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

Преподаватель С. Новоселов 2023

Лабораторная работа № 6

Опубликована **02.11.2023**

Дэдлайн **23.11.2023**

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

1. `Prove_prime(`p`)`, где p – простое или составное число. Функция реализует алгоритм теста на простоту Goldwasser-Killain и возвращает (с большой вероятностью) либо -сертификат простоты p, либо делитель p; с малой вероятностью возвращает “fail”.
2. `Check_prime(`$p_0, C = [A_0, B_0, L_0, p_1], \ldots [A_i, B_i, L_i, p_{i+1}]$`)`, где C – сертификат простоты числа p_0. Функция реализует алгоритм проверки сертификата на простоту и возвращает либо “Accept” (в случае принятия сертификата), либо “Reject” с пояснением, почему.

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, заменяя строку

  `"# your code here."`

  на код, реализующий функцию.
- Функции должны работать на всех примерах, что проверяется запуском команды:
  `sage -t file_with_tests.sage`
- Студент должен понимать, что он написал, зачем, а также ответить на теоретические вопросы.