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

Преподаватель Е. Киршанова 2019–2020

Лабораторная работа № 2

Опубликована **20.09.2019**

Дэдлайн **04.10.2019 (16:50)**

Разработать программу в системе компьютерной алгебры Maple или Sage (в одной на выбор), реализующую следующие функции:

1. `Sum(a, b, q, x1, y1, x2, y2)`, где `a, b` – коэффициенты эллиптической кривой E, заданной над полем $\mathbb{F}_q$, где 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 в 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

- 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