БФУ им. И. Канта – Компьютерный практикум по криптографии на эллиптических кривых

Преподаватель С. Новоселов 2022

Лабораторная работа № 4

Опубликована **26.10.2022**

Дэдлайн **16.11.2022**

Разработать программу в системе компьютерной алгебры Sage, реализующую следующие функции:

1. `order_BSGS(a, b, q)`, где `a, b` – коэффициенты эллиптической кривой $E : y^2 = x^3 + ax + b$, заданной над полем $\mathbb{F}_q$, где q - простое, $\neq 2, 3$. Функция реализует алгоритм Baby Step – Giant Step подсчета $\mathbb{F}_q$– рациональных точек кривой, и возвращает $\#E(\mathbb{F}_q)$.

Требования к сдаче

- Функция должна быть оптимизирована так, чтобы выполняться на тестах за разумное время (около минуты).
- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров
- Лабораторную следует выполнять модификацией файла с тестами, заменяя строку

  `"# your code here."`

  на код, реализующий функцию.
- Функции должны работать на всех примерах, что проверяется запуском команды:
  `sage -t file_with_tests.sage`
- Студент должен понимать, что он написал, зачем, а также ответить на теоретические вопросы.