攻防世界crypto easy_ECC

原创

发发发发哥哥 于 2019-10-16 19:13:15 发布 3117 收藏 2

分类专栏： crypto 文章标签： 攻防世界 easy_ECC ctf crypto

本文链接：https://blog.csdn.net/qq_43550956/article/details/102592719

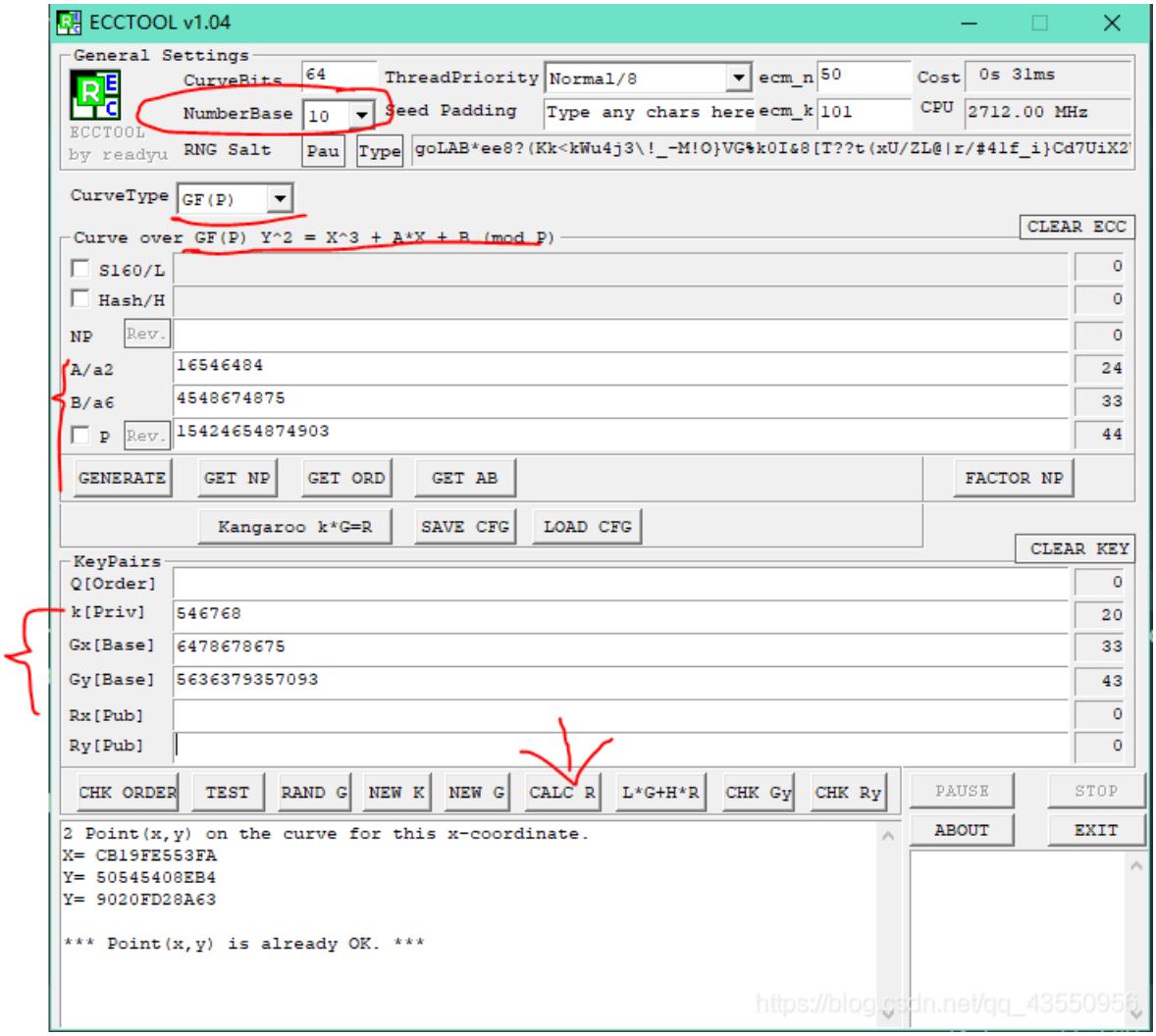
攻防世界easy_ECC

第一次写博客

因为写到这题不会，然而找不到答案，最后决定自己写个答案！

主要是使用了*ECCTOOL*这个软件

下面开始：

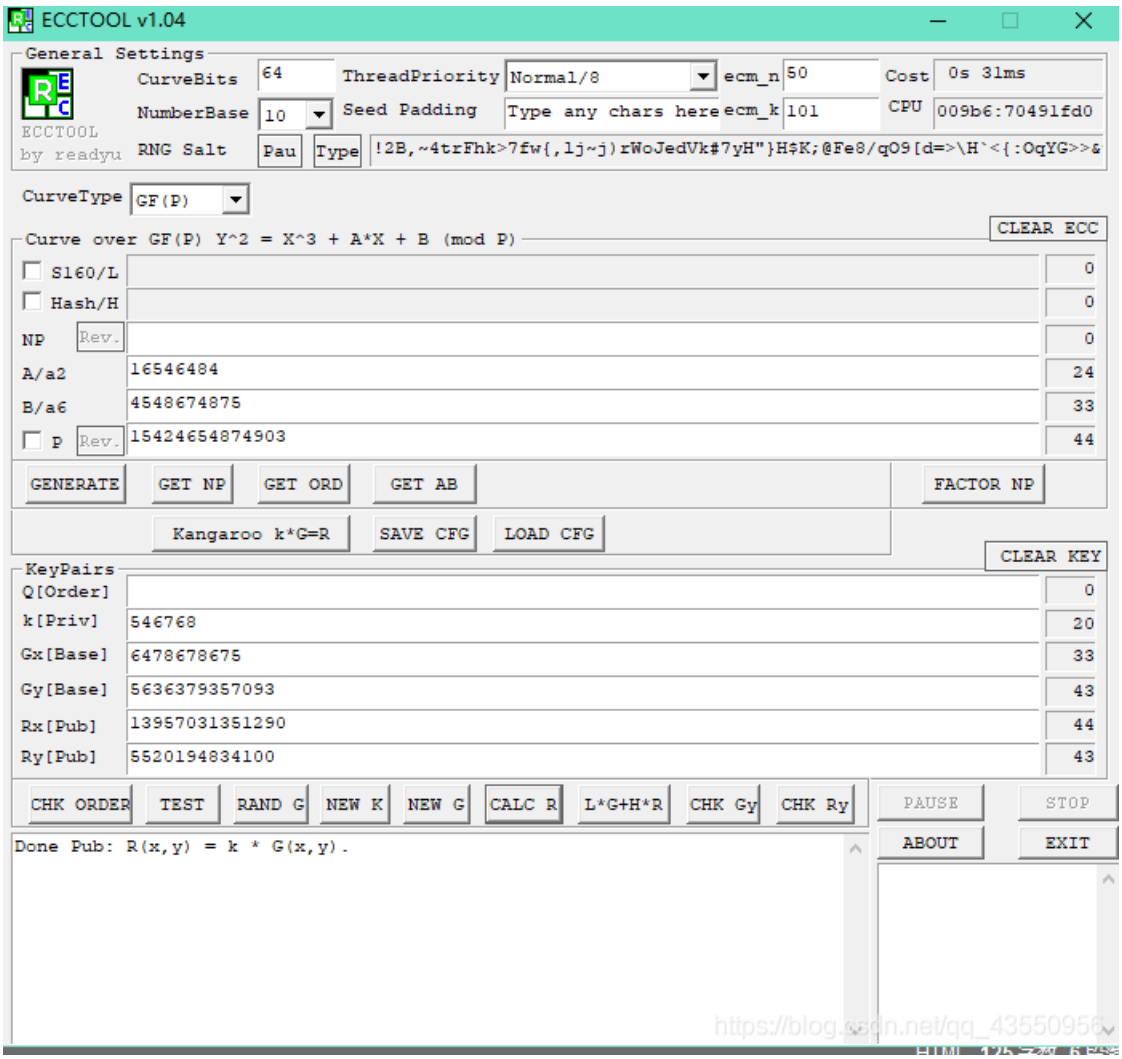


首先我们选择数据为十进制，其次椭圆曲线类型为G§，接着输入a、b、p还有下面的GX,GY以及k后，点击CALC R即可得到RX,RY,然后相加就得到答案了。

rx = 13957031351290

ry = 5520194834100

rx + ry = 19477226185390



第一次写博客有点水额，就这样！