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 № 4
по курсу «Криптография»

Группа: М8О-308Б-22

Студентка: К. А. Былькова

Преподаватель: А. В. Борисов

Оценка:

Дата: 20.04.2025

Москва, 2025

ОГЛАВЛЕНИЕ

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 криптография — раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. Роль основной криптографической операции выполняет операция скалярного умножения точки на эллиптической кривой на данное целое число, определяемая через операции сложения и удвоения точек эллиптической кривой. Последние, в свою очередь, выполняются на основе операций сложения, умножения и инвертирования в конечном поле, над которыми рассматривается кривая.

Особый интерес к криптографии эллиптических кривых обусловлен теми преимуществами, которые дает её применение в беспроводных коммуникациях — высокое быстродействие и небольшая длина ключа. Асимметричная криптография основана на сложности решения некоторых математических задач. Ранние криптосистемы с открытым ключом, такие как алгоритм RSA, криптостойки благодаря тому, что сложно разложить составное число на простые множители. При использовании алгоритмов на эллиптических кривых полагается, что не существует субэкспоненциальных алгоритмов для решения задачи дискретного логарифмирования в группах их точек. При этом порядок группы точек эллиптической кривой определяет сложность задачи. Считается, что для достижения такого же уровня криптостойкости, как и в RSA, требуются группы меньших порядков, что уменьшает затраты на хранение и передачу информации.

Преимущества использования шифрования на основе эллиптических кривых.

- Шифрование на основе эллиптических кривых (ECC) требует меньше вычислительных ресурсов и меньше полосы пропускания для генерации ключей, шифрования и дешифрования;
- Благодаря меньшему размеру ключа, операции шифрования на основе эллиптических кривых (ECC), такие как генерация ключа, шифрование и дешифрование, могут выполняться быстрее по сравнению с RSA, что означает меньшую задержку для конечного пользователя.

Эллиптические кривые, лежащие в основе современных криптографических систем, требуют точного знания порядка группы точек. Именно с этим прекрасно справляется алгоритм Шуфа: для безопасности криптосистемы необходимо, чтобы порядок группы содержал большой простой делитель, и данный алгоритм позволяет его вычислить даже для очень больших полей.

Алгоритм Шуфа — эффективный алгоритм подсчёта числа точек на эллиптической кривой над конечным полем. Его особенность заключается в замене полного перебора на анализ кривой в точках кручения малого порядка. Благодаря этому, в отличие от полного перебора, алгоритм Шуфа работает за полиномиальное время, что делает его применимым для криптографически значимых параметров.

4 Ход лабораторной работы

Для выполнения задания использовалась каноническая форма эллиптической кривой (уравнение Вейерштрасса): $y^2 = x^3 + ax + b$. Коэффициенты a и b были выбраны случайным образом, а модуль кривой p подбирался вручную. В криптографии на эллиптических кривых модуль p должен быть большим простым числом, чтобы обеспечить безопасность. Основываясь на этом, перебирались простые числа (примерно в диапазоне от 25000 до 40000, в реальности же используются числа минимум 256 бит), пока подсчёт порядка точки не стал удовлетворять условию.

После нахождения всех нужных коэффициентов, кривая проверяется на сингулярность: в сингулярных точках нельзя определить касательную, и групповой закон сложения не работает. И как раз условие несингулярности гарантирует, что кривая является группой. Для построения криптосистем данная проверка обязательна, так как эллиптические кривые используются в криптографии благодаря своей сложности для взлома. А если кривая сингулярна, её безопасность полностью разрушается.

Далее полным перебором находятся все точки, принадлежащие кривой. Выбирается случайная точка, находится её порядок путём последовательного сложения самой с собой до получения точки на бесконечности (0, 0).

Характеристики вычислителя:

- Процессор: AMD Ryzen 9 5900HS with Radeon Graphics 3.30 GHz
- Оперативная память: 16,0 GB

Код:

```
import random
import time

A = 12345
B = 6789

def extended_euclidean_algo(a, b):
    old_r, r = a, b
    old_s, s = 1, 0
    old_t, t = 0, 1
    while r != 0:
        quotient = old_r // r
        old_r, r = r, old_r - quotient * r
        old_s, s = s, old_s - quotient * s
        old_t, t = t, old_t - quotient * t
    return old_r, old_s, old_t

def inverse_mod(n, p):
```

```
    gcd, x, _ = extended_euclidean_algo(n, p)
    if gcd != 1:
        raise ValueError("Обратного элемента не существует")
    return x % p

def add_points(P, Q, p):
    if P == (0, 0):
        return Q
    if Q == (0, 0):
        return P
    if P[0] == Q[0] and P[1] != Q[1]:
        return (0, 0)

    if P == Q:
        m = (3 * P[0]**2 + A) * inverse_mod(2 * P[1], p) % p
    else:
        m = (P[1] - Q[1]) * inverse_mod(P[0] - Q[0], p) % p

    x = (m**2 - 2 * P[0]) % p
    y = (P[1] + m * (x - P[0])) % p
    return (x, -y % p)

def find_point_order(point, p):
    order = 1
    current = add_points(point, point, p)
    while current != (0, 0):
        current = add_points(current, point, p)
        order += 1
    return order

def elliptic_curve(x, y, p):
    return (y ** 2) % p == (x ** 3 + A * x + B) % p

def print_curve(p):
    print(f"y^2 = x^3 + {A} * x + {B} (% {p})")

def main():
    p = 35573
    assert (4 * A**3 + 27 * B**2) % p != 0, "Кривая сингулярна"
    print_curve(p)

    start_time = time.time()
    points = []
    for x in range(p):
        for y in range(p):
            if elliptic_curve(x, y, p):
                points.append((x, y))

    curve_order = len(points)
    print(f"Порядок кривой = {curve_order}")
    point = random.choice(points)

    print(f"Точка: {point}, порядок: {find_point_order(point, p)}")
    print(f"Время вычисления: {time.time() - start_time:.2f} сек")

if __name__ == '__main__':
    main()
```

Результат:

```
y^2 = x^3 + 12345 * x + 6789 (% 35573)
Порядок кривой = 35321
Точка: (10484, 2974), порядок: 21569
Время вычисления: 600.74 сек
```

В итоге, за 10 минут полным перебором была найдена нужная эллиптическая кривая.

Для ускорения решения задачи вместо полного перебора можно воспользоваться алгоритмом Шуфа, который в свою очередь использует теорему Хассе. Его особенность заключается в сведении задачи к вычислениям в точках кручения малого порядка с последующим восстановлением результата. Это эффективный метод определения порядка эллиптической кривой над конечным полем, работающий за полиномиальное время — сложность: $O(log^8 p)$, где p — число элементов поля.

5 Выводы

Был написан скрипт на Python, который подбирает такую эллиптическую кривую, порядок точки которой полным перебором находится за 10 минут. Также заранее был подобран модуль кривой p.

В ходе выполнения данной лабораторной работы было выяснено, какие именно кривые используются в криптографических алгоритмах и почему они обеспечивают достаточный уровень безопасности. Также теперь известно, что существуют различные алгоритмы подсчёта числа точек на эллиптической кривой над конечным полем, которые активно применяются в эллиптической криптографии, разделе криптографии, который изучает асимметричные криптосистемы.

В результате выполнения данной лабораторной работы были приобретены навыки, которые будут полезны для выполнения других работ и курсовых проектов.

6 Список используемой литературы

1. Применко Э. А. Алгебраические основы криптографии — М.: Книжный дом “ЛИБРОКОМ”, 2013. — 289 с.
2. Доступно о криптографии на эллиптических кривых // Хабр — URL: https://habr.com/ru/articles/335906/ (дата обращения: 20.04.2025)
3. Эллиптическая кривая // Cyclowiki.org — URL: https://cyclowiki.org/wiki/Эллиптическая_кривая (дата обращения: 20.04.2025)
4. Факторизация и эллиптическая кривая. Часть III // Хабр — URL: https://habr.com/ru/articles/523282/ (дата обращения: 20.04.2025)