CTF-RSA-WP-2017第二届广东省强网杯线上赛

原创

网安小小白 于 2022-03-25 17:32:38 发布

分类专栏： CTF 文章标签： 蓝桥杯 算法 leetcode

本文链接：https://blog.csdn.net/u013671216/article/details/123741356

2017第二届广东省强网杯线上赛-RSA

难度：简单

题目下载地址

下载后是文件，打开有如下内容

```
n is 96680893262749719063585923605496034909946397522735056426538437328033669985338725407066288126593756516300075
86061543087579440305718371750485145744730614015663308363346471766552826192685925601727265266430744995341298782174
09046045533656897050117438496357231575999185527675071002803951800635220029015932007465117818739948903750200830 8
56115668691007706836952244842719419452946259275251773298338162389930518838272704908887016474007051397194588396039
91112167088662146147796275669593351706760550258509326310536415765661656941214205460810432858067832392967997956551
91121966377590175780618944910532816988143056757054052679968538901460893571204904394975714081055455240523895653 3
05315517745729334114549756695334171142876080477105070409544777981602152762154610738540163796164295222810243309051
50309086667463444035922619253072463547705157651517986446117491197566716259728676907938066078264795294480859631 0
47697393915618747207695293572824906113748188758910397359108287298864195827028516965080379239555636330405629007781
01453980822097583574309682935697260204862756923865556397686696854239564541407185709940107806536773160263764483443
85942572695314296414821620996843758704461761351805877928716785334936453371645867606673421687756618151460769388 2
375533
e is 65537
c is 16850291008885829563431507024437740955656763713973630808218636900322777193640732178355779562427916216230520
04364469039763859486778976654662908527698775621674871423853080273416398164010550818204970020189088962028603423910
29082581621987305533097386652183849657065952062433988387640990383623264405525144003500286531262674315900537001 8
45043225363148359766771033899680111076181672797077410584747509581932045540801777738548872747597899965366950827 0
55294324837798211581529288999478371963915556661654864418781832880087535611089957159619204729278448775698559405 5
14884353099887811372283042780792667932424114118223890356768204241014534555188944215889515787579899090371510578 6
82083886461661307063583447696168828687126956147955886493383805513557604179029050981678755054945607866353195793 5
41084039392427238616519191523699239040029668739948118263910803181462604169784993771825406844097903572574908162 3
13849936963449089755322776356355398124689167761344639013447783214317524899216164169801119596879210520184797608 3
22786623390242470226740685822218140263182024226228692159380557661591633072091945077334191987860262448385123599 5
96472285621373691780690728044980494631362338563378173859779901455710422317953329955239881748954328198728321700 9
690848
```

很明显，是一道分解n的题。两种方式分解，一种直接上网页分解，另一种用代码分解只适用于p,q比较接近的情况。

直接上代码

```
import binascii

import gmpy2


def fermat(n):
    a = gmpy2.isqrt(n)
    b2 = a * a - n
    b = gmpy2.isqrt(n)
    count = 0
    while b * b != b2:
        a = a + 1
        b2 = a * a - n
        b = gmpy2.isqrt(b2)
        count += 1
    p = a + b
    q = a - b
    assert n == p * q
    return p, q


n = 96680893262749719063585923605496034909946397522735056426538437328033669985338725407066288126593756516300075860615430875794403057183717504851457447306140156633083633464717665528261926859256017272652664307449953412987821749046045533656897050117438496357231575999185527675071002803951800635220029015932007465117818739948903750200830856115668691007706836952244842719419452946259275251773298338162389930518838272704908887016474007051397194588396039111216708866214614779627566959335170676055025850932631053641576566165694121420546081043285806783239296799795655191121966377590175780618944910532816988143056757054052679968538901460893571204904394975714081055455240523895653305315517745729334114549756695334171142876080477105070409544777981602152762154610738540163796164295222810243309051503090866674634440359226192530724635477051576515179864461174911975667162597286769079380660782647952944808596310476973939156187472076952935728249061137481887589103973591082872988641958270285169650803792395556363304056290077801453980822097583574309682935697260204862756923865556397686696854239564541407185709940107806536773160263764483443859425726953142964148216209968437587044617613518058779287167853349364533716458676066734216877566181514607693882375533p, q = fermat(n)
e = 0x10001
phi_n = (p - 1) * (q - 1)
d = gmpy2.invert(e, phi_n)
c = 16850291008885829563431507024437740955656763713973630808218636900322777193640732178355779562427916216230520043644690397638594867789766546629085276987756216748714238530802734163981640105508182049700201890889620286034239102908258162198730553309738665218384965706595206243398838764099038362326440552514400350028653126267431590053700184504322536314835976677103389968011107618167279707741058474750958193204554080177773854887274759789996536695082750552943248377982115815292889994783719639155566616548644187818328800875356110899571596192047292784487756985594050514884353099887811372283042780792667932424114118223890356768204241014534555188944215889515787579899090371510578268208388646166130706358344769616882868712695614795588649338380551355760417902905098167875505494560786635319579365410840393924272386165191915236992390400296687399481182639108031814626041697849937718254068440979035725749081620313849936963449089755322776356355398124689167761344639013447783214317524899216164169801119596879210520184797608232278662339024247022674068582221814026318202422622869215938055766159163307209194507733419198786026244838512359945964722856213736917806907280449804946313623385633781738597799014557104223179533299552398817489543281987283217002969084853099887811372283042780792667932424114118223890356768204241014534555188944215889515787579899090371510578268208388646166130706358344769616882868712695614795588649338380551355760417902905098167875505494560786635319579365410840393924272386165191915236992390400296687399481182639108031814626041697849937718254068440979035725749081620313849936963449089755322776356355398124689167761344639013447783214317524899216164169801119596879210520184797608232278662339024247022674068582221814026318202422622869215938055766159163307209194507733419198786026244838512359945964722856213736917806907280449804946313623385633781738597799014557104223179533299552398817489543281987283217002969084853
m = gmpy2.powmod(c, d, n)
m = binascii.unhexlify(hex(m)[2:])
print(m)
```