй главе будут изложены основные факты из теории эллиптических кривых, которые необходимо знать для построения эллиптических криптосистем и подтверждения их криптостойкости, которая основана на задаче дискретного логарифма. В третьей главе приведены основные протоколы шифрования на эллиптических кривых, описаны возможные атаки и детали выбора параметров для эллиптической кривой для реализации на ЭВМ. В качестве практической части (Приложение А) реализован программный модуль для сложения точек эллиптической кривой неписаный на языке программирования Java.

Основным преимуществом эллиптической криптографии является малый размер ключа относительно других схем асимметричного шифрования (например RSA). Это свойство особенно важно при реализации криптографических протоколов в условиях ограниченности ресурсов памяти и производительности, например при программировании смарт-карт. Также ясно, что с улучшением производительности компьютеров шифры постепенно будут становиться все более уязвимыми при малых длинах ключа.

А с увеличение длины ключа преимущества схем на эллиптических кривых над другими схемами шифрования возрастает многократно. За счет меньшей длины ключа возрастает и эффективность вычислительных процессов.

1 Основные понятия

1.1 Основные определения алгебры

Определение 1. *Множество R называется кольцом, если в нём определены две операции — сложение и умножение, обе коммутативные и ассоциативные, а также связанные законом дистрибутивности, причём сложение обладает обратной операцией — вычитанием.*

Определение 2. *Абелева (или коммутативная) группа — группа, в которой групповая операция является коммутативной; иначе говоря, группа $(G, +)$ абелева, если $a + b = b + a$ для любых двух элементов $a, b \in G$.*

Определение 3. *Пусть R — произвольное кольцо. Если существует такое целое положительное число n, что для каждого элемента $r \in R$ выполняется равенство*

$$n \cdot r = \underbrace{r + \cdots + r = 0}_{n} ,$$

то наименьшее из таких чисел n называется характеристикой кольца R и обозначается $charR$. При этом кольцо R называется кольцом положительной характеристики $charR$.

Если же таких чисел n не существует, то полагают $charR = 0$ и называют R кольцом характеристики нуль. В случае, если кольцо R содержит единицу, определение несколько упрощается. В этом случае характеристику обычно определяют как наименьшее ненулевое натуральное число n такое, что $n \cdot 1 = 0$, если же такого n не существует, то характеристика равна нулю.

Определение 4. *Конечное поле или поле Галуа — поле, состоящее из конечного числа элементов*

Определение 5. *Китайская теорема об остатках. Пусть* $n_1, n_2, \cdots, n_k$ *— натуральные попарно взаимно простые числа, а* $r_1, r_2, \cdots, r_k$ *— некоторые целые числа, тогда существует такое целое число* M*, что оно будет решением системы сравнений:*

$$\begin{cases} M \equiv r_1 \ (mod\ n_1), \\ M \equiv r_2 \ (mod\ n_2), \\ \cdots, \\ M \equiv r_n \ (mod\ n_n), \end{cases}$$

При этом для любых двух решений A *и* B *этой системы справедливо* $A \equiv B \ (mod\ n_1 n_2 \cdots n_k)$*, то есть решение системы сравнений существует и единственно по модулю* $n_1 n_2 \cdots n_k$*.*

1.2 Основные сведения криптографии

Криптография изучает методы пересылки сообщений в замаскированном виде, при которых только намеченные отправителем получатели могут удалить маскировку прочитать сообщение.

Определение 6. *Предназначенное для пересылки сообщение называется открытым текстом, а замаскированное сообщение шифрованным текстом или кратко шифртекстом.*

Открытый текст и шифртекст записываются в некоторых алфавитах; обычно, но не всегда, эти алфавиты совпадают и состоят из некоторого числа N букв. Термин «буква» (или «символ») может относится не только к обычным буквам, но также к цифрам, к пробелам, к знакам пунктуации и ко всяким другим символам, используемым при записи сообщения. (Если мы не включим, например, пробелы, то все слова слипнутся и сообщение будет

трудно читать.)

Определение 7. *Процесс преобразования открытого текста в шифртекст называется шифрованием (или зашифрованием), а обратная процедура называется дешифрованием расшифрованием).*

Открытый и шифрованный тексты разбиваются на элементарные сообщения («элементы»). Элементом может быть отдельная буква, пара букв (биграмма), тройка букв (триграмма) или даже блок из 50 букв.

Определение 8. *Шифрующее преобразование является функцией, которая преобразует элемент открытого текста в элемент шифртекста. Другими словами, это — отображение f из множества P всех возможных элементов открытого текста в множество C всех возможных элементов шифртекста.*

Будем всегда предполагать, что это отображение взаимно однозначное, т. е. для одного элемента шифртекста существует один и только один элемент открытого текста, из которого элемент шифртекста получается при шифровании. Дешифрующее преобразование действует в обратном направлении, это — функция f^{-1} восстанавливающая открытый текст по шифртексту. Всю эту ситуацию можно схематически изобразить диаграммой

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P.$$

Любая такая конструкция называется криптосистемой.

На самом деле термин «криптосистема» чаще применяется к целому семейству таких преобразований, зависящих от выбора некоторых параметров (от них могут зависеть как отображение f, так и множества P и C). Шифрующее преобразование можно задать: алгоритмом, единым для всего

семейства, и значениями параметров. Значения параметров называются ключом шифрования K_E. На практике считается, что алгоритм известен (т.е. общий вид процедуры шифрования сохранить в тайне нельзя). Однако ключи легко меняются и, если это необходимо, держатся в секрете. Для дешифрования (т.е. вычисления f^{-1}) также необходимы алгоритм и ключ. Этот ключ называется ключом дешифрования K_D.

Определение 9. *Под классической криптосистемой (иначе, системой с секретным ключом или симметричной криптосистемой понимается криптосистема, в которой, имея информацию о преобразовании шифрования, можно реализовать преобразование дешифрования примерно за такое же время, что и преобразование шифрования.*

Определение 10. *Криптографическая система с открытым ключом — система шифрования и/или электронной цифровой подписи, при которой открытый ключ передаётся по открытому каналу и используется для шифрования сообщения и проверки электронной подписи. Для расшифровки сообщения и для генерации электронной цифровой подписи используется закрытый ключ*

По определению, криптосистема с открытым ключом обладает тем свойством, что знание шифрующего преобразования не позволяет по ключу шифрования найти ключ дешифрования, избежав чрезвычайно длинных вычислений. Другими словами, шифрующая функция $f : P \to C$ легко вычисляется, если ключ шифрования K_E известен, но вычислять значения обратной функции $f^{-1} : C \to P$ очень сложно. С точки зрения практической вычислимости это значит, что функция f^{-1} необратима (без дополнительной информации — ключа дешифрования K_D). Таким образом, функция f — это легко вычислимая функция, для которой обратную функцию f^{-1} вы-

числить трудно, если не иметь некоторой дополнительной информации сверх той, что используется при вычислении f. Обратная функция f^{-1} , однако, легко вычислима, если известна дополнительная информация K_D — ключ дешифрования.

Примерами таких криптосистем являются криптосистема на эллиптических кривых благодаря проблеме дискретного логарифма в группе точек эллиптической кривой (Elliptic Curve Discrete Logarithm Problem, сокращенно ECDLP) и криптосистема RSA, в которой стоит сложная задача факторизации больших чисел.

Электронная подпись

Часто одной из наиболее важных частей сообщения является подпись. Если сообщение имеет особенную важность, могут потребоваться дополнительные способы заверения подлинности сообщения. А в электронных средствах связи, где нельзя передать физическую подпись, приходится полагаться совершенно на другие методы.

Криптография с открытым ключом предоставляет простое решение этой задачи. Пусть A (Алиса) и B (Боб) — два пользователя системы. Пусть f_A – шифрующее преобразование, которым должен воспользоваться любой, кто отправляет сообщение Алисе, а f_B — соответствующее преобразование для Боба. Для простоты считаем, что множества P и C элементов открытого и шифрованного текстов совпадают и одинаковы у всех пользователей. Пусть P – подпись Алисы (включающая в себя, возможно, идентификационный номер Алисы, время отправления сообщения и т.п.). Если Алиса просто пошлет Бобу некоторое сообщение $f_B(P)$, то (поскольку способ вычисления $f_B(P)$ общеизвестен) нет способа проверки, гарантирующего, что подпись принадлежит Алисе. Однако, если в начале или конце сообщения будет помещено

$f_B f_A^{-1}$(P), то Боб, применив f_B^{-1} , дешифрует сообщение, включая этот добавок, и все превратится в открытый текст, за исключением добавка, который примет вид f_A^{-1}(P). Так как Боб знает, что сообщение должно было быть послано от Алисы, то он применит к добавку f_A (ключ Алисы открыт и ему известен) и получит P. Так как никто, кроме Алисы, не может воспользоваться функцией f_A^{-1} , обратной к f_A, то он удостоверяется в том, что сообщение послано Алисой.

2 Теория эллиптических кривых

2.1 Основные факты

В этом параграфе мы предполагаем, что $K-$ поле: либо поле $\mathbb{R}$ вещественных чисел, либо поле $\mathbb{Q}$ рациональных чисел, либо поле $\mathbb{C}$ комплексных чисел, либо поле F_q из $q = p^r$ элементов, где p простое.

Определение 11. *Пусть K – поле характеристики, отличной от 2, 3, и $x^3 + ax + b$ (где $a, b \in K$) – кубический многочлен без кратных корней. Эллиптическая кривая над* K *– это множество точек $(x, y), x, y \in K$, удовлетворяющих уравнению*

$$y^2 = x^3 + ax + b \tag{1}$$

вместе с единственным элементом, обозначаемым O и называемым 'точка в бесконечности'.

Если K – поле характеристики 2, то эллиптическая кривая над K – это множество точек, удовлетворяющих уравнению либо типа

$$y^2 + cy = x^3 + ax + b, \tag{2}$$

либо типа

$$y^2 + xy = x^3 + ax^2 + b \tag{3}$$

(здесь кубические многочлены в правых частях могут иметь кратные корни), вместе с 'точкой в бесконечности' O.

Если K – поле характеристики 3, то эллиптическая кривая над K – это множество точек, удовлетворяющих уравнению

$$y^2 = x^3 + ax^2 + bx + c \tag{4}$$

(здесь кубические многочлены в правых частях могут иметь кратные корни), вместе с 'точкой в бесконечности' O.

Предложение 1. *Имеется общая форма уравнения эллиптической кривой, которая применима при любом поле:*

$$y + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

В случае, когда $charK \neq 2$, *ее можно привести к виду*

$$y^2 = x^3 + ax^2 + bx + c$$

или к виду

$$y^2 = x^3 + bx + c,$$

если $K > 3$. *В случае, когда поле* K *имеет характеристику* 2, *это уравнение преобразуется либо к виду 2), либо к виду 3).*

Отметим чрезвычайно важное свойство множества точек эллиптической кривой: они образуют аддитивную абелеву группу.

Теорема 1. *Морделла. Точки эллиптической кривой на полем* $\mathbb{Q}$ *рациональных чисел –* $E(\mathbb{Q})$ *образуют конечно порожденную абелеву группу.*

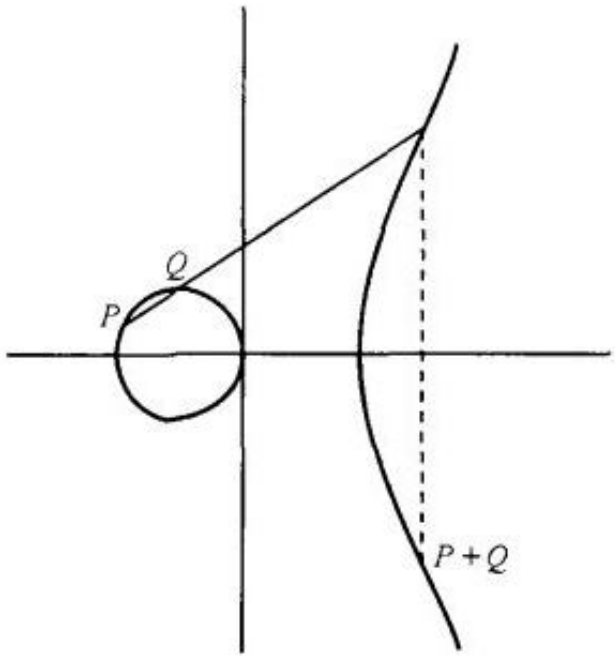
Чтобы объяснить наглядно, как это получается, временно будем полагать, что $K = \mathbb{R}$, т.е. что эллиптическая кривая – обычная плоская кривая (с добавлением еще одной точки O 'в бесконечности').

Определение 12. *Точка в бесконечности O — это тождественный элемент группового (группа точек эллиптической кривой) закона.*

Определение 13. *Пусть E — эллиптическая кривая над вещественными числами, и пусть P и Q — две точки на E. Определим точки $-P$ и $P+Q$ по следующим правилам.*

1. *Если P — точка в бесконечности O, то $-P = O$ и $P+Q = Q$, т.е. O — тождественный элемент по сложению ('нулевой элемент') группы точек. В следующих пунктах предполагается, что ни P, ни Q не являются точками в бесконечности.*
2. *Точки $P = (x, y)$ и $-P$ имеют одинаковые x-координаты, а их y-координаты различаются только знаком, т.е. $-(x, y) = (x, -y)$. Из 1 сразу следует, что $(x, -y)$ — также точка на E.*
3. *Если P и Q имеют различные x-координаты, то прямая $l = \overline{PQ}$ имеет с E еще в точности одну точку пересечения R (за исключением двух случаев: когда она оказывается касательной в P, и мы тогда полагаем $R = P$, или касательной в Q, и мы тогда полагаем $R = Q$). Определяем теперь $P + Q$ как точку $-R$, т.е. как отражение от оси x третьей точки пересечения. Геометрическое построение, дающее $P + Q$, приводится ниже в примере 1.*
4. *Если $Q = -P$ (т.е. x-координата Q та же, что и у P, а y-координата отличается лишь знаком), то полагаем $P + Q = O$ (точке бесконечности; это является следствием правила 1).*
5. *Остается возможность $P = Q$. Тогда считаем, что l — касательная к кривой в точке P. Пусть R — единственная другая точка пересечения l с E. Полагаем $P + Q = -R$ (в качестве R берем P, если касательная прямая в P имеет 'двойное касание', т.е. если P есть точка перегиба кривой).*

Пример 1. *В соответствии с рисунком ниже изображены эллиптическая кривая* $y^2 = x^3 - x$ *в плоскости* xy *и типичный случай сложения точек* P *и* Q*. Чтобы найти* $P + Q$*, проводим прямую* PQ *и в качестве* $P + Q$ *берем точку, симметричную относительно оси* x *третьей точке, определяемой пересечением прямой* PQ *и кривой. Если бы* P *совпадала с* Q*, т.е. если бы нам нужно было найти* $2P$*, мы использовали бы касательную к кривой в* P*; тогда точка* $2P$ *симметрична третьей точке, в которой эта касательная пересекает кривую.*



2.2 Арифметика

F_q^* – мультипликативная группа конечного поля. Для эллиптических кривых аналогом умножения двух элементов группы F_q^* служит сложение двух точек эллиптической кривой E, определенной над F_q^*. Таким образом, аналог возведения в степень k элемента из F_q^* – это умножение точки $P \in E$ на целое число k.

Определим операцию сложения двух точек эллиптической кривой алгебраически. Запишем $P + Q = -R$.

Пусть координатами точки P будут (x_P, y_P), а координатами точки Q соответственно (x_Q, y_Q).

$$x_{P+Q} = \lambda^2 - x_P - x_Q$$

$$y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P,$$

где

$$\lambda = (y_P - y_Q)/(x_P - x_Q),\ P \neq Q$$

$$\lambda = (3x_P^2 + a)/(2y_P),\ P = Q,$$

где a коэффициент при x в правой части уравнения 1

Пример 2. *Чтобы найти* $100P$*, записываем*

$$100P = 2(2(P + 2(2(2(P + 2P)))))$$

и приходим к цели, производя 6 *удвоений и* 2 *сложения точек на кривой.*

Определение 14. *Точки конечного порядка.*

Порядком N *точки* P *на эллиптической кривой называется такое наименьшее натуральное число, что* $NP = 0$*; конечно, такого конечного* N *может и не существовать.*

Пример 3. *Найти порядок точки* $P = (2, 3)$ *на* $y^2 = x^3 + 1$.

Решение. Находим из арифметических формул на эллиптической кривой, что $2P = (0, 1)$ *и* $4P = 2(2P) = (0, -1)$. *Поэтому* $4P = -2P$ *и, следовательно,* $6P = 0$. *Тем самым порядок* P *может быть равен* 2, 3 *или* 6. *Но* $2P = (0, 1) \neq 0$, *а если бы* P *имела порядок* 3, *то было бы* $4P = P$, *что неверно. Итак,* P *имеет порядок* 6.

Отметим следующие важные определения:

Определение 15. *Пусть* G *— конечная группа,* b *— элемент группы* G *и* y *— элемент группы* G, *являющийся степенью* b. *Любое целое число* x, *для которого* $b^x = y$, *называется дискретным логарифмом* y *по основанию* b.

Определение 16. *Пусть* E *— эллиптическая кривая над* F_q *и* B *— точка на* E. *Задачей дискретного логарифмирования на* E *(с основанием* B*) называется задача нахождения для данной точки* $P \in E$ *такого целого числа* $x \in Z$ *(если оно существует), что* $xB = P$.

Именно из-за наличия задачи дискретного логарифмирования, эллиптические криптосистемы имеют высокую криптостойкость. Но стоит отметить, что не все эллиптические кривые подходят для использования.

2.3 Выбор кривой и точки

Существуют различные способы выбора эллиптической кривой и (в системах Диффи-Хеллмана и Эль-Гамаля о которых будет рассказано в следующей главе) точки B на ней.

Случайный выбор (E, B). Взяв какое-либо большое конечное поле F_q, можно следующим образом осуществить одновременный выбор E и $B = (x, y) \in E$. Будем предполагать, что характеристика p поля F_q больше 3, так что эллиптическая кривая задана уравнением 1; при $q = 2^r$ или 3^r нетрудно

сделать очевидные изменения в дальнейшем изложении. Выбираем сначала случайным образом три элемента из F_q^* в качестве x, y, a. Далее полагаем $b = y^2-(x^3+ax)$. Убеждаемся в том, что кубический многочлен x^3+ax+b не имеет кратных корней, что равносильно проверке условия $4a^3 + 27b^2 \neq 0$. Если это условие не выполняется, берем другую случайную тройку x, y, a. Полагаем $B = (x, y)$. Тогда B – точка, на эллиптической кривой $y^2 = x^3 + ax + b$.

Для нахождения асимптотики N количества точек эллиптической рассмотри следующую теорему

Теорема 2. *Хассе. Пусть N – число точек эллиптической кривой, определённой над F_q. Тогда*

$$|N - (q + 1)| \leq 2\sqrt{q}$$

Подведём небольшой итог по главе. Отметим важные факты из теории эллиптических кривых. Точки эллиптической кривой образуют аддитивную абелеву группу и для эллиптической кривой есть задача дискретного логарифмирования на эллиптических кривых, что обеспечивает криптостойкость, т.к. на данный момент не найдено быстрых алгоритмов способных решать эту задачу. Но стоит знать, что не все эллиптически кривые подходят, т.к. задача дискретного логарифма для некоторых упрощается и становится решаемой за субэкспоненциальное время. Подробнее об этом будет рассказано в следующей главе. За более подробным изложением информации по первой главе следует обратится к источникам литературы: [2], [3], [4], [5], [7], [11], [12].

3 Криптосистемы на эллиптических кривых

Отметим важную деталь. Рассмотрение эллиптических кривых, например, над вещественными числами или любым другим полем, отличным от конечного, приводит нас к проблемам. Например в случае вещественного поля — это округление, т.е. используя кривые над вещественными числами, мы не сможем получить биекцию между исходным текстом и зашифрованными данными. Чтобы избежать проблемы с округлением и ей подобных в случае кривых над другими полями, в криптографии используются только кривые над конечными полями. Это означает, что под эллиптической кривой понимается набор точек, чьи координаты принадлежат конечному полю.

В криптографии рассматривается два вида эллиптических кривых: над конечным полем $\mathbb{Z}_p$ — кольцо вычетов по модулю простого числа. И над полем $GF(2^m)$ — бинарное конечное поле. У эллиптических кривых над полем $GF(2^m)$ есть одно важное преимущество, элементы поля могут быть легко представлены в виде $n-$битных кодовых слов, это позволяет увеличить скорость аппаратной реализации эллиптических алгоритмов.

Все математические операции на эллиптических кривых над конечным полем производятся по законам конечного поля над которым построена эллиптическая кривая. Т.е. для вычисления, например, суммы двух точек кривой $E(\mathbb{Z}_p)$ над кольцом вычетов все операции производятся по модулю числа p.

Однако здесь есть один нюанс. Если мы сложим два одинаковых элемента из бинарного конечного поля, то получим в результате 0, т.к. сложение происходит по модулю 2. Это означает что характеристика такого поля

равна 2. Но эллиптическая кривая вида

$$y^2 = x^3 + ax + b$$

описанная над полем характеристики 2 или 3 становится сингулярной, а как уже замечалось выше в главе про эллиптические кривые это неудачная идея использовать сингулярные кривые в криптографии.

Поэтому над бинарным конечным полем используются кривые вида:

$$y^2 + xy = x^3 + ax^2 + b,\ b \neq 0$$

Напомним важное понятие эллиптической криптографии – порядок эллиптической кривой, который показывает количество точек кривой над конечным полем. И воспользуемся Теоремой Хассе для определения асимптотики порядка эллиптической кривой над бинарным конечным полем. Т.к. бинарное конечное поле $GF(2^n)$ состоит из 2^n элементов, мы можем показать, что порядок эллиптической кривой равен

$$E_{2^n}(a, b) = 2^n + 1 - t,\ |t| \leq 2\sqrt{2^n}$$

С числом t связано определение суперсингулярной эллиптической кривой:

Определение 17. *Эллиптическая кривая над бинарным конечным полем называется суперсингулярной, если t делится на характеристику поле(в случае бинарного поля характеристика равна 2) без остатка.*

Определение 18. *Кривая называется сингулярной (особой), если существует хотя бы одна точка (x, y) в которой частные производные по функции $F(x, y) = y^2 - x^3 - ax - b$ равны нулю*

Вспомним два важных факта. Первый: точки эллиптической кривой над конечным полем представляют собой аддитивную абелеву группу. И как мы отмечали выше для этой группы определена операция сложения(см. раздел Арифметика). Соответственно мы можем представить умножение числа k на точку G как $G + G + \cdots + G$ с k слагаемыми.

Теперь представим, что у нас имеется сообщение M представленное в виде целого числа. Мы можем зашифровать его используя выражение $C = M \cdot G$. Вопрос в том, насколько сложно восстановить M зная параметры кривой $E(a, b)$, шифротекст C и точку G. Второй факт: данная задача называется дискретным логарифмом на эллиптической кривой и не имеет быстрого решения. Более того, считается, что задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях. Наиболее быстрые методы, разработанные для конечных полей оказываются бесполезны в случае эллиптических кривых.

Так для решения дискретного логарифма существуют достаточно быстрые алгоритмы имеющие сложность $O(exp(c(logploglogp)^d))$, где c и d $-$ некоторые константы, а p $-$ размер поля. Такие алгоритмы называются субэкспоненциальными и позволяют сравнительно легко вскрывать дискретный логарифм в конечном поле, если размер поля не выбран очень большим, порядка 2^{1024}. В тоже время наиболее быстрые методы решения дискретного логарифма на эллиптической кривой имеют сложность $O(\sqrt{q})$, где q $-$ количество точек эллиптической кривой.

Следует, заметить, что поскольку мощность вычислительной техники постоянно повышается, значение q будет постоянно увеличиваться. Но так как графики функций $O(exp(c(logploglogp)^d))$ и $O(\sqrt{q})$ резко отличаются друг от друга, в группе точек эллиптической кривой q будет расти намного

медленнее, чем в произвольном конечном поле.

Рассмотрим некоторые варианты атак на эллиптические криптосистемы.

1. Алгоритм Полига — Хеллмана (также называемый алгоритм Сильвера — Полига — Хеллмана) — детерминированный алгоритм дискретного логарифмирования в кольце вычетов по модулю простого числа. Одной из особенностью алгоритма является то, что для простых чисел специального вида можно находить дискретный логарифм за полиномиальное время.

   Предположим, что n — количество точек эллиптической кривой. Пусть число n раскладывается на простые числа $p_1, p_2, \cdots, p_n$. Суть метода сводится к тому, чтобы найти дискретные логарифмы по модулю числе p_i, а затем получить общее решение с помощью китайской теоремы об остатках. Атака позволяет свести проблему дискретного логарифма в большом поле n к той же задаче, но с гораздо меньшим полем p. Для того, чтобы противостоять атаке необходимо просто выбирать кривые, количество точек которых делится на очень большое простое число q порядка n.
2. Алгоритм Шенкса, более известный как шаги младенца/шаги гиганта. Для группы размером n вычисляется таблиц размером $n^{1/2}$, затем по этой таблице происходит поиск нужного элемента. Сложность алгоритма $O(\sqrt{q})$.
3. Уязвимость сингулярных и суперсингулярных кривых. Ранее упоминалось, что для решения задачи дискретного логарифма не существует субэкспоненциальных методов решения. На самом деле есть одна оговорка, такие методы есть, но только для определенного рода кривых: сингулярных и суперсингулярных. Особые свойства таких

кривых позволяют свести задачу дискретного логарифма на эллиптической кривой, к задаче дискретного логарифма в конечном поле. Соответственно, для такого класса кривых стандартные ключи будут фатально уязвимы, что позволит злоумышленникам вскрыть секретный ключ, за относительно небольшое время.

4. Уязвимость аномальных кривых. Как отмечалось ранее, количество точек эллиптической кривой вычисляется по формуле $n = q + 1 - t$, где q $-$ размер исходного поля. Кривая называется суперсингулярной, если t делится на 2. Поэтому, на первый взгляд может показаться хорошей идеей использовать кривые в которых количество точек равно q, т.е. $t = 1$. Однако такие кривые называются аномальными и решение дискретного логарифма на аномальных эллиптических кривых является еще более простой задачей, чем для суперсингулярных и сингулярных кривых.

Подведем небольшой итог и выделим плюсы и минусы. Итак, основные плюсы:

1. Гораздо меньшая длина ключа по сравнению к «классической» асимметричной криптографией.
2. Скорость работы эллиптических алгоритмов гораздо выше, чем у классических. Это объясняется как размерами поля, так и применением более близкой для компьютеров структуры бинарного конечного поля.
3. Из-за маленькой длины ключа и высокой скорости работы, алгоритмы асимметричной криптографии на эллиптических кривых могут использоваться в смарт-картах и других устройствах с ограниченными вычислительными ресурсами.

Но стоит отметим также и основной минус эллиптической криптографии. Все

плюсы эллиптической криптографии вытекают из одного конкретного факта: для задачи дискретного логарифмирования на эллиптических кривых не существует субэкспоненциальных алгоритмов решения. Это позволяет уменьшить длину ключа и увеличить производительность. Однако если такие алгоритмы появятся, то это будет означать крах эллиптической криптографии.

Далее мы рассмотрим конкретные примеры эллиптических криптосистем на наиболее популярных протоколах. Мы рассмотрим классическую реализацию и реализацию на эллиптических кривых. Для более подробной информации следует обратиться к источникам: [1], [6], [10], [13], [14], [15], [16], [17], [18], [19], [20]

Мы намереваемся кодировать наши открытые тексты точками некоторой заданной эллиптической кривой E, определенной над конечным полем F_q. Мы хотим это осуществить простым и систематическим способом так, чтобы открытый текст m (который можно рассматривать как целое число из некоторого интервала) можно было легко прочитать, зная координаты соответствующей точки P_m. Заметим, что это 'кодирование' — не то же самое, что засекречивание.

3.1 Система Диффи-Хеллмана обмена ключами

Рассмотрим классическую реализацию системы Диффи-Хеллмана.

Так как криптосистемы с открытым ключом значительно медленнее классических криптосистем (по крайней мере, при нынешнем состоянии науки и техники), то разумнее использовать их в качестве дополнения к классическим криптосистемам, с помощью которых и передаются сообщения. Зато процедуру согласования ключей классической криптосистемы можно очень эффективно реализовать с помощью системы с открытым ключом. Первая такая детально проработанная схема, предложенная Диффи и Хеллманом,

основана на задаче дискретного логарифмирования.

Пусть два пользователя (Аида и Бернардо) хотят согласовать ключ — случайный элемент из F_q^*, — посредством которого они будут зашифровывать переписку между собой. Аида выбирает случайное число a между 1 и $q-1$, которое она держит в секрете, вычисляет $g^a \in F_q^*$, которое объявляет открыто. Бернардо делает то же самое: он случайно выбирает b и объявляет $g^b \in F_q^*$. В качестве секретного ключа используется g^{ab}. Оба пользователя могут вычислить этот ключ. Например, Аида знает g^b (это открытая информация) и свой собственный секретный ключ a. Однако посторонние знают только g^a и g^b. Если для мультипликативной группы F_q^* выполнено следующее предположение, то посторонние не смогут определить ключ.

Предложение 2. *Диффи—Хеллмана. Сложность вычисления g^{ab} по g^a и g^b чрезвычайно велика.*

Предположение Диффи-Хеллмана априори не слабее предположения о чрезвычайной сложности дискретного логарифмирования в конечной группе. Если бы можно было вычислять дискретные логарифмы, то, очевидно, предположение Диффи-Хеллмана было бы неверным. Некоторые считают, что справедливо и обратное, однако пока этот вопрос остается открытым. Другими словами, никто еще не предложил способ получения g^{ab} из g^a и g^b без использования a и b. Однако вполне возможно, что такой способ существует. Теперь рассмотрим эту же систему, но на эллиптических кривых.

Ключевой обмен Диффи-Хеллмана на эллиптических кривых

Предположим, что Маша и Петя хотят договориться о ключе, которым будут впоследствии пользоваться в некоторой классической криптосистеме. Прежде всего они открыто выбирают какое-либо конечное поле F_q и какую-либо эллиптическую кривую E над ним. Их ключ строится по случай-

ной точке P на этой эллиптической кривой. Если у них есть случайная точка P, то, например, ее x-координата дает случайный элемент F_q, который можно затем преобразовать в r-разрядное целое число в p-ичной системе счисления (где $q = p^r$), и это число может служить ключом в их классической криптосистеме. (Здесь мы пользуемся словом случайный в неточном смысле; мы лишь хотим сказать, что выбор из некоторого большого множества допустимых ключей произволен и непредсказуем). Они должны выбрать точку P так, чтобы все их сообщения друг другу были открытыми и все же никто, кроме них двоих, ничего бы не знал о P.

Маша и Петя открыто выбирают точку $B \in E$ в качестве основания. Не требуется, чтобы B была образующим элементом в группе точек кривой E. Эта группа может и не быть циклической. Если она циклическая, мы не хотим тратить время на проверку того, что B – образующий элемент (или даже на нахождение общего числа N точек, которое нам не понадобится в последующем). Достаточно, чтобы порожденная B подгруппа была большой, предпочтительно того же порядка величины, что и сама E. Предположим, что B – взятая открыто точка на E весьма большого порядка (равного либо N, либо большому делителю N). Чтобы образовать ключ, Маша вначале случайным образом выбирает целое число a, сравнимое по порядку величины с q (которое близко к N); это число она держит в секрете. Она вычисляет $aB \in E$ и передает эту точку открыто. Петя делает то же самое: он выбирает случайно b и открыто передает $bB \in B$. Тогда используемый ими секретный ключ – это $p = abB \in E$. Оба пользователя могут вычислить этот ключ. Например, Маша знает bB (точка была передана открыто) и свое собственное секретное a. Однако третья сторона знает лишь aB и bB. Кроме решения задачи дискретного логарифмирования – нахождения a по B и aB (или нахождения b по B и bB), пока нет способа найти abB, зная лишь aB и bB.

3.2 Криптосистема Мэсси—Омуры для передачи сообщений

Далее рассмотрим криптосистему Мэсси—Омуры.

Предположим, что все согласились использовать конечное поле F_q; оно зафиксировано и общеизвестно. Каждый пользователь системы втайне выбирает такое случайное целое e между 0 и $q-1$, что НОД$(e, q—1) = 1$, и с помощью алгоритма Евклида вычисляет обратное к нему число $d = e(mod\ q-1)$, т.е. $de = 1(mod\ q-1)$. Если Алиса (пользователь А) намерена передать сообщение P Бобу, она сначала посылает ему элемент P^{e_A}. Это послание для Боба бессодержательно, так как он не знает d_A (или e_A, что то же самое) и не может восстановить P. Не пытаясь понять смысл сообщения, Боб возводит его в свою степень e_B и отсылает $P^{e_A e_B}$ обратно Алисе. Третий шаг состоит в том, что Алиса несколько «распутывает» сообщение, возводя его в степень d_A; так как $P^{e_A d_A} = P$, то, по сути дела, она отсылает Бобу P^{e_B}, который теперь может прочитать сообщение, возведя его в степень d_B. Весьма простая идея этой системы может быть реализована и в схемах, где используются процедуры, отличные от возведения в степень в конечных полях. Однако не все так просто. Прежде всего, отметим, что при использовании системы Мэсси-Омуры абсолютно необходима хорошая схема подписи сообщений. Без нее любое постороннее лицо C, которому сообщение P не предназначено, может представиться Бобом и вернуть Алисе сообщение $P^{e_A e_C}$. Алиса, не зная, что оно прислано самозванцем, пользовавшимся своим ключом e_C, продолжит процедуру, возведя сообщение в степень d_A, дав тем самым С возможность прочитать сообщение. Поэтому промежуточное сообщение $P^{e_A e_B}$ от Боба Алисе должно сопровождаться аутентификацией, т.е. некоторым сообщением в схеме подписи, которое может послать только Боб.

Кроме того, важно, чтобы такие пользователи, как В или С, которые после дешифрования различных сообщений P будут знать пары (P, P^{e_A}), не

могли воспользоваться этим для определения e_A. Так, если бы Боб мог решать задачу дискретного логарифмирования в F_q^* и по P и P^{e_A} определять, каким должно быть e_A, то он мог бы легко вычислить $d_A = e_A(mod\ q-1)$ и затем перехватывать и читать все дальнейшие сообщения Алисы, кому бы они ни были адресованы.

Система Мэсси—Омуры на эллиптических кривых

Теперь посмотрим на систему Мэсси—Омуры с реализацией на эллиптических кривых. Это криптосистема с открытым ключом для передачи элементов сообщения m, которые мы теперь предположим представленными точками P_m фиксированной (и не скрываемой) эллиптической кривой E над F_q (q берется большим). Предполагается также, что общее число N точек на E вычислено и не составляет секрета. Каждый пользователь системы секретно выбирает такое целое случайное число e между 1 и N, что НОД$(e, N) = 1$. Используя алгоритм Евклида, он находит затем обратное e^{-1} к числу e по модулю N, т.е. такое целое число d, что $de \equiv 1(mod\ N)$. Если Алиса хочет послать Вове сообщение P_m, то она сначала посылает ему точку e_AP_m (индекс A указывает на пользователя Алису). Это ничего не говорит Вове, который, не зная ни e_A, ни d_A, не может восстановить P_m. Однако, не придавая этому значения, он умножает ее на свое e_B и посылает обратно Алисе $e_Be_AP_m$. На третьем шаге Алиса должна частично раскрыть свое сообщение, умножив $e_Be_AP_m$ на d_A. Так как $NP_m = 0$ и $d_Ae_A \equiv 1(modN)$, при этом получается точка e_BP_m, которую Алиса возвращает Вове. Тот может теперь прочитать сообщение, умножив точку e_BP_m на d_B.

Злоумышленник может знать e_AP_m, $e_Be_AP_m$ и e_BP_m. Умел бы он решать задачу дискретного логарифмирования на E, то он мог бы определить e_B по первым двум точкам, вычислить $d_B \equiv e_B^{-1}(mod\ N)$ и $P_m = d_Be_BP_m$.

3.3 Криптосистема Эль-Гамаля

Далее мы покажем систему Эль-Гамаля.

Сначала зафиксируем очень большое конечное поле F_q и элемент $g \in F_q^*$ (желательно, хотя и не обязательно, чтобы он был порождающим). Предположим, что используются элементы открытого текста с численными эквивалентами P в F_q. Каждый пользователь A выбирает случайно целое число $a = a_A$, скажем, из диапазона $0 < a < q - 1$. Это секретный ключ дешифрования. Открытым ключом шифрования является элемент да $g^a \in F_q$.

Чтобы передать сообщение P пользователю A, мы выбираем случайно целое число k и посылаем A следующую пару элементов из g^k, Pg^{ak} Заметим, что вычислить g^{ak} можно, не зная a, просто возведя g^{ak} в степень k. Теперь A, зная a, может по этой паре раскрыть P, возведя первый элемент g^k в a-ю степень и разделив на результат второй элемент (или, что эквивалентно, возведя g^k в степень $q - 1 - a$ и умножив на второй элемент). Другими словами, наше послание состоит из замаскированного сообщения (P «несет маску» g^{ak}) и «ключа», а именно, g^k, которым можно снять маску (но воспользоваться ключом может лишь тот, кто знает a).

Тот, кто умеет решать задачу дискретного логарифмирования в F_q, вскроет эту криптосистему, определив ключ дешифрования a по ключу шифрования g^a. Вообще говоря, может существовать способ определения g^{ak} по g^k и g^a, а значит, и вскрытия шифра, не связанный с дискретным логарифмированием. Однако, как уже упоминалось при обсуждении системы Диффи-Хеллмана, считается, что нет способа получить g^{ak} из g^k и g^a, не решив, по существу, задачи дискретного логарифмирования.

Система Эль-Гамаля на эллиптических кривых

Теперь рассмотрим систему Эль-Гамаля на эллиптических кривых.

Это – другая криптосистема с открытым ключом для передачи сообщений P_m. Как и в описанной выше системе ключевого обмена, мы исходим из данных несекретных:

1. конечного поля F_q
2. определенной над ним эллиптической кривой E
3. точки 'основания' B на ней

Знать общее число N точек на E нам не нужно. Каждый из пользователей выбирает случайное целое число a, которое держит в секрете, затем находит и делает общедоступной точку aB. Чтобы послать Борису сообщение P_m, Анна выбирает случайно целое число k и посылает пару точек $(kB, P_m + k(a_B B))$ (где $a_B B$ – открытый ключ Бориса). Чтобы прочитать сообщение, Борис умножает первую точку из полученной пары на свое секретное число a_B и вычитает результат умножения из второй точки:

$$P_m + k(a_B B) - a_B(kB) = P_m. \tag{5}$$

Таким образом, Анна посылает замаскированное P_m вместе с 'подсказкой' kB, при помощи которой можно снять 'маску' $ka_B B$, если знать секретное число a_B. Злоумышленник, который умеет решать задачу дискретного логарифмирования на E, может, конечно, найти a_B, зная $a_B B$ и B.

3.4 Аналог криптосистемы RSA на эллиптических кривых

Теперь рассмотрим аналог одной из самых популярных криптосистем − RSA на эллиптической кривых. Для начала вкратце опишем классическую реализацию.

Итак, каждый пользователь A выбирает два простых числа $p_A,\ q_A$, а вслед за этим − случайное число e_A, которое не имеет общих множителей с $(p_A - 1)(q_A - 1)$. Далее, A вычисляет $n_A = p_A q_A$, $\varphi(n_A) = n_A + 1 - p_A - q_A$ и число, обратное относительно умножения к e_A по модулю $\varphi(n_A)$ $d \equiv e_A^{-1}(mod\, \varphi(n_A))$. Ключ шифрования $K_{n_A,e} = (n_A, e_A)$ делается открытым, а ключ дешифрования $K_{\varphi(n),d} = (\varphi(n), d)$ − секретным. Шифрующее преобразование − это отображение $\mathbb{Z}/n_a\mathbb{Z}$ в себя по формуле $f(P) \equiv P^{e_A}(mod\, n_A)$. Дешифрующее преобразование − это отображение $\mathbb{Z}/n_a\mathbb{Z}$ в себя по формуле $f^{-1}(C) \equiv C^{d_A}(mod\, n_A)$. Нетрудно заметить, что согласно нашему выбору d_A эти два отображения взаимно обратны. А именно, последовательное применение в любом порядке f и f^{-1} приводит к возведению в степень $d_A e_A$. Поскольку $d_A e_A$ дает при делении на $\varphi(n_A)$ остаток 1, это эквивалентно возведению в первую степень.

Теперь рассмотрим эллиптический аналог заметив, что на эллиптические кривые над кольцом вычетов $\mathbb{Z}/n\mathbb{Z}$ для составного числа $n = p \cdot q$, где p, q − различные простые числа, можно переложить криптографический протокол RSA. Эллиптические кривые вида $y^2 \equiv x^3 + B(mod\ p)$ при $p \equiv 5(mod\ 6)$ и $y^2 \equiv x^3 + Ax(mod\ p)$ при $p \equiv 3(mod\ 4)$ имеют порядок группы $p + 1$. Поэтому эллиптические кривые $E(\mathbb{Z}/n\mathbb{Z})$ вида $y^2 \equiv x^3 + B(mod\ p)$ при $p \equiv q \equiv 5(mod\ 6)$ и $y^2 \equiv x^3 + Ax(mod\ p)$ при $p \equiv q \equiv 3(mod\ 4)$ имеют порядок группы $(p + 1)(q + 1)$.

Оригинальная система RSA имеет порядок группы $\varphi(n) = (p-1)(q-1)$. Поэтому такие эллиптические кривые позволяют строить криптосистемы

аналогичные RSA. Если безопасность системы RSA связана с вычислением функции $\varphi(n)$, то в случае эллиптических кривых она связана с нахождением числа $(\mathrm{p}+1)(\mathrm{q}+1)$. Рассмотрим аналог шифрования с открытым ключом на эллиптической кривой $y^2 \equiv x^3 + B(mod\ n)$. Открытым ключом является пара (n, e), секретным $-$ показатель $d \equiv e^{-1}(mod\ (p+1)(q+1))$. Для шифрования сообщения m отправитель генерирует случайно положительно число $y < n$, вычисляет шифрограмму, умножая точку $(m, y) \in E(\mathbb{Z}/n\mathbb{Z})$ на открытый показатель e и полученную шифрограмму отсылает получателю. Последний в свою очередь умножает полученную точку $eP,\ P = (m, y)$ на d, тем самым расшифровывая сообщение m.

Но стоит отметить, что использование алгоритма RSA на эллиптических кривых ведет к появлению отличий от оригинальной реализации протокола в части из безопасности, например одной из которой является проблема сводимости к соответствующей массовой задачи выбора. Поэтому такое механическое переложение должно сопровождаться криптографическим анализом.

ЗАКЛЮЧЕНИЕ

Актуальность данной темы очень велика в наше время. Как было отмечено ранее: средства и системы криптографической защиты информации играют важную роль в современных компьютерных информационных системах, используемых в сфере финансовой и коммерческой деятельности.

В данной работе были изложены базовые понятия теории эллиптических кривых, необходимые для реализации криптографических систем на них. Рассмотрены основные алгоритмы арифметики точек эллиптической кривой, а также некоторые способы выбора кривых, пригодных для использования в криптографических системах. Приведены примеры атак на эллиптические кривые без деталей и тонкостей. Показаны системы шифрования Эль-Гамаля, Мэсси-Омуры, Диффи-Хеллмана и RSA в классическом их использовании и реализацией на эллиптических кривых с примерами. В практической части (Приложение А) реализован программный модуль для сложения точек эллиптической кривой написаный на языке программирования Java.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Коблиц Н. Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001.

2 Болотов А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2006.

3 Hankerson D. Guide to Elliptic Curve Cryptography, 2004.

4 Washington, Lawrence C. Elliptic Curves: Number Theory and Cryptography, 2008.

5 Нестеренко Ю. В. Теория чисел: учебник для студ. высш. учебных заведений / Ю.В. Нестеренко - М.: Издательский центр 'Академия', 2008.

6 Ростовцев А.Г., Моховенко Е.Б. Теоритическая криптография. Спб.: Изд-во АНО НпО 'Профессионал', 2004.

7 Коблиц Н. Введение в элиптические кривые и модулярные формы: пер. с англ. - М.: Мир, 1988.

8 Лидл Р., Нидеррайтер Г. Конечные поля. пер. с англ. - М.: Мир, 1988.

9 Виноградов И. М. Основы теории чисел. М.: Гостехиздат, 1952.

10 Бухштаб А. А. Теория чисел. М.: Просвещение, 1966.

11 Курош А. Г. Курс высшей алгебры. М.: Наука, 1968.

12 Курош А. Г. Теория групп. М.: Физматлит, 1967.

13 Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.

14 Шнайер Б. Практическая криптография. М.: Издательский дома 'Вильямс' 2005.

15 Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. М.: Наука, 1982.

16 Кадужнин Л. А. Введение в общую алгебру. М.: Наука, 1973.

17 Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.

18 Болотов А. А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.

19 Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. МЦНМО, 2003.

20 Н. Смарт. Криптография. М.: ТЕХНОСФЕРА, 2005.

Приложение А

Практическая часть

```
import java.math.BigInteger;

//класс для арифметических операций точек эллиптической кривой
public class ECPoint
{
    public BigInteger x;
    public BigInteger y;
    public BigInteger a;
    public BigInteger b;
    public BigInteger FieldChar;

    public ECPoint(ECPoint p)
    {
        x = p.x;
        y = p.y;
        a = p.a;
        b = p.b;
        FieldChar = p.FieldChar;
    }

    public ECPoint()
    {
```

```
}

//сложение двух точек P1 и P2
public static ECPoint add(ECPoint p1, ECPoint p2)
{
    ECPoint p3 = new ECPoint();
    p3.a = p1.a;
    p3.b = p1.b;
    p3.FieldChar = p1.FieldChar;

    BigInteger dy = p2.y.add(p1.y.negate());
    BigInteger dx = p2.x.add(p1.x.negate());

    if (dx.signum() < 0)
    {
        dx = dx.add(p1.FieldChar);
    }

    if (dy.signum() < 0)
    {
        dy = dy.add(p1.FieldChar);
    }

    BigInteger m =
            dy.multiply(dx.modInverse(p1.FieldChar))
              .mod(p1.FieldChar);
```

```
    if (m.signum() < 0)
    {
        m = m.add(p1.FieldChar);
    }

    p3.x = m.pow(2).add(p1.x.add(p2.x).negate()).mod(p1.FieldChar);
    p3.y = m.multiply(p1.x.add(p3.x.negate()))
            .add(p1.y.negate()).mod(p1.FieldChar);

    if (p3.x.signum() < 0)
    {
        p3.x = p3.x.add(p1.FieldChar);
    }
    if (p3.y.signum() < 0)
    {
        p3.y = p3.y.add(p1.FieldChar);
    }
    return p3;
}

//сложение точки P с собой же
public static ECPoint Double(ECPoint p)
{
    ECPoint p2 = new ECPoint();
    p2.a = p.a;
    p2.b = p.b;
```

```
p2.FieldChar = p.FieldChar;

BigInteger dy = p.x.pow(2).multiply(p.a)
                 .multiply(BigInteger.valueOf(3));
BigInteger dx = p.y.multiply(BigInteger.valueOf(2));

if (dx.signum() < 0)
{
    dx = dx.add(p.FieldChar);
}
if (dy.signum() < 0)
{
    dy = dy.add(p.FieldChar);
}

BigInteger m =
        dy.multiply(dx.modInverse(p.FieldChar))
          .mod(p.FieldChar);

p2.x = m.pow(2).add(p.x.pow(2).negate()).mod(p.FieldChar);
p2.y = m.multiply(p.x.add(p2.x.negate()))
        .add(p.y.negate()).mod(p.FieldChar);

if (p2.x.signum() < 0)
{
    p2.x = p2.x.add(p.FieldChar);
}
```

```
    if (p2.y.signum() < 0)
    {
        p2.y = p2.y.add(p.FieldChar);
    }

    return p2;
}

//умножение точки на число x,
//по сути своей представляет x сложений точки самой с собой
public static ECPoint multiply(BigInteger x, ECPoint p)
{
    ECPoint temp = p;
    x = x.add(BigInteger.valueOf(-1));

    while (x.signum() != 0)
    {

        if (x.mod(BigInteger.valueOf(2)).signum() != 0)
        {
            if (temp.x.equals(p.x) || temp.y.equals(p.y))
            {
                temp = Double(temp);
            }
            else
            {
                temp = ECPoint.add(temp, p);
```

```
                }
                x = x.add(BigInteger.valueOf(-1));
            }
            x = x.divide(BigInteger.valueOf(2));
            p = Double(p);
        }
        return temp;
    }
}
```