Лабораторная работа 3

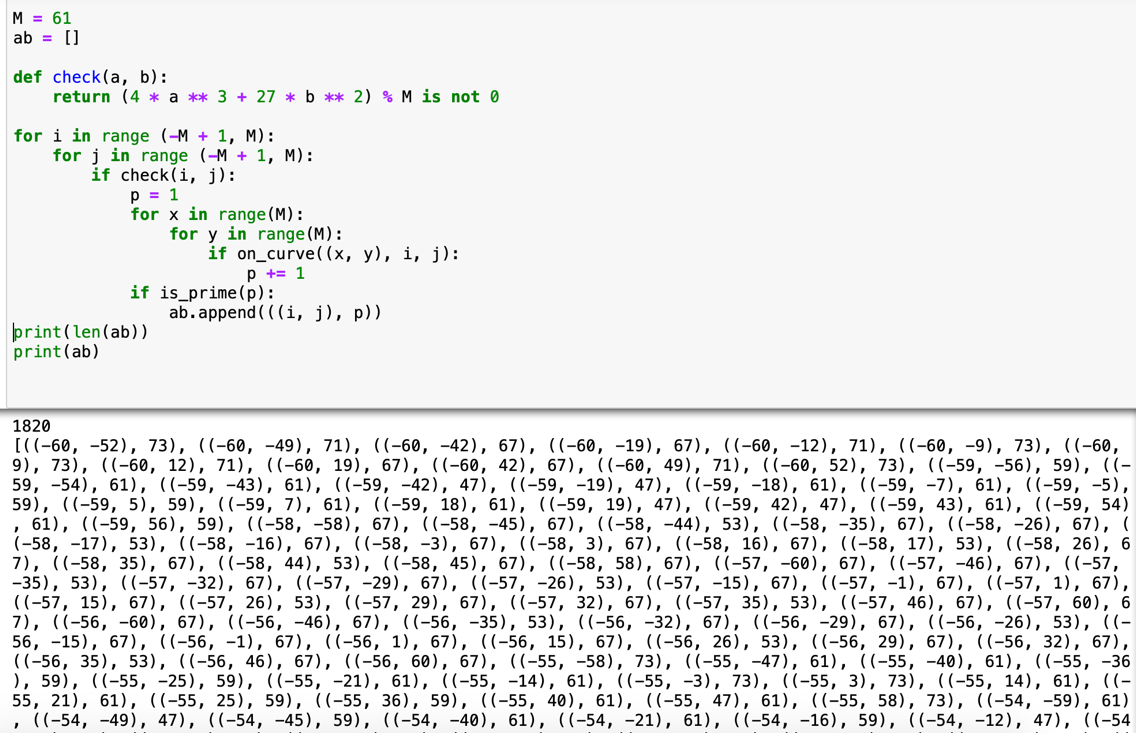
Оба алгоритма ESCDA и RSA являются алгоритмами с открытым ключом, поэтому для сравнения сложности алгоритмов необходимо сказать о понятии уровня безопасности(число операций, которое необходимо совершить злоумышленнику для получения доступа к необходимой информации. Обычный ключ RSA размером 204 бит дает уровень безопасности в 112 бит, когда же алгоритм ECDSA для такого же уровня безопасности нужен только ключ размером 224 бита, что значительно меньше. Следовательно, для взлома ECDSA понадобится намного больше времени.

Для алгоритма ECDSA можно определить сложность приблизительно в O(n) (или O(2k/2) если рассматривать длину ключа) в случае алгоритма «маленьких и больших шагов». В случае алгоритма «Pollard’s p» временная сложность также составит O(n) , но пространственная сложность будет только O(1).  Это по прежнему экспоненциальное время, но уже намного лучше атаки грубой силой.

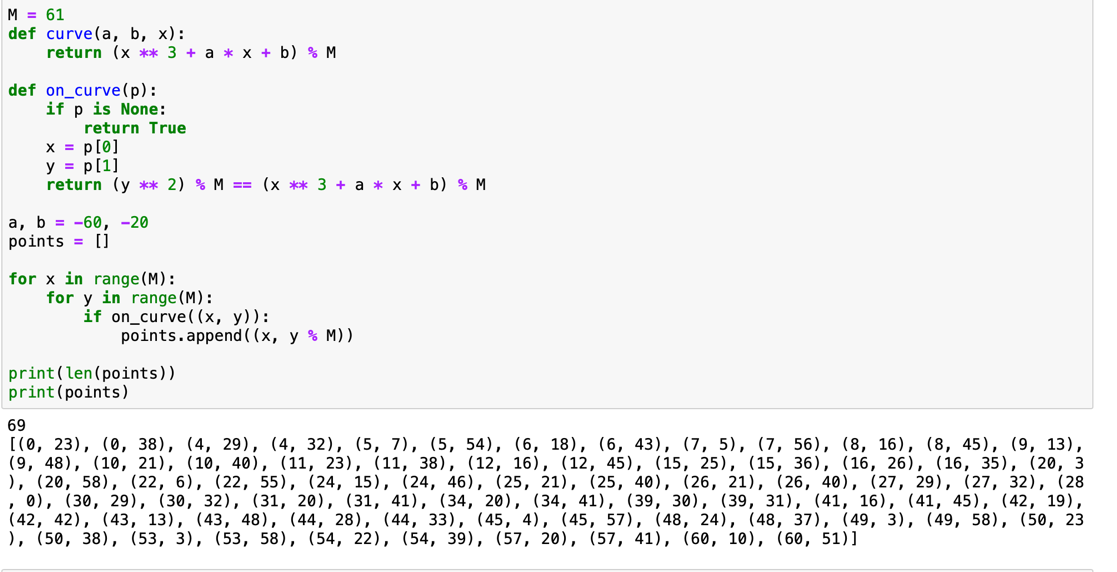
Для алгоритма RSA Serpent(который был реализован в предыдущей лабораторной работе) можно указать временную сложность O(N · 2k). Сложность подделки сообщений, как и для алгоритмов с использованием эллиптический кривых составит O(2k/2).

Таким образом можно сделать вывод, что алгоритм ECDSA использует меньше памяти, но и генерация ключей и подпись производится быстрее.

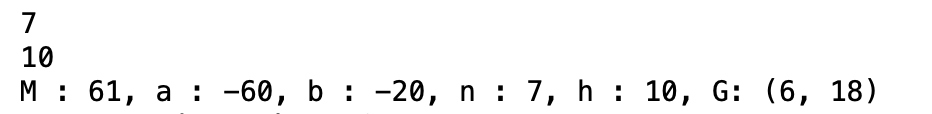
Сгенерировала значения a и b:



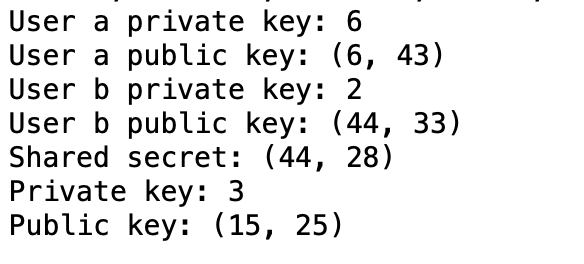
Для найденных в задании 1 параметров сгенерированы все элементы эллиптической группы EM(a, b). В данном случае значение a и b взяты из ранее сгенерированных значений.







Реализован алгоритм обмена ключами для эллиптической группы EM(a,b).



Реализована цифровая подпись на основе эллиптической группы EM(a, b).