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

Преподаватель Е. Киршанова 2019–2020

Лабораторная работа № 7

Опубликована **06.12.2019**

Дэдлайн **20.12.2019**

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

1. `Velu_curve`(G, a, b), где $G \subset E(\mathbb{F}_q)$ – конечная группа, $a, b \in \mathbb{F}_q$ – коэффициенты эллиптической кривой E. Функция реализует алгоритм Велу для вычисления кривой E', изогенной E, с ядром G и возвращает коэффициенты E'.

2. `Velu_point`(G, a, b, P), где $G \subset E(\mathbb{F}_q)$ – конечная группа, $a, b \in \mathbb{F}_q$ – коэффициенты эллиптической кривой E, $P \in E$ – точка на кривой. Функция реализует алгоритм Велу вычисления образа точки P в изогенной кривой E', полученной в алгоритме `Velu_curve`(G, a, b).

3. `SIKE()` – функция, имитирующая протокол обмена ключами SIKE. Исходные параметры (кривую и образующие подгрупп) можно взять отсюда `https://crypto-kantiana.com/elena.kirshanova/teaching/curves_2019/SIKE_params.txt`

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