网鼎杯-writeup-第二场-babyRSA

原创

TaiJi1985 于 2018-08-24 12:00:25 发布 2804 收藏 2

分类专栏： 网络安全

本文链接：https://blog.csdn.net/TaiJi1985/article/details/82015721

题目给出了 n , e , d 这样加密解密的所有要素就都有了。 加密用 (n,e) ， 解密用 （n,d）

解密公式 MC = pow(C,d,n) ,即 密文C的d次方 模上 n。

当然题目给出的密文enc 是 Base64编码， 解码为字符串后，还要转换成 一个大整数。

用到了base64库和libnum库。

```
d = 171667543985758425014232627985840717336387122108163758500542139626729279212540485673813409388397427

n = 365848589691553391654453815696801609393691558975114732077589431735072735814004481321693204054611153

e = 65537

# 题目给出的代码加上三个单引号就构成了一个多行字符串。

enc = '''ICCHhzayltixzeuA++PPbDwlialEjQuDBx38ecgQwl5lOTnemrcWYbDeQkIIE5oPQOcSmNX8nmcD
gyl4O05jYD7VmDcgwQTIgHeOLovcqGVPHEW4hHSmIR3BB/CBjb3/5+HfeifXF1w+/o148o76D9Nt
TBYaLk8CTjOscT23PBI8w+WPhHBIPaSbJlDuaHA4Ie6ojsE6mM7cp79dz7bCdAf5a2tUGA6AbNCu
P1WVnsBI+IIHX8EDELmBnQ5c13JuYnjHL5lmqL3QK88QwQQ4h/3vUODAWBuzn8meWBgfpqxmHTGJ
+du2mRoUTpUBzZy2OxrKdD8J11Hc+yJJJkQe5QgqACbM00K0rTv7kIyB2aB/gUGLNP4IOwV09avU
pzLS2PPLgeAVP/JSGYlXZTthy4FlqL5pMN4/+swNnEN6Z+lPzLNe0JB0uNN/yPJ3C3lsSuoFLh0I
nYI46Tycs8vz1nHQWjQdE6hpD/HpyCbjoC2BE4ugCJKUtmp7mbyDxkjkn5ZkHhrJXK/DF4NQgYmf
kZxyLOWsI2UC1niq5qGD3SIspW8NcupyGakYVzD1R9PP8xoxpkjX62f7myXLMmacbJgYe7ExeWdY
XMZd76Tnqu9IJJwEO43LZz+w2rqH8DIlhr64JenxaDcIixqFzKmkk6WK71VVT3t788ZxaNhG2yo='''


print enc
import base64
import libnum
enc = base64.b64decode(enc)
enc = libnum.s2n(enc)
print enc

MC = pow(enc,d,n)
print "MC = ",MC
print libnum.n2s(MC)
```

结果

```
MC =  436781373568887824525751565285366931498183565909514177451304564550015112465013704
472405699788410707029785953643815454408255474233298388457559469682568301340479261424860
399542281245430588896589649118386518602185685757322224766970361865825657359897289202778
165774548644492638960657714603810592811684803301803684576619127411644646852589392255959
802765440908303176283203127589636197018893388399231948526003680182561488436153337913189
429565222653205468414692552701022709051077773631336817616137341118503042416400425591452
516511082568126089757353837328489552436356470072762485105510012067793728575977645582158
971869784146972084540458291895969832468315723794586815081653395687761086970639550131646
427482034834196467246513403311197831646726074314200449443051868728850985245400564319305
966751651427678469963461344402107385020805180752606613359667908446008164353837453441514
892346939093644672779614208470253203402427527033322463636110682896399697252245236712879
688350222791310199326881474346465023960623110752610117078206560610708303755800160567457
498974418923834869455586138143181672220039690225269065799126029773413598403105509282438
990663906043439208934791837347779077381570438996434866354526952537761994720762313987772
10327898562249853
½¦萎³7xg£ძ%G*硊̱?t~
                    AT
                        ̱*;CPRZ۶УIEþ¥"¯¿_±b
-ª蕊 EC´Tᅔ{M6bbµlX3>Ч꜖ v0~Iἓ&&iJ(c□□,HK颱kτц©□¹ΏN祀EXW2ꞰH-摖ዓ0o@□º ′d+□□dAWǽ©z%□¢IFºKþ@R¾
S.¯_.P0YC̱ □HC¢Yь/ℏ䘮Ȅ@«
\ù)Ⴣº Sȸ̱ {敛¹▯ L¨b        □T□ÿPþµ$]□V!i8̱ flag{w3lC0M3_t0_rS4_w0RlD}6)f¾Ȯþ
→  rsa Xshell
```