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 $f{-}1_A$, обратной к f_A, то он удостоверяется в том, что сообщение послано Алисой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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