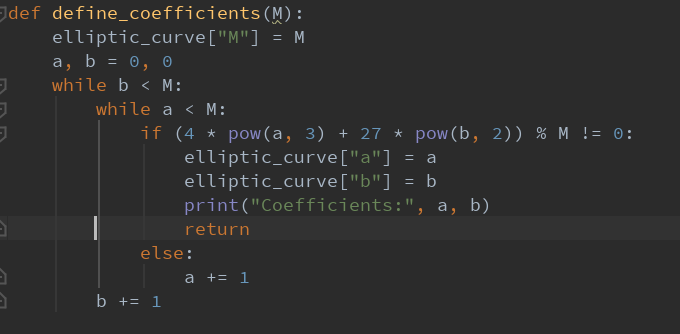
**Отчет по лабораторной работе №3**

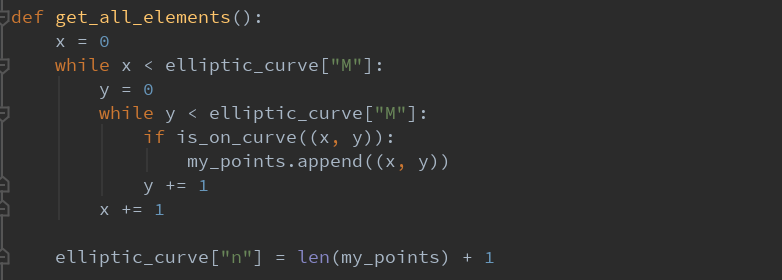
**«Криптосистемы на основе эллиптических кривых»**

**Вариант 3:** Модуль М = 59

Функция, определяющая значения a, b для построения эллиптической группы:

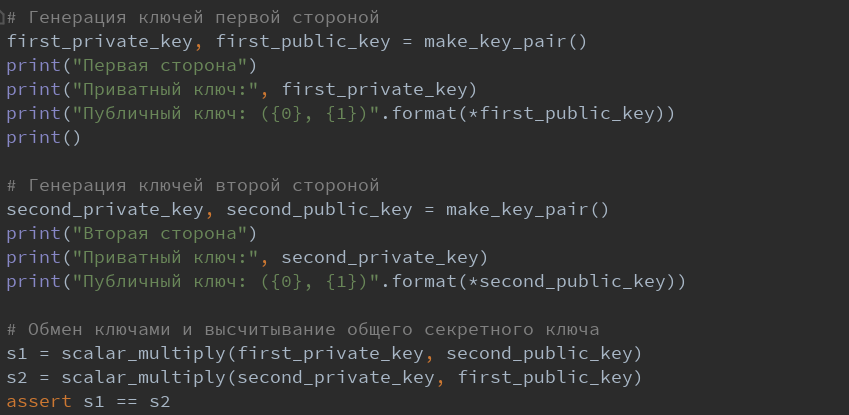


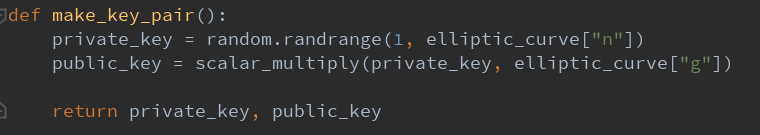
Расчет значения n:

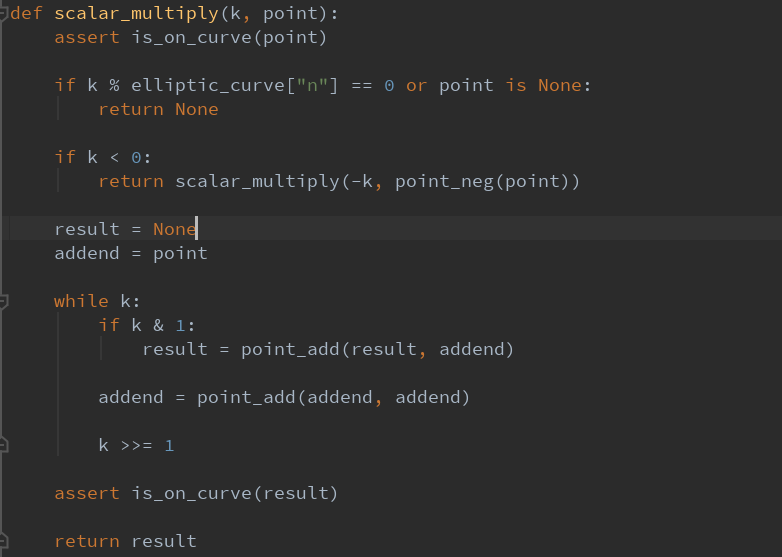


Рассчитать генерирующую точку G для эллиптической группы у меня корректно не получилось, потому демонстрация работы алгоритмов приводится на данных из примера.

Алгоритм обмена ключами для эллиптической группы:







Алгоритм цифровой подписи на основе эллиптической группы:



Демонстрация работы алгоритмов на данных из примера:

