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

Преподаватель Е. Киршанова 2019–2020

Лабораторная работа № 4

Опубликована **25.10.2019**

Дэдлайн **08.11.2019**

Разработать программу в системе компьютерной алгебры Maple или Sage (в одной на выбор), 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

- Для программ разработанных в системе Maple, следует сдавать подгружаемый модуль.
- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров