i春秋-Crypot-RSA？

转载

weixin_30401605 于 2018-06-06 20:38:00 发布 65 收藏
文章标签： php
原文链接：http://www.cnblogs.com/nldyy/p/9147178.html


```
N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb454a34dab7684589bc32b19eb27cffff8c07179e349ddb62898ae896f8c681796052ae1598bd41f35491175c9b60ae2260d0d4ebac05b4b6f2677a7609c2fe6194fe7b63841cec632e3a2f55d0cb09df08eacea34394ad473577dea5131552b0b30efac31c59087bfe603d2b13bed7d14967bfd489157aa01b14b4e1bd08d9b92ec0c319aeb8fedd535c56770aac95247d116d59cae2f99c3b51f43093fd39c10f93830c1ece75ee37e5fcdc5b174052eccadcadeda2f1b3a4a87184041d5c1a6a0b2eeaa3c3a1227bc27e130e67ac397b375ffe7c873e9b1c649812edcd

e=0x1

c=0x4963654354467b66616c6c735f61706172745f736f5f656173696c795f616e645f7265617373656d626c65645f736f5f637275646564656c797d
```

尝试分解N，发现无论是http://factordb.com/index.php?或者是使用yafu都不行，再仔细观察发现e=1。好像发现了什么

$m^e \bmod n = c$，因为e=1

所以可以得出

m = c+k*n （k=0，1，2，3，4....）

于是可以进行尝试，发现k=0的时候，刚刚就得到了flag

（尝试写代码，但代码运行总是不成功，就放弃了）

本人小白一枚，只为自己巩固知识，不喜勿喷

转载于:https://www.cnblogs.com/nldyy/p/9147178.html