little RSA

发表于 2021-01-08 分类于 Challenge， 2020， CSICTF， Crypto
Challenge | 2020 | CSICTF | Crypto | little RSA

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/crypto/2020/07/21/little-RSA.html

by `anishbadhri`

题目描述

> *The flag.zip contains the flag I am looking for but it is password protected. The password is the encrypted message which has to be correctly decrypted so I can useit to open the zip file. I tried using RSA but the zip doesn't open by it. Can you help me get the flag please?*

***Files**:*

- *a.txt*
- *flag.zip*

题目考点

- *RSA n分解*

解题思路

The file `a.txt` has a really small value of `n`. The factors of this value can be brute-forced for directly and then an integer is obtained. The only file in `flag.zip` is `flag.txt` which is password-protected. The password to this file is the integer which is obtained.

```
import mod

c=32949
n=64741
e=42667

p = None
for i in range(2,n):
  if n % i == 0:
    p = i
    break

q = n // p
em = mod.Mod(e, (p-1) * (q-1))
d = int(1//em)
cm = mod.Mod(c,n)
ans = int(cm ** d)
print(ans)
```

Flag

```
csictf{gr34t_m1nds_th1nk_4l1ke}
```

- ***本文作者：** CTFHub*
- ***本文链接：** https://writeup.ctfhub.com/Challenge/2020/CSICTF/Crypto/nx2ZVsc7z3FufzENJ9YkY5.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 # CSICTF
honormap01

The-Climb