HGAME 2020 Week3 wp

sage 就做了一题白给的保命。

LikiPrime

还是白给RSA，别看那么多比上次RSA多出来的代码唬人，还是**已知 公钥（n, e） 和 密文 c 求 明文 m**

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

c = 0x6cd55a2bbb49dfd2831e34b76cb5bdfad34418a4be96180b618581e9b6319f86
n =
10853984726857399027523402435467243724652508507660551696032000572274158989864 1
#n = int("",16)
e = 65537
#e = int("",16)
q = 333360321402603178263879595968004169219
p = 325593180411801742356727264127253758939

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
```

copy from https://blog.csdn.net/vhkjhwbs/article/details/101160822

结果就出来了，纯纯跟week2RSA一样，我还以为这次n,e很大会有不一样，特地把RSA学清楚了，结果就三秒。