

you_raise_me_up

发表于 2021-01-04 更新于 2021-01-21 分类于 [Challenge](#) , [2020](#) , [网鼎杯](#) , [青龙场](#) , [Crypto](#)
[Challenge](#) | [2020](#) | [网鼎杯](#) | [青龙场](#) | [Crypto](#) | [you_raise_me_up](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

本WP由Vanish提供

题目考点

- 离散对数

解题思路

```
1 #!/usr/bin/env python
2 # -*- coding: utf-8 -*-
3 from Crypto.Util.number import *
4 import random
5 n = 2 ** 512
6 m = random.randint(2, n-1) | 1
7 c = pow(m, bytes_to_long(flag), n)
8 print 'm = ' + str(m)
9 print 'c = ' + str(c)
10 # m = 391190709124527428959489662565274039318305952172936859403855079581402770986890308469084735451207885386318986881041563704825943945069343345307381099559075
11 # c = 6665851394203214245856789450723658632520816791621796775909766895233000234023642878786025644953797995373211308485605397024123180085924117610802485972584499
```

题中我们的flag在m的指数位置，所以这题是解一个DLP(离散对数问题)

发现题中的 $n = 2^{512}$ ，所以 $\phi(n) = 2^{511}$ ；即本题模数的欧拉函数具有smooth的性质，即其是由很多小素数乘积而来，所以可用Pohlig Hellman 算法来解决这个DLP，sage的discrete_log用的方法就包括Pohlig Hellman算法，exp:

```
1 m = 391190709124527428959489662565274039318305952172936859403855079581402770986890308469084735451207885386318986881041563704825943945069343345307381099559075
2 c = 6665851394203214245856789450723658632520816791621796775909766895233000234023642878786025644953797995373211308485605397024123180085924117610802485972584499
3 n = 2 ** 512
4 m = Mod(m,n)
5 c = Mod(c,n)
6 discrete_log(c,m)
```

得到结果之后数字转字符串即可

```
1 import libnum
2 d = 56006392793405651552924479293096841126763872290794186417054288110043102953612574215902230811593957757
3 print(libnum.n2s(d))
```

Flag

```
1 flag{5f95ca93-1594-762d-ed0b-a9139692cb4a}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/网鼎杯/青龙场/Crypto/hcTTwuy2RWrs5DDHG1RSp7.html>
- 版权声明: 本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[#Challenge](#) # [2020](#) # [Crypto](#) # [网鼎杯](#) # [青龙场](#)
[easy_ya](#)
[rua](#)