Московский авиационный институт
(Национальный исследовательский университет)

Факультет: «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»
Дисциплина: «Криптография»

Лабораторная работа № 4

Тема: эллиптические кривые

Студент: Хренов Геннадий
Группа: 80-307Б
Преподаватель: Борисов А. В.
Дата:
Оценка:

Москва, 2021

1. Постановка задачи

Подобрать такую эллиптическую кривую над конечным простым полем порядка p, такую, порядок точки которой полным перебором находится за 10 минут на ПК. Упомянуть в отчёте, какие алгоритмы и теоремы существуют для облегчения и ускорения решения задачи полного перебора.

2. Метод решения

Эллиптическая кривая, определённая над конечным полем, имеет конечное количество точек. Количество точек в группе называется порядком группы. Самый простой метод определение порядка группы – полный перебор, но он выполняется очень долго, если p – большое простое число. Более быстрый алгоритм - алгоритм Шуфа. В подходе Шуфа для подсчёта мощности используется теорема Хассе об эллиптических кривых, которая утверждает, что если E/Fq является эллиптической кривой над конечным полем Fq, то ||E(Fq)|| удовлетворяет неравенству $| q+1 - ||E(Fq)|| | \leq 2\sqrt{q}$. Этот сильный результат упрощает нашу задачу путём сужения к конечному (хотя и большому) множеству возможностей.

Порядок P(подгруппы) — это минимальное положительное целое n, такое, что nP=0. Порядок P связан с порядком эллиптической кривой теоремой Лагранжа, согласно которой порядок подгруппы — это делитель порядка исходной группы. Иными словами, если эллиптическая кривая содержит N точек, а одна из подгрупп содержит n, то n является делителем N. Два этих факта вместе дают нам возможность определить порядок подгруппы с базовой точкой P:

1. Вычисляем порядок эллиптической кривой N с помощью алгоритма Шуфа.

2. Находим все делители N.

3. Для каждого делителя n порядка N вычисляем nP.

4. Наименьшее n, такое, что nP=0, является порядком подгруппы.

Более простой способ – по определению. Вычисляем nP , при n = 1,2,3…, пока nP не станет равным 0.

Коэффициенты кривых подобраны случайно. P – простое число, подобранное для времени работы в 10 минут. После нахождения всех точек кривой выбирается случайная, и для неё считается порядок.

3. Структура программы

Sol.py – реализация программы

Основные функции:

elliptic_curve(x, y, p) – проверка принадлежности кривой

extended_euclidean_algorithm(a, b) – расширенный алгоритм Евклида

inverse_of (n, p) – обратная величина по модулю p

add_points(P, Q, p) – алгебраическая сумма точек

4. Результаты работы

```
D:\Kripta\lab4>python sol.py
y^2 = x^3 + 12345 * x + 67890 (mod 27017)
Group(curve) oder is 27016
Order of P=(7981, 9220) is 13508
Time: 10.74137376944224 min.

D:\Kripta\lab4>
```

Проверка: 27016/13508 = 2 - теорема Лагранжа выполняется

5. Выводы

В криптографии используется следующая идея: в качестве закрытого ключа берется случайное целое d, выбранное из {1,...,n-1} (где n - порядок подгруппы). В качестве открытого ключа - точка H=dG (где G - базовая точка подгруппы). Если мы знаем d и G (вместе с другими параметрами области определения), то найти H «просто». Но если мы знаем H и G, то поиск закрытого ключа d является «сложной» задачей, потому что требует решения задачи дискретного логарифмирования.

СПИСОК ЛИТЕРАТУРЫ

1. Доступно о криптографии на эллиптических кривых https://habr.com/ru/post/335906/