МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Московский Авиационный Институт»
(Национальный Исследовательский Университет)

Институт: №8 «Информационные технологии
и прикладная математика»
Кафедра: 806 «Вычислительная математика
и программирование»

Лабораторная работа № 5
по курсу «Криптография»

Группа: М8О-306Б-21

Студент(ка): О. А. Мезенин

Преподаватель: А. В. Борисов

Оценка:

Дата: 05.05.2024

Москва, 2024

Оглавление

1 Тема 3
2 Задание 3
3 Теория 4
4 Ход лабораторной работы 5
5 Выводы 8

1 Тема

Эллиптические кривые.

2 Задание

Подобрать такую эллиптическую кривую, порядок точки которой полным перебором находится за 10 минут на ПК. Упомянуть в отчёте результаты замеров работы программы, характеристики вычислителя. Также указать какие алгоритмы и/или теоремы существуют для облегчения и ускорения решения задачи полного перебора.

Рассмотреть для случая конечного простого поля Z_p.

3 Теория

Эллиптическая кривая над конечным простым полем Z_p (где p — простое число) — это множество точек:

$$\{(x, y) \in Z_p^2 \mid y^2 = x^3 + ax + b(mod\ p), 4a^3 + 26b^2 \neq 0(mod\ p)\} \cup \{0\},$$

где 0 – точка в бесконечности, a и b – два целых числа в Z_p.

Порядок группы эллиптической кривой — это количество точек на кривой.

Порядок точки P (или порядок подгруппы, порожденной точкой P) эллиптической кривой — это наименьшее положительное число n такое, что nP=0.

Для нахождения такого n методом полного перебора нужно перебирать все k=1,2,3,..., пока не будет выполнено равенство kP=0.

Для ускорения алгоритма можно воспользоваться алгоритмом Шуфа для поиска порядка группы эллиптической кривой и теоремой Лагранжа, согласно которой порядок подгруппы — это делитель порядка исходной группы:

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.

4 Ход лабораторной работы

Характеристики ПК:
Процессор AMD Ryzen 5 2600
ОЗУ 16 ГБ

Реализация класса эллиптической кривой была взята отсюда — https://github.com/andreacorbellini/ecc/blob/master/logs/common.py (с небольшими доработками).

Идея алгоритма перебора была в том, чтобы перебирать кривые с разными p (простые числа, найденные с помощью решета Эратосфена), затем находить k первых точек, принадлежащей кривой и для каждой из них уже находить порядок, замеряя время. Так продолжать до тех пор, пока не закончатся простые числа или не будет достигнуто нужное время.

Реализация функции get_order_of_point:

```
def get_order_of_point(curve, point):
    p = point
    order = 0
    while p := curve.add(p, point):
        order += 1

    return order
```

Реализация функции get_first_n_points:

```
def get_first_n_points(curve, n):
    points = []
    for x in range(curve.p):
        for y in range(curve.p):
            if curve.is_on_curve((x, y)):
                points.append((x, y))
                if len(points) >= n:
                    return points
```

Реализация функции main:

```
def main():
    n = int(input())
    a = int(input())
```

```
    b = int(input())
    required_time = int(input())  # in seconds
    prime_step = int(input())
    start_step = int(input())

    primes = get_primes(n)
    max_time = 0
    max_point = 0
    max_p = 0
    max_point_order = 0
    cur_i = start_step
    while max_time < required_time and cur_i < len(primes):
        p = primes[cur_i]
        curve = EllipticCurve(p, a, b)
        points = get_first_n_points(curve, 2)
        for point in points:
            start_time = time.time()
            point_order = get_order_of_point(curve, point)
            end_time = time.time()
            cur_time = end_time - start_time
            if max_time < cur_time:
                max_time = cur_time
                max_point = point
                max_p = p
                max_point_order = point_order
            print(f"p={p}, cur_time={cur_time}, point={point}")
        cur_i += prime_step

    print(f"a={a}, b={b}, p={max_p}, time={max_time} seconds, point
order={max_point_order}, point={max_point}")
```

Здесь для ускорения поиска были добавлены prime_step и start_step — шаг по простым числам и начальный индекс простых чисел. Для каждой кривой берутся две точки.

Было очень много попыток подбора чисел n, prime_step и start_step: чаще всего это были недостаточно большие числа, и с такими параметрами пришлось бы ждать целевую кривую очень долго.

Итоговый запуск программы прошел с такими входными данными:

```
n=400000000
a=-2
b=2
required_time=600
prime_step=100000
start_step=5000000
```

Вывод программы:

```
p=86028157, cur_time=128.15531587600708, point=(1, 1)
p=86028157, cur_time=129.25277638435364, point=(1, 86028156)
p=87857533, cur_time=133.16771912574768, point=(1, 1)
p=87857533, cur_time=131.91567468643188, point=(1, 87857532)
p=89687693, cur_time=108.58084774017334, point=(1, 1)
p=89687693, cur_time=109.79701566696167, point=(1, 89687692)
p=91519081, cur_time=280.70820450782776, point=(0, 10706785)
p=91519081, cur_time=280.5695593357086, point=(0, 80812296)
p=93354689, cur_time=566.002200126648, point=(0, 44947215)
p=93354689, cur_time=568.2784616947174, point=(0, 48407474)
p=95189093, cur_time=190.49081206321716, point=(1, 1)
p=95189093, cur_time=191.45387506484985, point=(1, 95189092)
p=97026263, cur_time=293.99523973464966, point=(0, 6576277)
p=97026263, cur_time=291.6543004512787, point=(0, 90449986)
p=98866931, cur_time=595.0886433124542, point=(1, 1)
p=98866931, cur_time=606.4621770381927, point=(1, 98866930)
a=-2, b=2, p=98866931, time=606.4621770381927 seconds, point order=98866926,
point=(1, 98866930)
```

Найдена кривая с параметрами a=-2, b=2, p=98866931. Порядок точек для неё искался примерно 10 минут (595 и 606 секунд для двух точек).

5 Выводы

В ходе лабораторной работы познакомился с понятием эллиптических кривых, в том числе над конечным простым полем, и посмотрел, как они применяются в криптографии. Изучил операции, применяемые над эллиптическими кривыми, и такие понятия, как порядок группы и порядок точки. Методом перебора подобрал эллиптическую кривую, порядок точки который находится примерно за 10 минут. Также посмотрел алгоритм, который может ускорить нахождения порядка точки.

6 Список используемой литературы

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