Преподаватель Е. Киршанова 2019–2020

Лабораторная работа № 7

Опубликована **29.11.2019**

Дэдлайн **13.12.2019**

Разработать программу в системе компьютерной алгебры Maple или Sage (в одной на выбор), программу, проверяющую кривые, рекомендованные КриптоПро^{TM}, `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. Программа должна осуществлять как минимум следующие проверки:

1. На простоту модуля и порядка подгруппы, заданной образующей
2. На неравенство модуля порядку подгруппы
3. На стойкость задачи дискретного логарифма в данной группе относительно ρ-метода Полларда
4. На принадлежность образующей заданной кривой
5. На стойкость к атаке MOV (подсчет степени вложения)

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