*Project: implement sm2 2P sign with real network communication

代码介绍：

代码一共分为6个py文件：

ECC文件中是椭圆曲线运算的实现以及椭圆曲线的参数

sig_partonel以及sigpartwo中主要写了两方前面的主要计算过程的API调用，

test文件是没有网络通信的测试环境

socket_p1,socket-p2是在UDP协议下签名两方交互过程

代码运行方法：

1、将代码load到本地

2、安装必要的第三方库（json,hashlib,socket等）

3、test.py可直接运行

4、socket_p1,socket_p2,运行时要先运行socket_p2.py，再运行socket_p2.py

运行结果：

```
---------- RESTART: D:\desk\大一下ppt\创新创业课程\SM2_2P__SIG\socket_p1.py ----------
请输入Z,M （用空格分开）
avd d21314
avdd21314
当前监听地址： ('127.0.0.1', 9000)
----------初始化成功----------
n= 60275702009245096385686171515219896415919644698453424055561665251330296281527
G= (29905514254078361236418469080477708234343499662916671209092838329800180225085, 29405937379755419157903904478921572542806770830401260612308519640632340013l4)
d1= 1541901249988522045598354437538318586664728741797636520754616996475749766872 4
k1= 52414533130858761835820980842527168077142118656552213205728601099803455706124
----------------------------------------
发送P1成功：P1= (76456081157971045370351212819431160421877057382456495772401966201558651491 32, 62125169172371956453512290371452763204046972628985505788748415399988639416l8)
----------------------------------------
收到Public key : [21193966292826643019781989370371400997259785214183619937611971723575087075018, 18248299596220273316125527630059398009617813492607347546997398107224352862399]
----------------------------------------
Q1,e发送成功 (Q1,e)= ((51857953470023984529042939088762438287974004767052914765226170224931937995915, 21303207329374214863724780142781703327942719401883722242496012210126356217677), 80573938165412102536538800690312767614023436674760213358297786283306955935392)
----------------------------------------
success recieve (r,s2,s3): (10439927772086451394632017301658574556940592310045711205231713791557650767 62, 9447980451630655291925717456382129805640579425645218241669909613549897298373, 24182205860910207660381582165727775260712776797491010342850353263736410610638)
----------签名生成成功----------
(10439927772086451394632017301658574556940592310045711205231713791557650767 62, 13636008468928000726787356063927219940496584370168093775696456622800839489934)
----------开始验证签名----------
签名验证结果为
True
```

```
当前监听地址： ('127.0.0.1', 5088)
----------初始化成功----------
n= 60275702009245096385686171515219896415919644698453424055561665251330296281527
G= (29905514254078361236418469080477708234343499662916671209092838329800180225085, 29405937379755419157903904478921572542806770830401260612308519640632340013l4)
d2= 36007658161302183751510136015401354195840828687610974377368726866179270664134
k2= 50467874969976218844057213194295692951651564874364143939083943919472840630630
k3= 62467066838462385735900542370772561665282896713077943235396234606406286734 0
public key: (21193966292826643019781989370371400997259785214183619937611971723575087075018, 18248299596220273316125527630059398009617813492607347546997398107224352862399)
----------Public Key 生成成功----------
pk (21193966292826643019781989370371400997259785214183619937611971723575087075018, 18248299596220273316125527630059398009617813492607347546997398107224352862399)
```