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

Преподаватель: С. Новоселов 2020

Лабораторная работа № 7

Опубликована **26.11.2020**

Дэдлайн **10.12.2020**

Разработать программу в системе компьютерной алгебры Sage, реализующую функцию:
`Check_curve`(p, a, b, λ), где p – простое, размер конечного поля; a, b – коэффициенты эллиптической кривой $E/\mathbb{F}_p : y^2 = x^3 + ax + b$ и λ – уровень безопасности в битах. Возвращает $True$, если кривая проходит минимум следующие проверки:

1. на наличие подгруппы большого порядка (стойкость к атаке Полига-Хеллмана);
2. на неравенство характеристики порядку подгруппы;
3. на стойкость задачи дискретного логарифма в данной группе относительно ρ-метода Полларда;
4. на стойкость к атакам на спариваниях (подсчёт степени вложения);
5. кривая должна соответствовать минимальному уровню безопасности λ относительно всех предыдущих пунктов.

Проверить отдельно кривые, рекомендованные КриптоПро™, `https://www.cryptopro.ru/sites/default/files/blog/cpecc12-tc26.pdf`. А именно, два набора параметров: id-tc26-gost-3410-12-512-paramSetA и id-tc26-gost-3410-12-512-paramSetB.

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 (TP7_tests.sage), заменяя строку "`# your code here.`" на код, реализующий функцию.
- Функции должны работать на всех примерах, что проверяется запуском команды:
  `sage -t TP7_tests.sage`
- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров