Crypto—ExRSA
扩展维纳
Exp：

```
from Crypto.Util.number import *
from gmpy2 import invert
e1=5077048237811969427473111225370876122528967447056551899123613461792688002896788394304192917610564149766252232281576990293485239684145310876930997918960070816968829150376875953405420809586267153171717496198336861089523701832098322284501931142889817575816761705044951705530849327928849848158643030693363143757063220584714925893965587967042137557807261154117916358519477964645293471975063362050690306353627492980861008439765365837622657977958069853288056307253167509883258122949882277021665317807253308906355670472172346171177267688064959397186926103987259551586627965406979118193485527520976748490728460167949055289539
e2=1252684829834900539052027692392913246345915257499862575720825929789111513365411764821578294533252908136527386031620113079330657077773507653477216899970589564120753530383945507400305768781038111097832098897601132610691994079916097422831182476004637027350551106561926855769718258625923437923941048278444981573233529439567630222641686370934003298761271515191608429182109546262582102313356041532582488534722139149693721324636173636127084674112855759560305271361252845370994840310071127767964121852042987889756565548208641057637997140478921229769755374829243818306550099337504003173382549669279769936242101027159951026940 1
e3=1298594075757853081051937033206365834404668885660596747494101443687272036044404046464479098097699139397094702339835742220387328429484340114406501391146367050155988860114510865196109834825082416669766552841766837440881457295972278902011039624507627555350587856560350946622071021926003778384927647539728342106871608863818699477815354281768196305958165110356357880414515615758433671267888299568563261568685398017604768332697428389634332298152115021131759757155454248892129015812263414057114803673289380806411904832885513405470912087789594167016642166480618671034682449405478302573347589808124782488796755041850903827627 9
c=1414176060152301842110497098024597189246259172019335414900127452098233943041825926028517437075316294943355323947458928010556912909139739282924255506647305696872907898950473108556417350199783145349691087255926287362869220118411433395308633001982392314907073933830761747918189941588158573919308029362804475888084406074153773913366045334400997938492378572475575823073913293205159960218200003555605142175056435870269949185883111271435668580366533159851775519638364297285157456468071236371932598598566304521551389866102720674802573305921461351081900835788730941331144400508608441922594410932367870027157379323428471473999 
N=1785330373383806617311041789059370446414682488631645678087335255996974261575529446666443952935271843439955281863535276803353194800973717069756628684871083280042631132856092413369848165359400772787703150626
```

```
570634156081058806420968180914659757212617330346312566818383784042766
710182723475282374748379294453689307018801035764447851214333201478653
969853522013978444031448137146405395476982273840780816194694321671472
968582089697246702089349334905124398339001876207681286867809817241646
569155028537284640299199579434901583886822168621639659732727311016592
278981431585846204970625525406672401292581510043495382185685452975 3
a=2./5
D=diagonal_matrix(ZZ,[N**1.5,N,N**(1.5+a),N**0.5,N**(1.5+a),N**(1+a),
N**(1+a),1])
M = matrix(ZZ, [[  1, -N,  0,N ** 2,   0,   0, 0, -N ** 3],
             [  0, e1, -e1,-e1 * N, -e1, 0,e1*N,e1*N**2],
             [  0,  0,     e2, -e2 * N,0,e2*N,0,e2*N**2],
             [  0,  0,      0, e1 * e2,0,-e1*e2,-e1*e2,-e1*e2*N],
             [  0,  0,      0, 0,e3,-e3*N,-e3*N,e3*N**2],
             [  0,  0,      0, 0, 0,e1*e3,0,-e1*e3*N],
             [  0,  0,      0, 0, 0, 0,e2*e3,-e2*e3*N],
             [  0,  0,      0, 0, 0, 0, 0,e1*e2*e3]])*D
t=M.LLL()[0]
x=t*M^(-1)
phi = int(x[1]/x[0]*e1)
d = invert(0x10001,phi)
m=pow(c,d,N)
print (long_to_bytes(m))
#b"hgame{Ext3ndin9_W1en3r's_att@ck_1s_so0o0o_ea3y}"
```