RSA算法

转载

weixin_30905133 于 2018-07-11 15:56:00 发布 64 收藏
原文链接：http://www.cnblogs.com/Paranoid-4/p/9294964.html

RSA算法涉及三个参数n,e,d。私钥为n,d，公钥为n,e。（其中n为两个大素数p,q的乘积）

d是模$ varphi(n) $的逆元， $ varphi(n) $是n的欧拉函数。

假设c是密文，m是明文，则加密过程如下： $ cequiv m^e mod n $

解密过程： $ mequiv c^d$ mod n

n,e是公开的情况下，如果想要知道d的值，必须要将n分解计算出n的欧拉函数值，而n是两个大素数p,q的乘积，将其分解可以通过在线网站http://factordb.com

ctf的Crypto题型中难免会出现RSA加密，在做题之前，要将数据处理成可以做题的模式。一般题目不会直接给出具体参数的值，而是通过别的方式给出，则我们要做的就是将这些参数提取出来

1、pem文件：针对这类文件，我们可以直接使用Linux下的openssl提取。

```
root@paranoid:~# cd Desktop
root@paranoid:~/Desktop# openssl rsa -publin -text -modulus -in warmup -in publi
c.pem
```

2、pcap文件：针对这类文件，我们可以使用wireshark追踪一下。

下面以2017届广东省强网杯的这道crypto为例讲解一下RSA解法

首先根据下载下来的文件给出的参数n，可以知道第一步应该是到在线网站http://factordb.com去对n进行因数分解得到p,q的值

Search | Sequences | Report results | Factor tables | Status | Downloads

9668089326274971906358592360549603490994639752273505642653843732803366998533872540706628 Factorize! (?)

Result:		
status (?)	digits	number
CF	2471 (show)	9668089326...48<2471> = 2^5 · 3021277914...39<2470>

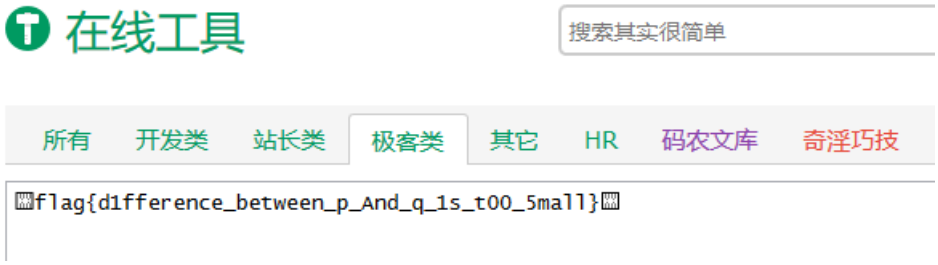
然后上代码，求明文信息

```
import gmpy2
n = 9668089326274971906358592360549603490994639752273505642653843732803366998533872540706628812659375651630007586061543087579
e = 65537
c = 16850291008885829563431507024437740955656763713973630808218636900322777193640732178355779562427916216230520043644690397638
p = 31093551302922880999883020803665536616272147022877428745314830867519351013248914244880101094365815998050115415308439610066
q = 31093551302922880999883020803665536616272147022877428745314830867519351013248914244880101094365815998050115415308439610066
d = int(gmpy2.invert(e , (p-1) * (q-1)))
m = pow(c ,d ,n)
print(m)
print(hex(m))
```

```
C:\Users\HP>cd Desktop

C:\Users\HP\Desktop>python a.py
93963134927620042394105413140815215028939038458857622011460526094079774361371732287208512192994694116385906 9
0x666c61677b643166666572656e63655f6265747765656e5f705f416e645f715f31735f7430305f356d616c6c7dL
```

运行后再进行hex转string，然后flag即出~



转载于:https://www.cnblogs.com/Paranoid-4/p/9294964.html