[NPUCTF2020]EzRSA Writeup

原创

_bestkasscn 于 2021-12-02 14:01:06 发布 139 收藏

分类专栏： CTF 文章标签： 密码学

本文链接：https://blog.csdn.net/bestkasscn/article/details/121675867

[NPUCTF2020]EzRSA

题目描述

```
from gmpy2 import lcm , powmod , invert , gcd , mpz
from Crypto.Util.number import getPrime
from sympy import nextprime
from random import randint
p = getPrime(1024)
q = getPrime(1024)
n = p * q
gift = lcm(p - 1 , q - 1)
e = 54722
flag = b'NPUCTF{******************}'
m = int.from_bytes(flag , 'big')
c = powmod(m , e , n)
print('n: ' , n)
print('gift: ' , gift)
print('c: ' , c)
```

```
#n:  170839412302134897004266364844877382824264714946070988472953353396381775836854579211985691054177346686920727277591393582076672487039524366801831533276061474219323658899833472820464391561766857651436206371073478704019469465016205316655736680683490804108079965822975058899462050528790020289361253153122564705836229136463197791255596912709160645886849973824514127474327229669195134137099873530383754771783851254535671119652597214849971567993556176421315690958103040771310535884830572443407427518049354940876873634169213140415470931185657676096670338595831252753220776175767832478537185161667438582652911353538952399811218#gift:  213549265377668621255332956056096728530330893682588735591191691745477219796068224014982113817721683358650909096989241977595840608799405458502289416595076842774154573624791841025580489452208572064295257963841848380243368312702566458196708508543635051350999572787188236243275631609875253617015664414032058822919469443284453403064076232765024248435543326597418851751586308514540124571309152787559712950209357825576896132278045112177910266019741013995106579484868768251084453338417115483515132869594712162052362083414163954681306259137057581036657441897428432575924018950961141822554251369262248368899977337886190114104#c:  373896063919473795766768414356500550359627645161792247466974552929992939550797143531118157838722332342932328692737057695507861833575750816126358516412604754541302882987326934292409233929895763507973644685183741435775731252515835657960721249606024440376582263651534719221181765817082231364674352083197767386186963751984313386328855005835942945505267632319672828040850861452795305721477916545035657782037881046752700637729619410267136030205990189797733972829234513282718422715506132632858564001991632884737229575447283231825863605466309147580123505065740185726296041589848371307413921259668536578026966750027110853831 9
```

lcm()函数是求两个数的最小公倍数，而最小公倍数和最大公因数满足

```
lcm(a,b)*gcd(a,b) == a*b
```

所以只要找到gcd(a,b)就能求出a*b的值，而题目给出了gift = lcm(p-1,q-1)
n的位数和gift的位数又很接近，所以可以写脚本爆破出phiN的值

exp

```
from Crypto.Util.number import *
import gmpy2

n = 17083941230213489700426636484487738282426471494607098847295335339638177583685457921198569105417734668692072727759139358207667248703952436680183153327606147421932365889983347282046439156176685765143620637107347870401946946501620531665573668068349080410807996582297505889946205052879002028936125315312256470583622913646319779125559691270916064588684997382451412747432722966919513413709987353038375477178385125453567111965259721484997156799355617642131569095810304077131053588483057244340742751804935494087687363416921314041547093118565767609667033859583125275322077617576783247853718516166743858265291135353895239981121
gift = 21354926537766862125533295605609672853033089368258873559119169174547721979606822401498211381772168335865090909689241977595840608799405458502289416595076842774154573624791841025580489452208572064295257963841848380024336831270256645819670850854363505135099957278718823624327563160987525361701566441403205882291946944328445340306407623276502424843554332659741885175158630851454012457130915278755971295020935782557689613227804511217791026601974101399510657948486876825108445333841711548351513286959471216205236208341416395468130625913705758103665744189742843257592401895096114182255425136926224836889997733788619011410 4
c = 37389606391947379576676841435650055035962764516179224746697455292999293955079714353111815783872233234293232869273705769550786183357575081612635851641260475454130288298732693429240923392989576350797364468518374143577573125251583565796072124960602444037658226365153471922118176581708223136467435208319776738618696375198431338632885500583594294550526763231967282804085086145279530572147791654503565778203788104675270063772961941026713603020599018979773397282923451328271842271550613263285856400199163288473722957544728323182586360546630914758012350506574018572629604158984837130741392125966853657802696675002711085383 19
e = 54722
# e与phiN不互素
e = e // 2
for i in range(1000):
    phiN = gift * i
    try:
        d = gmpy2.invert(e, phiN)
        m = pow(c, d, n)
        flag = long_to_bytes(gmpy2.iroot(m,2)[0])
        if b'NPUCTF{' in flag:
            print(flag)
            break
    except:
        pass
```

b’NPUCTF{diff1cult_rsa_1s_e@sy}’