HGAME 2021 Week2 WriteUp

Crypto

WhitegiveRSA

白给的 RSA 解密题。已知 N e c 三个参数，利用 python 脚本（见附件的代码1）即可计算出flag 。

其中 p q 为 大数 n 的质因数分解，使用了工具网站 http://factordb.com/ 。

MISC

DNS

简单的 dns 题，根据题目的 'dns' 提示，在流量包中找到疑似域名 flag.hgame2021.cf ，获取dns解析信息，在 txt 记录中发现 flag。

使用了在线 dns 解析网站 https://myssl.com/dns_check.html 。

附件

代码1

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

c = 747831491353896780365654517748216624798517769637260742155527
n = 882564595536224140639625987659416029426239230804614613279163
e = 65537
# q p 为 n 的质因数分解
q = 857504083339712752489993810777
p = 1029224947942998075080348647219

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