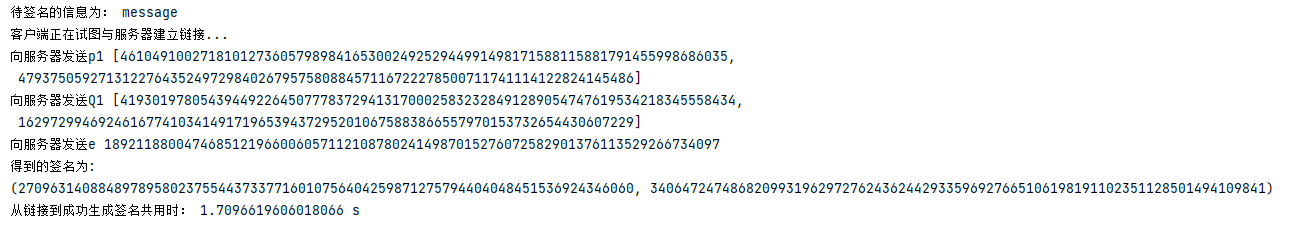


按照这种签名方案，定义并实现椭圆曲线的各种操作函数，实现起来是较为简单的。

由于要求模拟真实网络，我们调用socket库，在本机网络上实现了两方签名。

可得结果：



观察数据发现验证成功