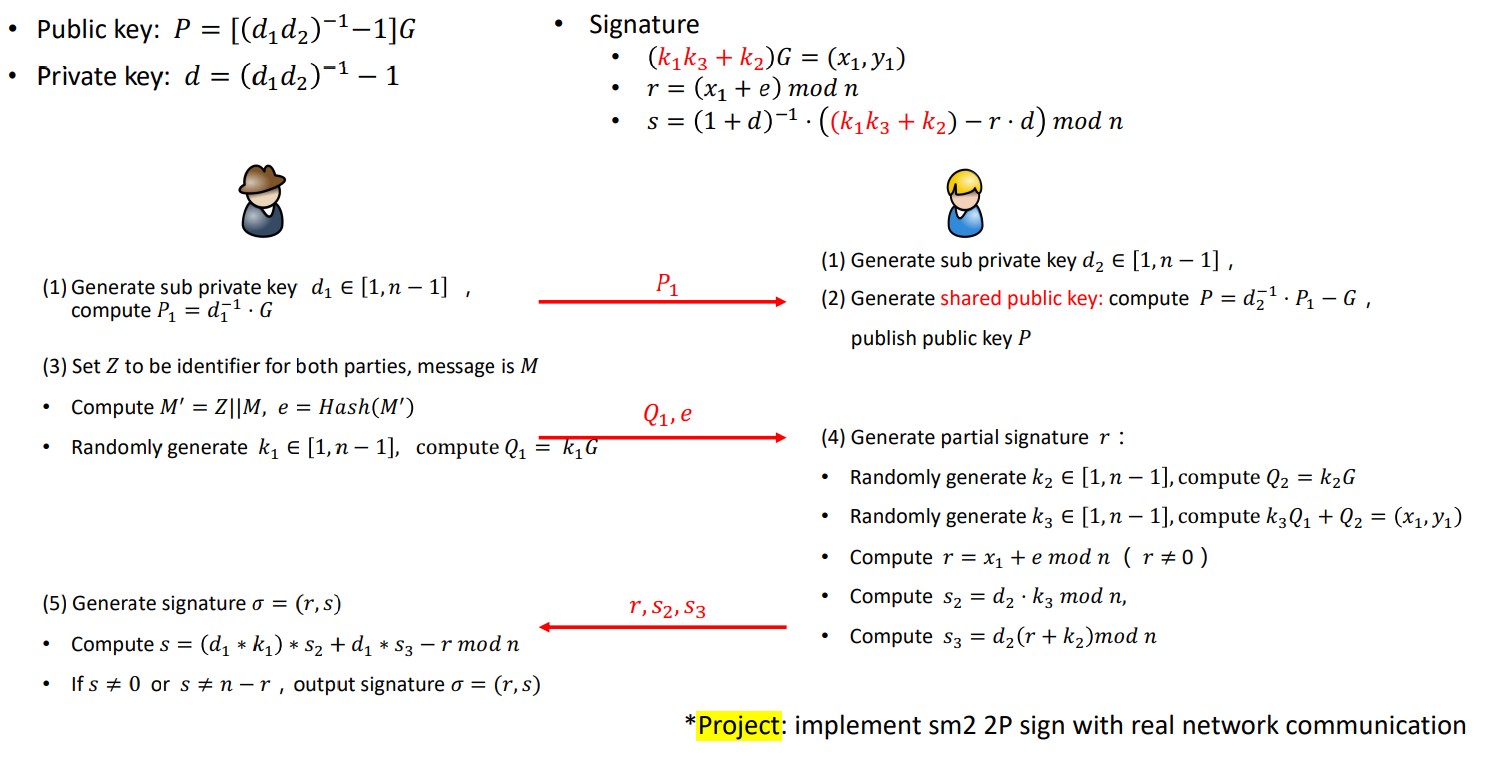
# project-15

implement sm2 2P sign with real network communication

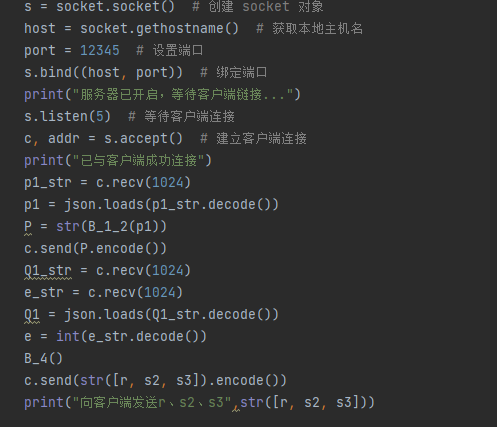
基于SM2的两方协同签名方案在真实网络中实现

# 实现方式

两方协同签名方案是指客户端与可信方服务器共同完成签名与验证的方案。 具体操作方式如图所示

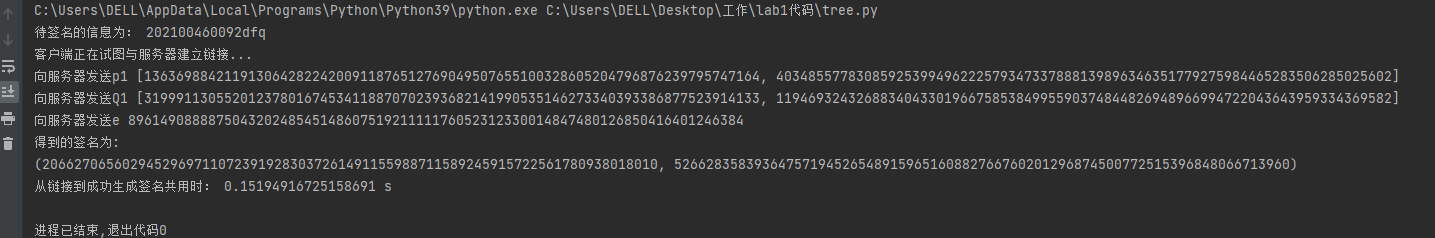
[](https://user-images.githubusercontent.com/129512207/255387137-78dd4f89-4ecf-41d2-8325-0b14b31ec12e.jpg)

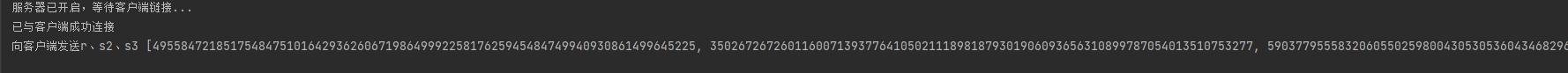
通过这种协同验签方式，单方不再能够生成合法的签名，双方协同生成签名，增加了签名的安全性，可信性。同时使用python中的网络链接代码库来模拟真实的网络连接中，客户端和服务器双方的签名和认证过程。如图所示：

[](https://user-images.githubusercontent.com/129512207/255389564-9330d8b1-5342-4e71-8104-a412b0063160.png)

# 实验结果

客户端：

[](https://user-images.githubusercontent.com/129512207/255389594-e8fb7370-ca69-43bd-b655-666e249a7fec.png) 运行速度：0.15194916725158691 s

[](https://user-images.githubusercontent.com/129512207/255389632-7ea2257d-30be-4fd9-a733-ed7ae1207770.png)服务器：

# 实验环境

Windows10

visual studio 2022

CPU：11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz

# 小组分工

202100460092 戴方奇单人完成project15