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

Преподаватель С. Новоселов 2020

Лабораторная работа № 8

Опубликована **03.12.2020**

Дэдлайн **21.12.2020**

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

1. `Velu_curve(`G, a, b`)`, где $G \subset E(\mathbb{F}_q)$ – подгруппа, $a, b \in \mathbb{F}_q$ – 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 $G \subset E(\mathbb{F}_q)$ – подгруппа, $a, b \in \mathbb{F}_q$ – 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. `SIDH()` – функция, имитирующая протокол обмена ключами SIDH. Исходные параметры (кривую и образующие подгрупп) можно взять отсюда:
`https://crypto-kantiana.com/semyon.novoselov/teaching/curves_2020/SIDH_params.sage`

Требования к сдаче

- Лабораторную следует выполнять модификацией файла с тестами (TP8_tests.sage), заменяя строку "`# your code here.`" на код, реализующий функцию.

- Функции должны работать на всех примерах, что проверяется запуском команды:
`sage -t TP8_tests.sage`

- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров