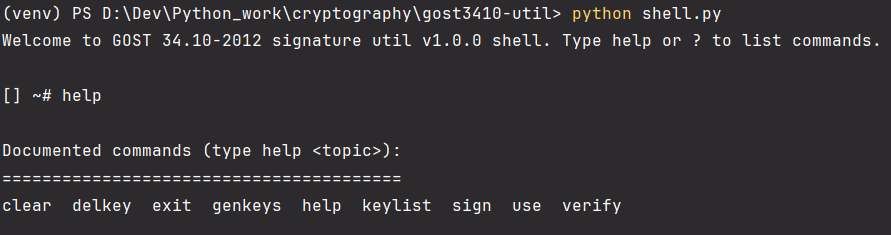
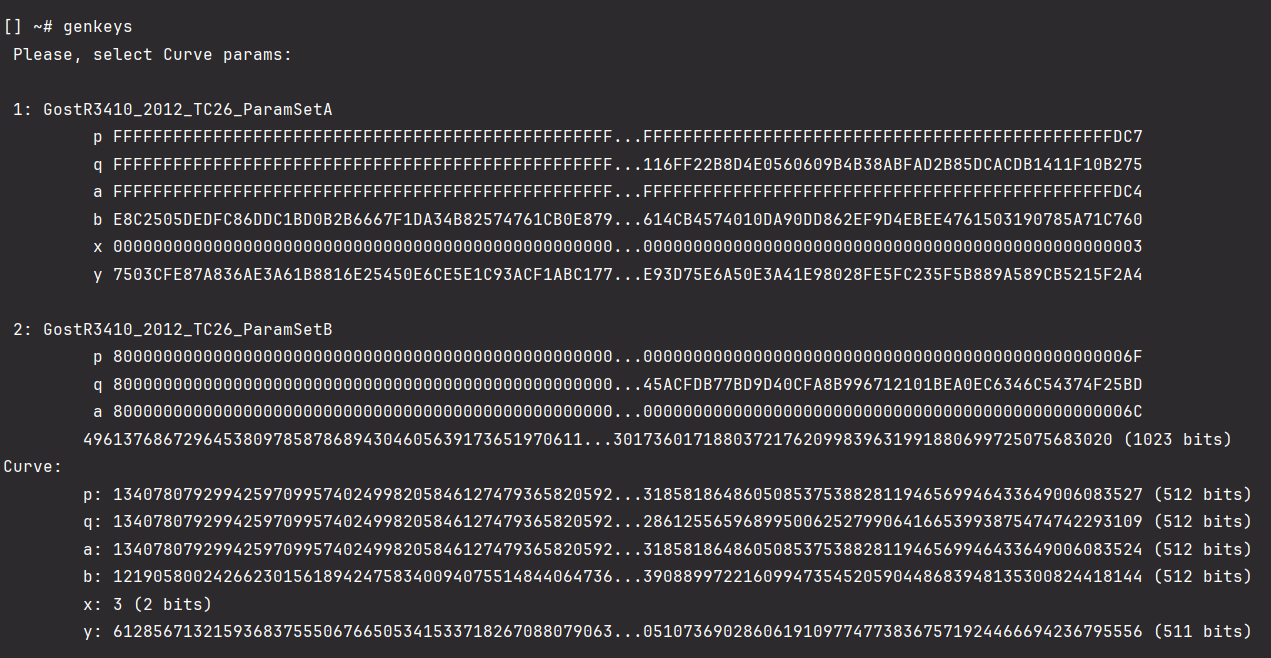
**Введение**

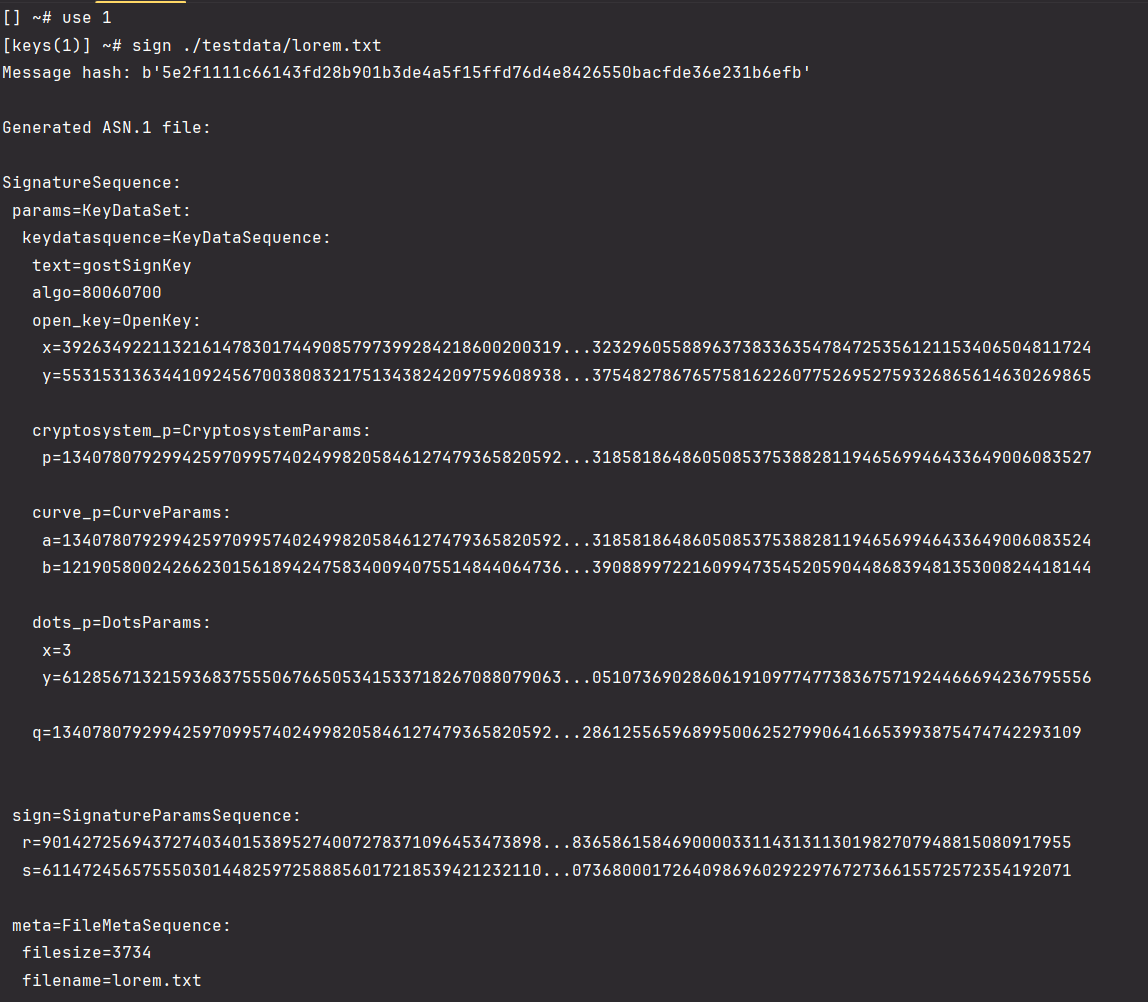
34.10-2018 (полное название: «ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации.

Процессы формирования и проверки электронной цифровой подписи», англ. «Information technology. Cryptographic data security. Signature and verification processes of electronic digital signature») — действующий межгосударственный криптографический стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем. Стандарт разработан на основе национального стандарта Российской Федерации ГОСТ Р 34.10-2012 и введен в действие с 1 июня 2019 года приказом Росстандарта № 1059-ст от 4 декабря 2018 года.

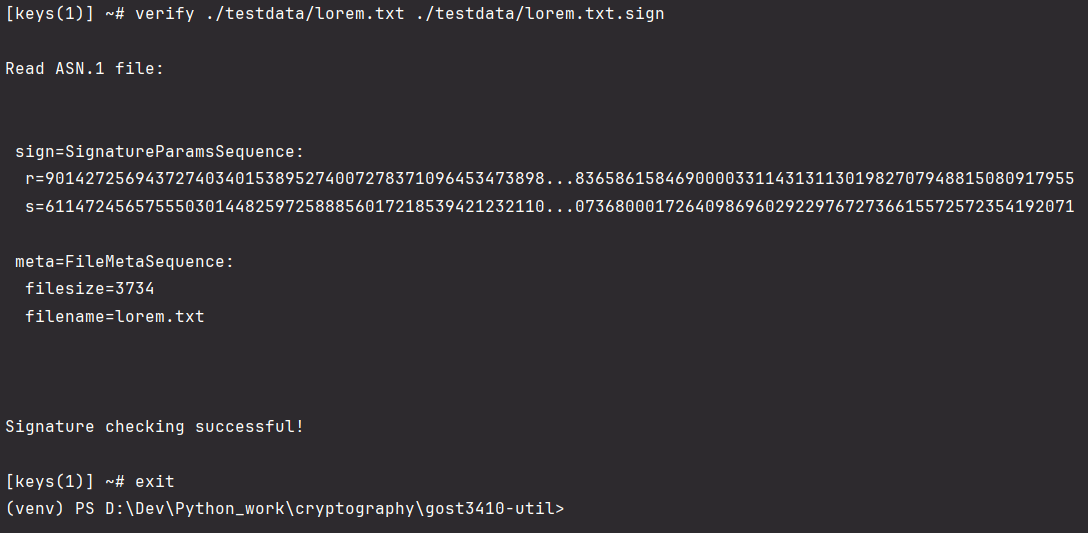
**Ход действий**







Signature created!



Вывод

Приведенный выше вывод представляет собой сеанс взаимодействия с оболочкой утилиты для работы с подписью ГОСТ 34.10-2012. Ниже объяснены основные шаги, происходящие в консоли:

genkeys: Пользователь вызывает команду genkeys, чтобы сгенерировать пару ключей - приватный и публичный. Он также может выбрать параметры кривой, которые будут использоваться для генерации ключей.

use 1: Пользователь выбирает сгенерированную пару ключей для дальнейшего использования.

sign: Пользователь подписывает файл lorem.txt с помощью выбранного приватного ключа. Подпись сохраняется в файл lorem.txt.sign.

verify: Пользователь проверяет подпись файла lorem.txt с помощью соответствующего публичного ключа. Процесс проверки подписи завершается успешно, что означает, что подпись действительна.

exit: Пользователь завершает сеанс и выходит из оболочки утилиты.