

运行从设置大质数，做循环域，设置参与者人数，t门限值，设置密钥值k，到自动出门限值，

最后输入各种子密钥恢复秘密值k。

其中，每个人的子密钥啥的按照顺序来，前面是编号，后面是秘密份额

（鉴于不了解核心算法的运算公式，只能恢复5-3个人的量。）

可以仿真数据了。

最新的可以运行的文件 shamir\_test.py

该算法就计算开销推演能说明一定问题：密钥长度128bit，人数在（5-40），t值（3-25），但是恢复的结果有一定问题，恢复算法按照拉格朗日公式来的，100以内随便恢复

有解决正确率的理论说明见网址：

<https://blog.csdn.net/haiminhuang/article/details/102716774>

解密过程该是数据溢出有问题

但是算力能说明了