Ez_equation

Description

怎么来解这个二元多次的方程呢？？？

hint1:e较小，怎么解一个有较小根的模方程呢?

hint2:small_roots使用

Solution

考虑消掉m然后直接用small_roots求解e，得到e=8,e=6的两个密文，共模攻击得到m^2,然后pad函数同Signin里面的简单移位填充一样，所以简单的移位开根号就ok