

HWS CTF 2023

1、ezRsa

题目附件代码如下：

```
from Crypto.Util.number import getPrime
from secret import flag

p = getPrime(512)
print(p,pow(flag, 2, p))

#
412482079973710723630883700852439735510778695041476999618132433355695015420698005
9406402767327725312238673053581148641438494212320157665395208337575556385
131079395635074597746162041412537474892320633362041739441232632845076043288856800
72478669016969428366667381358004059204207134817952620014738665450753147857
```

这里首先第一个点是p到底是哪个，这里的注释其实并不和输出对应

尝试分解因数，可得

4124820799737107236308837008524397355107786950414769996181324333556950154206980059406402767327 Factorize!

Result:		
status (?)	digits	number
CF	154 (show)	4124820799...85 <154> = $5 \cdot 7^2 \cdot 13 \cdot 31 \cdot 31013 \cdot 126037 \cdot 1068789352...11$ <140>

故

```
p=1310793956350745977461620414125374748923206333620417394412326328450760432888568
0072478669016969428366667381358004059204207134817952620014738665450753147857
pow(flag,2,p)=4124820799737107236308837008524397355107786950414769996181324333556
950154206980059406402767327725312238673053581148641438494212320157665395208337575
556385
```

题目说ezRsa，那这里就当rsa题做

只有一个素数p，则 $n=p$ ， $\phi(n)=p-1$ ，

由 $\text{pow}(\text{flag},2,p)$ ，得 $e=2$

此时发现e和phi不互素，参考https://blog.csdn.net/qq_57235775/article/details/132575196，利用sagemath求解一个模质数p意义下的方程 $x^e = c$ 的解

```

e=2
p =
131079395635074597746162041412537474892320633362041739441232632845076043288856800
72478669016969428366667381358004059204207134817952620014738665450753147857
c =
412482079973710723630883700852439735510778695041476999618132433355695015420698005
9406402767327725312238673053581148641438494212320157665395208337575556385
R = Zmod(p)['x']
(x,) = R._first_ngens(1)
f = f.monic()
print(f.roots())

```

得到

```

[(1310793956350745977461620414125374748923206333620417394412326327146759984606515
3978657975398261302535968199127597145828004727119047657179535038810099310932,
1),
(13040004482820526093820693618708125830699182230406913376202407698904962835203626
640653836925,
1)]

```

经验证, x为

13040004482820526093820693618708125830699182230406913376202407698904962835203626
640653836925, 可得flag

```

>>> long_to_bytes(13040004482820526093820693618708125830699182230406913376202407698904962835203626640653836925)
b'flag{9971e255f0c020e8e57fbae75f43d7fb}'

```

```
flag{9971e255f0c020e8e57fbae75f43d7fb}
```