CTF-CRYPTO-RSA-SupplementRabin

原创

大熊何在 于 2020-12-11 01:03:12 发布

分类专栏： CRYPTO

本文链接：https://blog.csdn.net/zippo1234/article/details/111027367

CTF-CRYPTO-RSA-SupplementRabin

有时间就多更新一两题

SupplementRabin

题目分析

1. supplement rabin
2. lcm最小公倍数

开始

1.题目

task.py

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import gmpy2
from libnum import n2s,s2n
from Crypto.Util.number import getPrime

p = getPrime(1024)
q = getPrime(1024)
n = p * q
e = 62674

gift = gmpy2.lcm(p - 1 , q - 1)

flag = 'flag{******}'
m = s2n(flag)
c = pow(m, e, n)

print('n: ', n)
print('gift: ', gift)
print('c: ', c)

# n = 109559521938671090070491712234483617032703161633815954758089779095705921862415727860005247793992511756396325062146597396541678916138770099097334654458503423264116056335778868191195919886661074942515251195266492540440835702995410595290647522552099482080822186521043032475825399927471963124660883198804613013891391176062694077038708350199911547586991183764087300388245611667931738381841744705553717137645158506878154484105331123373095983503919513047864807006783374206336442970598826232080075308261266777861316005803634103191938033070639740468344582304467416029056329621630267602698934415259509721999095833574689828740813
# gift = 456498008077796208627048800977015070969596506807566478158707412898774674426732199416688532474968798984984687758944155818923662150578208746238894393577097596933816901399078617463316332861087812260480213313610385585170148762480877480377698010633747842003425777171012635315939166364466513019420346661685887557872065839736629132505802075822875396741377694500918089173843789526174839060321832022100268187243257213917173221983445662947146747809251663111881830886870180454979426716332773356700423545040000189379843309371468459260828296151157054634095231514373653361915789381498348538500889098973984825991010648504425961736
# c = 23902874401518590749774312249342288719086585891142194370557783300780172560804072949508540317694150448495305001061079730644422247744167766133722720285208978877148534384119717413521202042809262155756276961984677874767764880463048551446484776115861810557603707434471670044376371490182610230771033947385264556993892734001553932248490437651053089588010398503696973690415202127138538380965657171442959984448427032047204186474542169969342271950234721683040896150948277361085477223899205953453218899088108045790949149297604314686221860304621584928202078448566154792679997395489989395648816634498661696514032989876705864881321
```

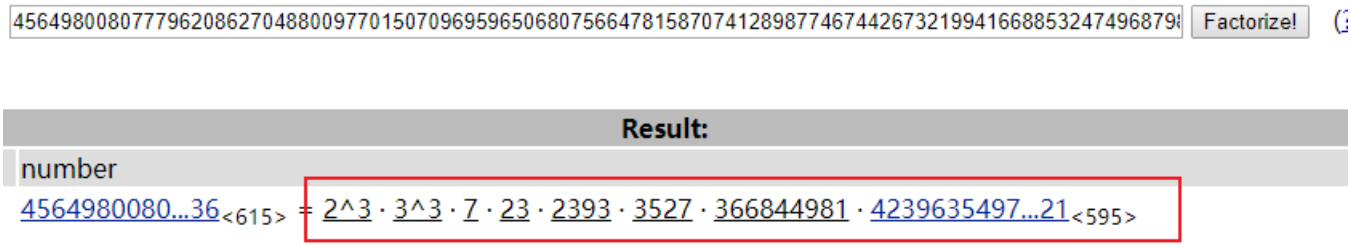
2.分析

（1）关系

$$gift = lcm((p-1),(q-1))$$ gmpy2.lcm求最小公倍数

（2）gift分解

使用factordb分解后



$gift = (2\ ) * (3\ ) * 7 *$

（3）数学原理

$\because$ 最小公倍数(p,q)*最大公因数(p,q)=

（4）最大公因数范围

gift的二进制位数为2042。

```
print(len(bin(gift)[2:]))
```

n的二进制位数为2047，因此gcd(p−1,q−1)占5bits，因此最大公因数的范围（十进制）为[4,32]。
在此范围内遍历最大公因数的值，然后与最小公倍数相乘得到ϕ(n)的值，再有e, ϕ(n)求得d，然后就可求得明文。

（5）e不是素数

e 值不是素数，分解可以得到

$e = 2*27361$

所以，在计算时，需要将原先的e值除以2才可以进行常规的解密操作。
8. 值的变化可通过以下表达式体现

$= (m\ ) \quad m \bmod n$

3.完整脚本

```python
#!python3
# -*- coding: utf-8 -*-
# @Time : 2020/12/11 0:39
# @Author : A.James
# @FileName: exp1.py
import gmpy2
from Crypto.Util.number import *
e = 62674
# e = 2*31337
n = 109559521938671090070491712234483617032703161633815954758089779095705921862415727860005247793992511756396325062146597396541678916138770099097334654458503423264116056335778868191195919886661074942515251195266492540440835702995410595290647522552099482080822186521043032475825399927471963124660883198804613013891391176062694077038708350199911547586991183764087300388245611667931738381841744705553717137645158506878154484105331123373095983503919513047864807006783374206336442970598826232080075308261266777861316005803634103191938033070639740468344582304467416029056329621630267602698934415259509721999095833574689828740 81
gift = 456498008077796208627048800977015070969596506807566478158707412898774674426732199416688532474968798984984687758944155818923662150578208746238894393577097596933816901399078617463316332861087812260480213313610385585170148762480877480377698010633747842003425777171012635315939166364466513019420346661685887557872065839736629132505802075822875396741377694500918089173843789526174839060321832022100268187243257213917173221983445662947146747809251663111881830886870180454979426716332773356700423545040000189379843309371468459260828296151157054634095231514373653361915789381498348538500889098973984825991010648504425961736 
c = 239028744015185907497743122493422887190865858911421943705577833007801725608040729495085403176941504484953050010610797306444222477441677661337227202852089788771485343841197174135212020428092621557562769619846778747677648804630485514464847761158618105576037074344716700443763714901826102307710339473852645569938927340015539322484904376510530895880103985036969736904152021271385383809656571714429599844842703204720418647454216996934227195023472168304089615094827736108547722389920595345321889908810804579094914929760431468622186030462158492820207844856615479267999739548998939564881663449866169651403298987670586488132
#gift = (2 ** 3) * (3 ** 3) * 7 * 23 * 2393 * 3527 * 366844981 * 42396354973817132953898924002069700889405268629062211422899893951610038624456575326817672024336177382141929128956836535099663182296922055948247307822400845352313347567348949900724592131372637189904620852356075082581394553478631930002731327151902305451460365609691254497336781676615444669148945402402512651127032445490279395516132463346676886510011656018080260135750238266827676095190390743128790932035837875881239680741153619505918001001814956746953237727606604319303534909991667418277374243509663297584995981889656170338004867955228062090672080211060167493747610868278937298353851301951919685 21
print(len(bin(gift)[2:]))
print(len(bin(n)[2:]))

# gift * gcd = (p-1) * (q-1)
# gift % gcd = 0
for gcd_val in range(4, 32):
    phi = gift * gcd_val
    try:
        d = gmpy2.invert(e // 2, phi)
        m_2 = pow(c, int(d), n)
        flag = long_to_bytes(gmpy2.isqrt(m_2))
        print(flag)
    except ZeroDivisionError:
        continue
```

4.get flag

```
flag{supplement_of_rabin_algorithm}
```

结语

据说是小学数学，$q)*$最大公因数$(p,q)=_{p*q}$