2024黄鹤杯Crypto easycry

by zijeff

打开题目，我们需要关注这道题的质数生成逻辑。这道题的质数选取是根据以下规则所生成的：

$$4p - 1 = D \times V^2$$

其中D是给定列表中的某个整数，V是随机生成的2048bits的正整数。

这道题应该是属于论文题，对于这种满足$4p-1$形式的质数等式，我们可以利用基于**"复杂乘法 / 特殊构造椭圆曲线 + n 次除法多项式 ψ_n"** 的方法来暴露p。具体的数学原理我也不太清楚，但是在浏览器上搜索相应的关键词时，可以找到对应的sagemath代码实现。

作者及其代码**链接：**https://github.com/pwang00/Cryptographic-Attacks/tree/master/Public%20Key/Factoring

由于这个标准脚本每次只是针对一个D进行尝试分解，所以这道题我们直接多试几次，最后可以确定$D = 427$。

从而得到完整脚本具体可见仓库，得到最后解密脚本为：

```
from Crypto.Util.number import *

p = ...
q = ...
n = p*q
c = ...
e = 65537
phi = (p - 1)*(q - 1)
d = inverse(e, phi)
m = pow(c, d, n)
print(long_to_bytes(m))
```

flag为：***flag{7c4a8d09ca3762af61e59520943dc26494f8941b}***