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

Преподаватель С. Новоселов Осень 2022

Лабораторная работа № 2

Опубликована **28.09.2022**

Дедлайн **12.10.2022**

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

1. `Sum(a, b, q, x1, y1, x2, y2)`, где `a, b` – коэффициенты эллиптической кривой E, заданной над полем $\mathbb{F}_q$, q – простое, $\neq 2, 3$, $P_1 = (\texttt{x1}, \texttt{y1}), P_2 = (\texttt{x2}, \texttt{y2})$– точки на E ($y_i = \text{infinity}$ для $P_i = \mathcal{O}$). Функция возвращает координаты $P_3 = (\texttt{x3}, \texttt{y3}) = P_1 + P_2$. Если P_1 или P_2 не лежат на E, функция возвращает ошибку.

2. `SumProj(a, b, q, x1, y1, z1, x2, y2, z2)`, те же параметры и выходные данные, что и для функции `Sum(a, b, q, x1, y1, x2, y2)`, но точки P_1, P_2 заданы в проективных координатах. Вычисления проводятся также с проективными координатами.

3. `Mul(a, b, q, x1, y1, k)`, где `a, b` – коэффициенты эллиптической кривой E, заданной над полем $\mathbb{F}_q$, где q – простое, $\neq 2, 3$, $P_1 = (x_1, y_1) \in E$, $k \in \mathbb{Z}$. Функция возвращает координаты точки $P_k = (x_k, y_k) = k \cdot P_1$. Если $P_1 \notin E$, функция возвращает ошибку.

Требования к сдаче

- 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.