BabyDH 2

本题主要考查选手阅读论文能力、编程能力，要求选手对于格归约算法、Coppersmith方法有一定了解。

题目描述

题目中服务端模拟Alice与Bob两方进行了一次DH密钥交换，随后我们可以作为第三方与Alice进行DH交换，同时提供了一个可以多次访问的额外Oracle，可以泄露出我们与Alice协商出来的点x坐标的低比特位数值。我们需要恢复出Alice与Bob协商出的共享密钥。

求解思路

本题中的场景相当于求解椭圆曲线隐藏数问题（ECHNP）。

选手需要编程复现发表于2022年亚密会的研究成果，注意原论文中考虑的是高比特泄露的场景，因此求解本题的格构造需要做出一定修改。

注意到本题的限时较短，考虑使用flatter工具完成快速格归约。实测发现设置参数n = 5，d = 3，t = 2，在1核的Ubuntu虚拟机上耗时约18s即可完成求解。