# 使用说明

1. 密码库调用直接import

```
from LB_crypto.math import *
from LB_crypto.SM4 import *
from LB_crypto.SM2 import *
from LB_crypto.SM3 import *
from LB_crypto.DS import *
```

2. SM4

   SM4初始化需要输入密钥。

   SM4两种工作模式为CTR与OFB。

   SM4_CTR(file_path, IV, MODE) 输入参数对应为 文件路径、初始向量、加解密模式（1为加密 0为解密）

   SM4_OFB(file_path, IV, n,MODE) 输入参数对应为 文件路径、初始向量、选取比特数、加解密模式（1为加密 0为解密）

   示例如下：

```
s = SM4('557cfb9c1c78b048ae02bf5c88bc781a')
s.SM4_CTR('test/SM4_CTR_test.txt', 0, 1)
s.SM4_CTR('test/SM4_CTR_test1.txt.SM4_CTR', 0, 0)
```

```
s.SM4_OFB('test/SM4_OFB_test.txt', '1996aaaa1ba34b3cadc348a330e018e0', 6, 1)
s.SM4_OFB('test/SM4_OFB_test1.txt.SM4_OFB', '1996aaaa1ba34b3cadc348a330e018e0', 6, 0)
```

3. SM2

   初始化输入椭圆曲线参数p,a,b,以及坐标参数Par

   加密调用需要输入明文m、G点和公钥PB点以及随机数k

   解密调用需要输入密文c和私钥d

   示例如下：

```
s = SM2(
    46517903151725473244214274887871634626171550704246252065 59,
    45988629358397366698090898885240207180898902304957509861 17,
    59659525405935472641529421649106912128837822098991736876 9,
    192
)
res1 = s.SM2_encrypt(
    '0x656e6372797074696f6e207374616e64617264',
    18349684876006478245144101402690643624591990602147572219 52,
    66972603455005182691778320537844117786519722001186891730,
    29899621541032548108048457048597758551032791694878150940 90,
    42719221795797698761894378500484483024734101071410465979 06,
    13807007380171794248497925455638702183951081399725155401 49
)
```

4. SM3

直接调用hash_get(m)得到字符串m的十六进制哈希值。

5. ElGamal DS

   初始化传入模数p和生成元g

   签名时需要私钥x、随机数k和明文M

   验证时需要公钥y、签名和明文M

   示例如下：

```
s = ElGamal_DS(
    831405185079551754106024075111536077567801699902164413420827763748903920817 47,
    839292043824743499977333590292458414640447575266251713154230983195445608929 9
)
s1, s2 = s.Sign(
    328184395775097434154144979187402537428854741120972941162970079238285513103 68,
    321594916339522944784435264261590166162886288429157816640188590959399579454 61,
    '是 谁 憋 疯 了'
)
assert s.Vrfy(
    fast_pow(s.g, 32818439577509743415414497918740253742885474112097294116297007923828551310368, s.p),
    s1,
    s2,
    '是 谁 憋 疯 了'
)
```

6. test

   test函数直接运行可以测试，并且生成函数关系调用图，生成这个图需要一定的依赖