1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7**

1. **«Решение задачи дискретного логарифмирования на эллиптической кривой»**
2. по дисциплине «Криптографические методы защиты информации»
3. Выполнил:
4. студент гр. 5151001/00201 А.А. Устюгов

<*подпись*>

1. Проверил
2. старший преподаватель, к.т.н А.В. Тулинова

<*подпись*>

1. Санкт-Петербург

2024

1. **СОДЕРЖАНИЕ**

[1 Формулировка задания 3](#_Toc165636489)

[2 Ход работы 4](#_Toc165636490)

[3 Тестирование 6](#_Toc165636491)

[4 Контрольные вопросы 8](#_Toc165636492)

[5 Выводы 10](#_Toc165636493)

# Формулировка задания

Цель работы – изучение методов дискретного логарифмирования на эллиптической кривой, реализация методов Полларда и Полига–Хеллмана в группе точек эллиптической кривой.

Задача – получить у преподавателя вариант задания и разработать программу П-1, которая, в соответствии с вариантом, реализует один из методов дискретного логарифмирования на эллиптической кривой: метод Полларда или метод Полига–Хеллмана. При реализации алгоритма Полига–Хеллмана допускается использование готовых процедур для вычисления логарифма 𝑙𝑜𝑔𝑃0 𝑄𝑘. В качестве входных данных программа П-1 должна принимать параметры эллиптической кривой, образующую точку 𝑃, порядок 𝑞 группы ⟨𝑃⟩; на выходе – возвращать значение логарифма 𝑑.

# Ход работы

В ходе выполнения данной лабораторной работы использовалась библиотека Miracl, предоставляющая возможности работы с эллиптическими кривыми.

Реализация ро-метода Полларда.

Схема логарифмирования на эллиптической кривой методом Полларда:

1. Выбрать 𝐿.

2. Выбрать функцию 𝐻:⟨𝑃⟩ → {1, . . . , 𝐿}.

3. Для 𝑗 = 1, . . . , 𝐿 выполнить следующие действия.

3.1. Случайным образом выбрать 𝑎𝑗, 𝑏𝑗 ∈ ℤ⁄𝑞ℤ.

3.2. Вычислить 𝑅𝑗 = 𝑎𝑗𝑃 + 𝑏𝑗𝑄.

4. Случайным образом выбрать 𝛼′, 𝛽′ ∈ ℤ⁄𝑞ℤ и вычислить точку 𝑇′ ← 𝛼′𝑃 + 𝛽′𝑄. Положить 𝑇′′ ← 𝑇′, 𝛼′′ ← 𝛼′, 𝛽′′ ← 𝛽′.

5. Повторять следующие действия, пока не получим 𝑇′ = 𝑇′′.

5.1. Положить 𝑗 ← 𝐻(𝑇′), 𝑇′ ← 𝑇′ + 𝑅𝑗, 𝛼′ ← 𝛼′ + 𝑎𝑗 (𝑚𝑜𝑑 𝑞), 𝛽′ ← 𝛽′ + 𝑏𝑗 (𝑚𝑜𝑑 𝑞).

5.2. Положить 𝑗 ← 𝐻(𝑇′′), 𝑇 ′′ ← 𝑇 ′′ + 𝑅𝑗 , 𝛼 ′′ ← 𝛼 ′′ + 𝑎𝑗 (𝑚𝑜𝑑 𝑞), 𝛽′′ ← 𝛽′′ + 𝑏𝑗 (𝑚𝑜𝑑 𝑞), 𝑗 ← 𝐻(𝑇′′), 𝑇′′ ← 𝑇′′ + 𝑅𝑗 , 𝛼′′ ← 𝛼′′ + 𝑎𝑗 (𝑚𝑜𝑑 𝑞), 𝛽′′ ← 𝛽′′ + 𝑏𝑗 (𝑚𝑜𝑑 𝑞).

6. Если 𝛼′ = 𝛼′′, 𝛽′ = 𝛽′′, то перейти на шаг 1. Иначе положить 𝑑 ≡ (𝛼′ − 𝛼′′)(𝛽′′ − 𝛽′)−1 (𝑚𝑜𝑑 𝑞).

7. Результат: 𝑑.

В данном методе на вход подается образующая подгруппы группы точек эллиптической кривой P, её порядок q, точка Q = dP. На выходе находится необходимый параметр d.

Для тестирования данного метода был написан скрипт на SageMath, генерирующий параметры кривой с заданным интервалом для порядка q.

Была разработана программа, реализующая метод Полларда. В результате она возвращает секретный показатель d, а также количество итераций алгоритма.

# Тестирование

Тестирование проходило на следующих параметрах:

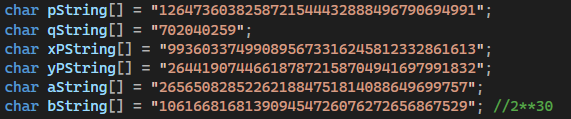


Рисунок 1 – параметры 1 кривой

Работа программы для данных параметров:

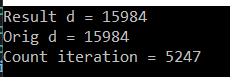


Рисунок 2 – результат для 1 кривой

В данном тесте q длиной 30 бит, d находится практически мгновенно.

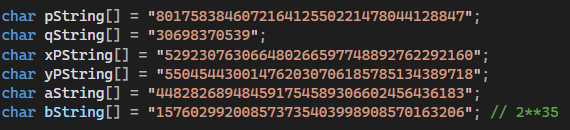


Рисунок 3 – параметры 2 кривой

Работа программы для данных параметров:

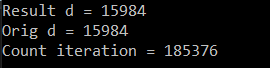


Рисунок 4 – результат для 2 кривой

В данном тесте q длиной 35 бит, d находится примерно за 20 секунд.

Тестирование проходило на следующих параметрах:

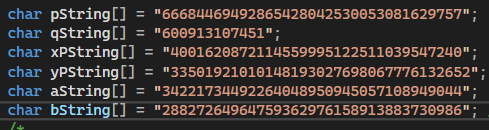


Рисунок 5 – параметры 3 кривой

Работа программы для данных параметров:

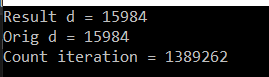


Рисунок 6 – результат для 3 кривой

В данном тесте q длиной 40 бит, d находится примерно за 2-3 минуты

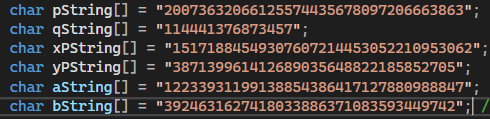


Рисунок 7 – параметры 4 кривой

Работа программы для данных параметров:

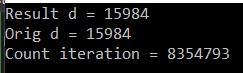


Рисунок 8 – результат для 4 кривой

В данном тесте q длиной 46 бит, d находится примерно за 25 минут.

# Контрольные вопросы

1. Сравните сложности задач дискретного логарифмирования на эллиптической кривой и в конечном поле.

Задача дискретного логарифмирования на эллиптических кривых является более трудной для решения, чем задача дискретного логарифмирования в конечных полях. Наиболее быстрые методы решения задачи дискретного логарифмирования в конечном поле не применимы к эллиптическим кривым.

Например, одни из наиболее быстрых алгоритмов решения задачи дискретного логарифмирования в конечном поле имеют сложность O(exp (c(logp log logp)d)),     где p- размер конечного поля. Наиболее быстрые алгоритмы на эллиптической кривой имеют сложность O(), где q- количество точек. Таким образом, при сопоставимых *p* и *q*, алгоритмы на конечном поле быстрее в десятки раз.

2. Оцените срок безопасноcти эксплуатации криптосистемы, основанной на задаче дискретного логарифмирования в группе точек эллиптической кривой, по отношению к методу Полларда, если характеристика поля и порядок группы имеют длину 256 бит. Оцените срок действия ключа в начале и в конце срока эксплуатации.

Сложность метода Полларда O(), где q- количество точек. Следовательно, для успешного взлома такой криптосистемы потребуется произвести около 2128 операций. Данная задача является вычислительно сложной и не может быть решена с использование обычного компьютера (в теории может быть решена при использовании квантового компьютера). На данный момент максимальный ключ взломанных криптосистем на эллиптических кривых имеет длину 109 бит. Таким образом, срок действия ключа 1,6\*1028 лет.

3. Сформулируйте требования к параметрам эллиптической кривой для обеспечения стойкости к методу Полига–Хеллмана.

Пусть q- порядок циклической группы, он раскладывается на множители вида . Затем для проведения атаки Полига-Хеллмана требуется вычислять dj по модулю . Тогда для обеспечения стойкости следует выбирать такие кривые, чтобы порядок q имел большие простые делители.

# Выводы

В ходе выполнения лабораторной работы были изучены методы Полларда и Полига-Хеллмана логарифмирования на эллиптических кривых. На основе метода Полларда была написана программа, реализующая дискретное логарифмирование в группе точек эллиптической кривой.