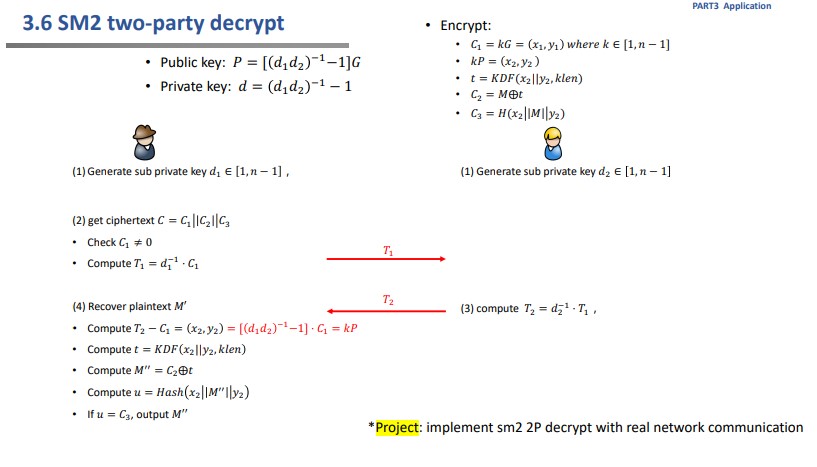
# project-16

implement sm2 2P decrypt with real network communication

基于SM2的两方协同解密方案在真实网络中实现

# 实现方式

具体协议如图所示：

[](https://user-images.githubusercontent.com/129512207/255391173-929b7fae-8ffe-4417-8db7-20e1b2884129.jpg)

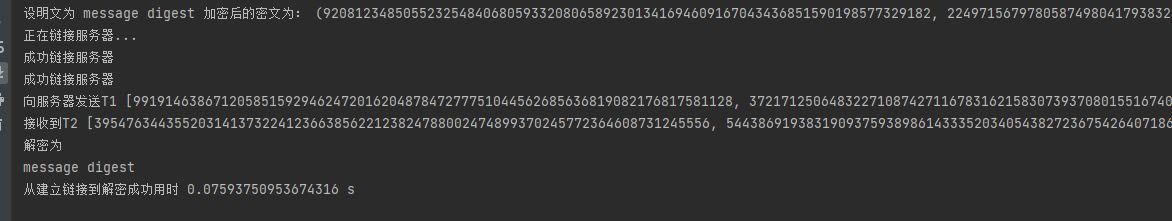
客户端与服务器在保存有各自的私钥分量的情况下，需要协同，通过交换利用各自私钥得到的参数T1、T2，才能最终解密

同时使用python中的网络链接代码库socket库来模拟真实的网络连接中，客户端和服务器双方的传递参数，解密密文的过程。

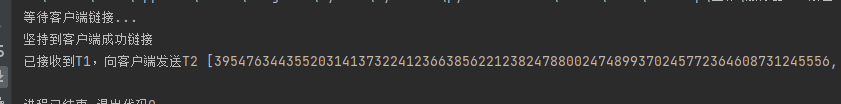
如图所示： [](https://user-images.githubusercontent.com/129512207/255393920-2ec449fc-728c-4ed8-98c5-3a4b1db58275.png)

# 实验结果

客户端页面：

[](https://user-images.githubusercontent.com/129512207/255393953-2c260b84-1389-4d4d-af03-db3f1dd4f5ed.png)

服务器页面：

[](https://user-images.githubusercontent.com/129512207/255393962-3a44c64a-4a6b-4453-84aa-c35afa8a2f93.png)

运行速度：从建立链接到解密成功用时 0.07593750953674316 s

# 运行环境

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project16