HGAME 2022 Week2 writeup by Seon

Crypto

RSA Attack

已知e,n,C求M

通过powershell打开yafu

运行.\yafu-x64.exe "factor(700612512827159827368074182577656505408114629807)"

得到

factors found

```
P24 = 978782023871716954857211
P24 = 715800347513314032483037
```

运行python

```
import libnum
from Crypto.Util.number import long_to_bytes

c = 122622425510870177715177368049049966519567512708
n = 700612512827159827368074182577656505408114629807
#n = int("",16)
e = 65537
#e = int("",16)
q = 978782023871716954857211
p = 715800347513314032483037

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)   # m 的十进制形式
string = long_to_bytes(m)  # m明文
print(string)  # 结果为 b‘ m ’ 的形式
```

得到flag

hgame{SHorTesT!fLAg}