

20-Web-Week2-Writeup

Crypto

WhitegiveRSA

1. 看到题目中所给的信息

描述

$N = 882564595536224140639625987659416029426239230804614613279163$

$e = 65537$

$c = 747831491353896780365654517748216624798517769637260742155527$

这三个值分别是模值、公钥指数、密文，应该是利用RSA加密算法来求明文

2. 进入[分解模值的网站](#)

将模值 $N = 882564595536224140639625987659416029426239230804614613279163$ 输入，得到两个素数

$p = 857504083339712752489993810777$

$q = 1029224947942998075080348647219$

The screenshot shows the factordb.com website interface. At the top, there's a search bar with the number 882564595536224140639625987659416029426239230804614613279163 entered. Below the search bar, there's a table with the following data:

Result:		
status (2)	digits	number
FF	60 (show)	$8825645955...63_{<60>} = 857504083339712752489993810777_{<30>} \cdot 1029224947942998075080348647219_{<31>}$

Below the table, there's a section for "More information" and "ECM". At the bottom, there's a footer that says "factordb.com - 14 queries to generate this page (0.01 seconds) (limits) (Imprint) (Privacy Policy)".

3. 用Anaconda自带的Jupyter里的python3运行解明文的代码，得到flag

The screenshot shows the Jupyter Notebook interface. At the top, there's a browser window with the URL localhost:8888/tree#notebooks. Below the browser window, there's a Jupyter logo and a "Quit" button. Below the logo, there's a "Files" tab selected. Under the "Files" tab, there's a table with the following data:

Name	Last Modified	File size
3D Objects	5 小时前	
ansel	5 个月前	
Contacts	5 小时前	
Desktop	4 分钟前	
Documents	5 小时前	
Downloads	5 小时前	
Favorites	5 小时前	
Links	5 小时前	
Music	5 小时前	
OneDrive	5 小时前	
Pictures	5 小时前	
Saved Games	5 小时前	
Searches	5 小时前	
source	5 个月前	
UIDownloader	2 个月前	
Videos	5 小时前	
WestWorldVPN	4 小时前	
Untitled.ipynb	运行 几秒钟	6.34 KB

jupyter Untitled1 最后检查: 4 小时前 (自动保存) Logout

File Edit View Insert Cell Kernel Widgets Help 未连接成功 可信的 Python 3

```
In [3]: #!/usr/bin/env python3
# coding:utf-8
#power by jedi

import gmpy2
import binascii

n = 882564595536224140639625987659416029426239230804614613279163
# p 和 q通过在线网站http://factordb.com/index.php分解
p = gmpy2.mpz(857504083339712752489993810777)
q = gmpy2.mpz(1029224947942998075080348647219)
e = gmpy2.mpz(65537)
phi_n = (p-1)*(q-1)
d = gmpy2.invert(e, phi_n)
c = gmpy2.mpz(747831491353896780365654517748216624798517769637260742155527)

m = pow(c, d, n)
print("十进制:\n%s"%m)
m_hex = hex(m)[2:]
print("十六进制:\n%s"%(m_hex,))
#print("ascii:\n%s"%((binascii.b2a_hex(hex(m)[2:])).decode('hex'),))
print("ascii:\n%s"%(binascii.a2b_hex(m_hex).decode("utf8"),))

十进制:
2559974471936861332250695601896749831380586717227729822077
十六进制:
6867616d657b730777e794f555f6b4e6f572b52354021d
ascii:
hgame{w0w~y0U_kNoW+R5@!}
```

```
<html>
#!/usr/bin/env python3
# coding:utf-8
#power by jedi

import gmpy2
import binascii

n = 882564595536224140639625987659416029426239230804614613279163
p = gmpy2.mpz(857504083339712752489993810777)
q = gmpy2.mpz(1029224947942998075080348647219)
e = gmpy2.mpz(65537)
phi_n = (p-1)*(q-1)
d = gmpy2.invert(e, phi_n)
c = gmpy2.mpz(747831491353896780365654517748216624798517769637260742155527)

m = pow(c, d, n)
print("十进制:\n%s"%m)
m_hex = hex(m)[2:]
print("十六进制:\n%s"%(m_hex,))
#print("ascii:\n%s"%((binascii.b2a_hex(hex(m)[2:])).decode('hex'),))
print("ascii:\n%s"%(binascii.a2b_hex(m_hex).decode("utf8"),))
</html>
```

得到flag

```
hgame{w0w~y0U_kNoW+R5@!}
```

