RoarCTF 2019 babyRSA writeup

原创

Slightwindsec 于 2020-04-17 23:57:02 发布 767 收藏 1

分类专栏： CTF 文章标签： 动态规划 算法

我的博客：https://blog.slight-wind.com/

做这题看到阶乘一下想到了 gxzy2020 的一题，也是考到了威尔逊定理（Wilson's theorem）：当且仅当p为素数时：(p -1)! ≡ -1 (mod p)。

阶乘只乘到 B，所以把（B+1）乘到（A-1）这一段也补上就得到了威尔逊公式，反之我们可以由用 -1 乘这一段的模反数，就得到了题目中的 (B!)%A 。

exp:

```python
from Crypto.Util.number import *
from sympy import nextprime
A1=21856963452461630437348278434191434000066076750419027493852463513469865262064340836613831066602300959772632397773487317560339056658299954464169264467234407
B1=21856963452461630437348278434191434000066076750419027493852463513469865262064340836613831066602300959772632397773487317560339056658299954464169264467140596

A2=16466113115839228119767887899308820025749260933863446888224167169857612178664139545726340867406790754560227516013796269941438076818194617030304851858418927
B2=16466113115839228119767887899308820025749260933863446888224167169857612178664139545726340867406790754560227516013796269941438076818194617030304851858351026

def f(a,b,P):# a*(a+1)*...*b  (mod P)
    ans=1
    for i in range(a,b+1):
        ans*=i
        ans%=P
    return ans%P

inv1=inverse(f(B1+1,A1-1,A1),A1)
ans1=((A1-1)*inv1)%A1
p=nextprime(ans1)

inv2=inverse(f(B2+1,A2-1,A2),A2)
ans2=((A2-1)*inv2)%A2
q=nextprime(ans2)

e=0x1001
c=75700883021669577739329316795450706204502635802310731477156998834710820770245219468703245302009998932067080383977560299708060476222089630209972629755965140317526034680452483360917378812244365884527186056341888615564335560765053550155758362271622330017433403027261127561225585912484777829588501213961110690451987625502701331485141639684356427316905122995759825241133872734362716041819819948645662803292418802204430874521342108413623635150475963121220095236776428
n=85492663786275292159831603391083876175149354309327673008716627650718160585639723100793347534649628330416631255660901307533909900431413447524262332326591530470679086934819471210690704515628224173576564321718709511846731325542136901233080426973619699863603750609547029206563641441541458128385583653341729359314414240962702061406918146623185626969257679919373697826279084082390873580331654100206901520677157111127322520385884328967584058987090103424678822643627 33

r=(n//p)//q
assert isPrime(r)
d=inverse(e,(p-1)*(q-1)*(r-1))
m=pow(c,d,n)
print(long_to_bytes(m))
# b'RoarCTF{wm-CongrAtu1ation4-1t4-ju4t-A-bAby-R4A}'
```