Quick Math

发表于 2021-01-08 分类于 Challenge， 2020， CSICTF， Crypto
Challenge | 2020 | CSICTF | Crypto | Quick Math

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/Quick-Math.html

by `anishbadhri`

题目描述

> *Ben has encrypted a message with the same value of 'e' for 3 public moduli* `n1 = 86812553978993` `n2 = 81744303091421` `n3 = 83695120256591` *and got the cipher texts* `c1 = 8875674977048` `c2 = 70744354709710` `c3 = 29146719498409`
> *Find the original message. (Wrap it with csictf{})*

题目考点

- *RSA e过小*

解题思路

The given problem is a typical example of hastad attack. Given 3 pairs of `n` *and* `c` *with the same value of* `e=3`*, the original message can be decoded.*

```
from pwn import remote
from sympy.ntheory.modular import crt
from gmpy2 import iroot
e = 3
N = [86812553978993, 81744303091421, 83695120256591]
C = [8875674977048, 70744354709710, 29146719498409]
resultant, mod = crt(N,C)
value, is_perfect = iroot(resultant,e)
print(bytes.fromhex(str(value)).decode())
```

Flag

```
csictf{h45t4d}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Crypto/dDkzYd5UMTyQkMArL6og71.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
The-Climb
Login-Error