**题目名称：rsa\_oula**

**类型：Crypto**

**介绍：**

欧拉函数是积性函数 ——若m,n互质，φ(mn)=φ(m)φ(n)

但是当m=n的时候是不成立的。欧拉函数φ(n)是小于或等于n的正整数中与n互质的数的数目

如果m=n，则其中一个求欧拉函数计算的时候不需要减去自己。即φ(m\*m)=(m-1)\*m

**解题步骤：**

**第一步：**分析加密脚本



发现rsa的公钥n的因子都为p

3～5次可以直接开根判断是否可以开到整数根

这边如果了解欧拉函数的定理，和常规解rsa的区别就在于计算phi（欧拉函数）上。

**第二步：**编写解密脚本



**简要总结：**了解rsa欧拉函数的定义。如何求解因子为同一个数的欧拉函数。