

# happy

发表于 2021-03-05 更新于 2021-03-15 分类于 [Challenge](#) , [2020](#) , [SWPU CTF 2020](#) , [Crypto](#)  
[Challenge](#) | [2020](#) | [SWPU CTF 2020](#) | [Crypto](#) | [happy](#)

[点击此处](#) 获得更好的阅读体验

## WriteUp来源

[官方WP](#)

## 题目描述

## 题目考点

- RSA

## 解题思路

EXP

```
1 #exp.happy
2 #python3
3 import binascii
4 import gmpy2
5 from z3 import *
6 s = Solver()
7 p=Int('p')
8 q=Int('q')
9 s.add(q*q*p**3 == 1285367317452089980789441829580397855321901891350429414413655782431779727560841427444135440068248152908241981758331600586)
10 s.add(p*q+q*p**2 ==1109691832903289208389283296592510864729403914873734836011311325874120780079555500202475594)
11 if s.check() == sat:
12     print(s.model())
13 n=0x989f5774c6f199031dc64d5aad7907665ea5e03cde2d74da21
14 e=0x872a335
15 c=0x7a7e031f14f6b6c3292d11a41161d2491ce8bc67ef1baa9e
16 p = 1158310153629932205401500375817
17 q = 827089796345539312201480770649
18 phi=(p-1)*(q-1)
19 d=gmpy2.invert(e,phi)
20 m=pow(c,d,n)
21 print(binascii.unhexlify(hex(m)[2:].strip("L")))
```

## Flag

```
1
2
```

- 本文作者: [CTFHub](#)
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Crypto/eHUJnHtEn14JEtHtj7f6gL.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 #SWPU CTF 2020](#)

[找找吧](#)

[Yusa的密码学课堂-ECB](#)