CTF WEEK3 WP

CRYPTO

1.LikiPrime

是一道比较基础的RSA解密题。

通过在线网站 http://www.factordb.com/index.php 解出 p 与 q。

然后由以下代码得到 flag：

```python
from libnum import s2n, n2s
import gmpy2

n = 4943876460977174846069696722821224491042114383968689683
e = 65537
c = 189613871951237786113947654705975292221854108665244884686
p = 25911708601320262777624676792244153094181888755312542730
q = 190797007524439073807468042969529173669356994749940177399
phi_n = (p-1)*(q-1)
d = gmpy2.invert(e, phi_n)
result = pow(c, d, n)
print(n2s(int(result)))
```

```
b'hgame{Mers3nne`Pr!Me`re4lly_s0+50-li7tle!}'
请按任意键继续. . .
```