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

Содержание

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 работы.

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.

1 Базовые понятия о криптосистемах

1.1 Основные сведенья

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

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} вычислить 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.

1.2 Электронная подпись (Аутентикация)

Часто одной из наиболее важных частей сообщения является подпись. Если сообщение имеет особенную важность, могут потребоваться дополнительные способы заверения подлинности (аутентикации) 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 аутентикации. 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 $f_B f_A^{-1}(\mathrm{P})$, то Боб, применив f_B^{-1} , дешифрует сообщение, включая этот добавок, и все превратится в открытый текст, за исключением добавка, который примет вид $f_A^{-1}(\mathrm{P})$. 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

!!!!!ТЕОРИЯ!!!!!!

3 Криптосистемы на эллиптических кривых

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 Ключевой обмен Диффи-Хеллмана на элиптических 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 случайной 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 первым делом открыто выбирают точку $B \in E$ в качестве основания. Мы, однако, не требуем, чтобы B была образующим элементом в группе точек кривой E. Эта группа может и не быть циклической. Даже 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). Нам хотелось бы, 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, сравни-

мое 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 любая 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 Система Мэсси—Омуры на элиптических 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 $de \equiv 1(modN)$. Если Алиса хочет послать Вове сообщение P_m, то она сначала посылает ему точку $e_A P_m$ (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 $e_B e_A P_m$. На третьем шаге Алиса должна частично раскрыть свое сообщение, умножив $e_B e_A P_m$ на d_A. Так как $NP_m = 0$ и $d_A e_A \equiv 1(modN)$, при этом получается точка $e_B P_m$, которую Алиса возвращает Вове. Тот может теперь прочитать сообщение, умножив точку $e_B P_m$ на d_B.

Заметим, что злоумышленник может знать $e_A P_m$, $e_B e_A P_m$ и $e_B P_m$. Если бы он умел решать задачу дискретного логарифмирования на E, то он мог бы определить e_B по первым двум точкам, вычислить $d_b \equiv e_B^{-1}(modN)$ и $P_m = d_B e_B P_m$.

3.3 Система Эль-Гамаля на элиптических 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:

$$P_m + k(a_B B) - a_B(kB) = P_m. \tag{1}$$

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 Выбор кривой и точки

Существуют различные способы выбора эллиптической кривой и (в системах Диффи-Хеллмана и Эль-Гамаля) 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 **??**; 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 $y^2 = x^3 + ax + b$.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Коблиц Н. «Курс теории чисел и криптографии»: Пер. с англ. – Научное изд-во ТВП, 2001. – x+254 с.