Rivest Shamir Adleman

发表于 2021-01-08 更新于 2021-01-09 分类于 Challenge， 2020， CSICTF， Crypto
Challenge | 2020 | CSICTF | Crypto | Rivest Shamir Adleman

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/crypto/2020/07/18/Rivest-Shamir-Adleman.html

by `anishbadhri`

题目描述

> *These 3 guys encrypted my flag, but they didn't tell me how to decrypt it.*

题目考点

解题思路

The values of `n` is generated using a small prime. One of the primes can be searched using brute-force and the message can then be decrypted.

```
import mod
f = open("enc.txt").read().split('\n')
n = int(f[0].split()[2])
e = int(f[1].split()[2])
c = int(f[2].split()[2])
p = None
for i in range(2,n):
  if n % i == 0:
    p = i
    break
q = n // p
phi = (p-1) * (q-1)
em = mod.Mod(e, phi)
d = int(1 // em)
cm = mod.Mod(c, n)
dec = int(cm ** d)
print(bytes.fromhex(hex(dec)[2:]))
```

Flag

```
csictf{sh0uld'v3_t4k3n_b1gg3r_pr1m3s}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Crypto/tTTyzhh9jCXFu8DRT9Ezrc.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
Login-Error
Modern Clueless Child