

李汶峰的write up

笔记本: My Notebook

创建时间: 2023/11/19 21:31

更新时间: 2023/11/19 21:55

作者: y4zh40nt

李汶峰的write up

2023.11.19 21:54

ezrsa

虽然就只做出一道题，但还是要认真写一下wp的。本题给的代码很少，首先给了一个512位的素数，然后就直接输出两个量了，一个是p，一个是flag平方后与p求模。由于数据没有标出哪个是p哪个是pow，就默认前p后pow了。没想在这里也会设一个坑.....我的做法是首先创建一个有限域R，x是一个生成元，并获得一个模p的整数环，将该整数集合放入有限域里。然后定义一个在有限域中的函数f，根据题目可写出函数的表达式，并求解该方程的根，再将根列表返回到res中，经过不断地尝试，最终找到flag的是在res[1][0]。代码如下，用sagemath运行。

```
from Crypto.Util.number import *

c =
412482079973710723630883700852439735510778695041476999618132433355695015420698005940640276732772
5312238673053581148641438494212320157665395208337575556385

p =
131079395635074597746162041412537474892320633362041739441232632845076043288856800724786690169694
28366667381358004059204207134817952620014738665450753147857

R.<x> = Zmod(p)[]
f = x^2 - c
res = f.roots()
flag = long_to_bytes(ZZ(res[1][0]))
print(flag)
```

```
b'flag[9971e255f0c020e8e57fbae75f43d7fb]'
```