```
from sage.all import *
from Crypto.Util.number import *
from os import urandom
from secret import flag
n = 16
bound = 2^15
A = [ZZ.random_element(-bound, bound) for _ in range(n*n)]
A = Matrix(ZZ, n, n, A)
B = [ZZ.random_element(-bound, bound) for _ in range(n*n)]
B = Matrix(ZZ, n, n, B)
res = []
for i in range(5):
    bound = 2^15
    S = [ZZ.random_element(-bound, bound) for _ in range(n*n)]
    S = Matrix(ZZ, n, n, S)

    tmp = []
    for i in range(0, 60):
        S = S*A+B
        bound = 2^(int(S[0, 0]).bit_length())
        if i % 3 == 2:
            tmp.append(Matrix(ZZ,n,n,[ZZ.random_element(-bound, bound) for _ in range(n*n)]))
            continue
        tmp.append(S)
    res.append(tmp)
e = A.LLL().determinant()
p = getPrime(512)
q = getPrime(512)
n = p * q
m = bytes_to_long(urandom(int(n).bit_length() // 8 - len(flag) - 1) + flag)
c = pow(m, e, n)
h1 = pow(p+q, e, n)
h2 = pow(p-q, e, n)
f = open('双人成行.txt', 'w')
f.writelines(str(res)+'\n')
f.writelines(str(n)+'\n')
f.writelines(str(c)+'\n')
f.writelines(str(h1)+'\n')
f.writelines(str(h2)+'\n')
f.close()
```

首先，根据题目代码，发现这题考察的是 RSA 加密和矩阵变化两种题型。对于 RSA 加密的部分，题目告诉了我们$(p+q)^e mod n$和$(p-q)^e mod n$的值，那么根据泰勒展开可以知道$(p+q)^e mod n = ((p)^e + (q)^e + f(p,q) \times pq) mod n$由于$n = pq$，再结合余数公式，可以知道$(p+q)^e mod n = ((p)^e + (q)^e) mod n$，同理$(p-q)^e mod n = ((p)^e - (q)^e) mod n$，由于我们直到两个式子的值 h1 和 h2，那么根据同余的加法性质，可以求得$2p^e mod n = (h1+h2)$，所以$p^e \equiv \frac{h1+h2}{2} (mod n)$，同理$q^e \equiv \frac{h1-h2}{2} (mod n)$，所以$\frac{h1+h2}{2}$一定是 p 的倍数，$\frac{h1-h2}{2}$一定是 q 的倍数，而$n = pq$，所以只需要将$\frac{h1+h2}{2}$和$\frac{h1-h2}{2}$分别和 n 取最大公因数，就可以求出 p 和 q 的值了。

代码如下：

```
import gmpy2
```

```
h1 = 870216076700806567507281892028116473216648253220859674321468859955381400049015
748306253479547243443315147318528737211001752996566181611738748187734156847397730555
620673258848991693719847569489515642296650035465632567910004553054397894647697286044
4465567405142149926303968235362573821060105908856127568162452912
h2 = 705288010000556186596383154631335041982385077227225701272150980170822059342908
678166957376827388317172284707998269574907829487607968448815086320603120803312644744
968266753069687287034453036854258618280625776346633340081217397502423530180647548747
7144401922660710323623212890923488339464759360304751017490144695
n = 126930298936285661712486297662920895162569606037310367763354747221281175771655642
4240713632662169591062303880877977853011240635531407120937068815787292801063318135139
0907245450136775930625563231193084579188055553120690556042372111176502201784162981650
2160321136684364033461621769541885803662658748378245210512265 3
c1 = (h1+h2)*gmpy2.invert(2,n)
c2 = (h1-h2)*gmpy2.invert(2,n)
print(gmpy2.gcd(c1,n))#p
print(gmpy2.gcd(c2,n))#q
```

然后就是求 e 的值，要知道 e 的值就必须先求 A 矩阵的值。由于题目不断地对矩阵 A 和 B 进行$S_{n+1} = S_n \times A + B$的操作，所以我们假设：$S_2 = S_1 \times A + B$，$S_4 = S_3 \times A + B$，将两式相减可得到$(S_4 - S_2) = (S_3 - S_1) \times A$，由矩阵的性质可以求得$A = (S_3 - S_1)^{-1} \times (S_4 - S_2)$，而题目中的 S 的值是告诉我们的，所以可以直接把 A 求出来，相应的，e 也就求出来了，sage 代码如下：

```
S1 = [[1032613861, 106816006, -579642058, -114961986, -1407150191, 2246208215, -
731032284, 1322758335, -530199387, 1086793794, 413715111, 2813583, -
10408686, 2540826776, 533417175, -28576837], [1315196062, -
2147222506, 1457422790, 725951720, 1932327742, 1405174748, 114563095, 49396155, -
298632492, -337759408, -190063519, -347862873, 1899867670, 174485325, -
738039578, 288495711], [-989605621, 3001040768, -1366155232, -2639014763, -
798679913, -1505776743, -1293775967, -2083309851, 695099207, -
556699855, 56109281, -262848585, -178337656, -661146821, -235304156, -
156969885], [1227418579, -1425755521, 714563908, 730564391, -
371777127, 1819865373, 1028304742, -961308399, 958251347, -
2399967719, 2145196053, -1033384088, -133287265, 3403594236, -735798137, -
1930708241], [-992200349, 273397344, 457772734, 1219170548, -
2916734480, 388270161, -344453199, -80649160, -823396397, 104711252, 1397090628, -
2304473497, -524670723, 2254223073, 491007648, -323393514], [169637022, 68351076, -
2258520458, 2031873445, -2205681986, -746794507, -
245934218, 756721845, 2952961836, 1116738808, 350540191, 653527279, -
1459512536, 760827762, 851822809, -702747039], [1653656177, -1060676663, -
41376980, -183951048, 1433473570, 437806435, -2719144899, -
334337596, 530920363, 909476128, -2891238205, 2530738181, 2311068521, -
397425506, 996330261, -210700939], [-619102845, 1213872831, 1567726850, -
1217388992, -971827845, -2440116285, 286118880, 1244695933, -238692553, -
```

```
876125692, -2363713770, 1734545363, 563182894, 1081453861, 321618106, -
2387800976], [-898283246, 236452115, -1491597556, 2189364067, -
490514498, 145128377, 621398295, -127981220, 390050013, 110820293, 199393396, -
2360152115, -1891225877, 3446162277, 1106399678, -
439552350], [97533185, 774478626, 3077940446, -1070775758, -30111913, -
2127497063, 1327679909, 1382311938, 575995582, -1119210977, -504610272, -
714458008, 1600329869, 1505305639, -2920083778, -
3136072034], [684846755, 2162931633, 4404936, -
3191953649, 1207044874, 2959383450, -431919033, -509260894, -
2840077610, 1114589069, 1525800685, 118969700, 1395083527, -
3667188934, 1229096356, 3174922403], [-283119890, -1354873881, -
538463855, 1237730916, -2640119665, -2935497918, 443809548, -330638492, -
16759938, -363349190, -3342717126, 2044675208, -
2068023044, 1247123636, 1526993674, 343740477], [2135824102, -
1465525238, 820086823, -1447137787, 3038780754, -120904544, -98058739, 446586489, -
31227506, 935079622, -1902274205, 2399987653, 578058470, -2262418213, -
1149997985, 926662344], [-4401261, -2805791783, -40382659, 1392106149, 214813732, -
223484613, -92163972, -849389921, 311804391, -1437090329, 155084981, 2110468048, -
1250841213, -2497005129, 2440158003, 404541707], [-330139748, 1541875159, -
905519693, 97666158, -1423714932, -767140640, -
1154873739, 140173456, 1474766572, 942065411, 163134665, 1334634385, -104414351, -
44143140, 506512633, -2033363424], [-936526289, -
1288157356, 63042838, 573357950, 287573906, 2396577024, -746033441, -1401408701, -
1863620994, -1143137451, 1600168035, -626033143, 969189909, -
204645083, 1692832029, 718951788]]
S2 = [[-133595935540106, -3024619048481, -30568590003134, -21170394809528, -
74284029024818, -179839781537115, -13622548754258, 4058932744998, -
61310275910819, 49511521811952, -88415585834451, 133538390054171, -
215532221977046, -12998081782565, -74267490172232, 72278103716321], [-
29560723404421, -87183875570882, 131865915675338, -12978527501115, 8617441530848, -
94884742451186, -151939864945579, 102821342306878, 34998051344836, -
84228129643954, -67030067113711, 16396905899250, -35803291504199, 81299567319797, -
14641155523649, -83365285747722], [28224549044370, 129129551544063, -
122154097479633, 27085908628192, -
46173208474388, 184805637399716, 60747207256744, -118328426287365, -
3550931652917, 92711215737880, 214246463543182, -
218231675924878, 108908281038108, -
70824356151442, 30295102953783, 131515698012176], [41833532188499, -
21720258953084, 81301647785747, -183792415267851, -48559159873408, -
137844781642803, -37761157988470, -60099634163868, -
99152256442598, 30377902072876, -116092040662200, 41691202572415, -
193783422944475, 122923346460554, -81210479732294, -33538625901686], [-
43072811522781, 125068467565293, -64267398704458, -82247872291985, -
140707566063773, -54518733841603, 156727111606449, -30683545401451, -
```

```
77735953198555, 49774143998011, 48325011719767, -4187414872949, -
182048471531044, 101402050022510, -39920693938820, -
106976031245296], [63435575231517, 65774742736715, -76975346982488, -
83146988338091, -9736579521760, 1105630903474, 146578871706036, -45066073003880, -
73617579860876, 43499961019342, -88615959501607, 80855419668279, 6934746903590, -
88742702929629, -18615620714421, 131974880283353], [-37772148437978, -
32345506373559, 134226947249194, 24715523324572, 54026981661058, -36119041641669, -
105255555540184, 113110815303383, -23235465589885, -37156318174418, -
40201578073249, -27886997889805, 77084208410166, -
92845264661444, 38124538631710, 116007864084969], [-43790677726984, -
55437348705008, 91250972359090, -38633618392576, 87232988462772, -
11400811445983, 37097090765766, -164474126222259, -132593977362832, -
52223190254454, 17500297705311, -35114328755235, 83314241666763, -
109870499637564, -
18896602811694, 27700457837568], [85939589937150, 8959858275549, -62355361281019, -
7133436349692, 6537916880173, 73350700524523, 1641299598745 57, 37537930209275, -
74176351408236, 167141590262154, -7710491210878, 11074524373897, -
103063317797832, 129876145464104, -120139087266052, -9370661513334], [-
111060590185861, -92303930543391, 93864724356276, -
55881653253409, 11996848010549, -134261963871663, -73436570615010, -
223881166995799, -48446831695132, -159859493354827, 1333001799043, -
121564097903124, 33308946134289, 6142994216912, -80889859865149, -
55433910323917], [-146451812016884, 137234123596961, -
73622578935436, 73128718504869, -14862621478765, 19475370121355, -
122749168248385, 92591155663104, 101258962359817, -
18280903221549, 76878388361245, -21074400394864, 29591190638526, -
13295835388300, 39556426870020, -20054425976431], [146461709495047, -
94823048660884, 67350211788350, -
15254639565494, 60841616819100, 142034444011743, 210318400093970, 61201255836254, -
162268949036302, 89372680709339, 29729715281636, 149227714340785, 22888139376357, -
190329576755533, 100969230503436, 104043700475824], [-27385696272222, -
191869084955978, 124786885546385, 143080296032062, 96473630822929, -
63493333443927, -185545466445583, 116395843070803, 104112965439801, -
99104059329874, -92335106239364, 57402199073314, 120080370861244, -
130306649362594, 69723239064693, 99974194134496], [200587262531429, 22167892090608,
 120859452826373, -
81827262019736, 82654944162445, 65140187075960, 52220127190213, 105800050991829, -
6189766265431, 174376866199, -83958956999404, 109076335297993, 96076961817391, -
52875235464354, 122424717301113, -92038728615528], [-
24265856887190, 123992949524203, -61460419935849, -68900465871825, -
8639863521562, -43263596396672, 77973882415822, -124252161863647, -
46323504035226, -9356755444233, -49758689826389, -42584386123607, 57057271159225, -
50951387241857, -
11536062836040, 90440989081251], [41124672662773, 106205702908303, 22479656206929,
```

```
-72964839796386, -62781628131437, 6550032378120, -
45350311859125, 82866923110471, 28124227695699, 48631084669781, 23080171473644, 894
6322523262, -85967668905723, 164043895079665, 19203877248916, -175156176830459]]
S3 = [[651601454138942099329339, 230331647258005002986351, 181886408336966633131294
, -
714028920938168946826229, 279688962710283815249135, 215110323502999152682787, 28990
843699712353931165 3, 676505717011976041924086, -
250312306090954962729659, 24199319864680246387413, -
719831903490575792769202, 106919229167955397113 8157, 202876144946804021063613, -
110728436104999705524906, 214113555516137766356633, -
488522544555111871128 12], [484949953091839183549379, 142282002470881172792323, 4211
642316870697370135 93, -25179452987926539054 2728, -
379714964076393840602 39, 822831296132179023 5557, 525456747416803368073999, 17774183
6736497848333905, -54107291193043997332171, -76665655266934039426420, -
716881139323299221 5565, -
140488518796186085809417, 146867393620031944816136, 146293153866548923176139, 17639
120273735772465414 8, -68353417656342790318 5741], [-
702064122855455862242257, 346203226065030467976938, -
110295097332910447024 9567, 915359997766706914 51588, -25086879121595426187 7248, -
473587938102297464411 05, -10145793030532181655 8948, -87328547939726906026 5575, -
615021457760944702829 19, 433540759182869900571511, 296911306482398038669208, -
197379645238217442296762, -49694395937938312711 1053, -11733875876174453185926, -
561234114445689712583340, 754499205333677474366066], [376695950536230248135103, -
876144987984055490923 6, 198281445750256588311122, -33086140056668262902717, -
943806223918376251692 36, 483467244522096755777 84, 537559144002596774614004, 6654153
58050466345463399, 112815020155798843008678, -33582760884482379858 5743, -
340630393975974449096252, 653985139698574286078187, 251916685953620921212430, -
252970322274794322809 22, 439548434441625843439829, -
484142127324305212481552], [208637615791590452231768, -13728264425589245608 3661, -
366438611650117216732059, 214806974569917504205480, 377184840298029959948 05, 447806
304622082221376285, -
384954758892894974761 62, 328576818051713831858899, 139024060345875762390292, 303929
377271515083227993, -
108480299971946390169686, 467004897975026344078932, 400335803670505616292127, -
174472582604075893118543, 294700769473522447612564, 710289119971113517115842], [-
162184419732471722416338, -13103766632151699152 9725, -
746099577819590145591 83, 222430751295521216990145, 153026879282928241216 65, -
711753189029644850196 62, -
596810269812520418637875, 290456964697075546317341, 384524518777041047188329, -
318546498724878890287067, -
222790960570864825426528, 406474141127768011330000, 609658259436960347348 3, 4561885
7717461451025434, 253826075485853993704638, -
895801315426226409733 5], [210415421066460181193919, 369390817028302085809140, 20790
2767337299309038523, -58097764472097511558 2315, 90530845880555193423422, -
```

232633854428601204059882, 138231357694757524612745, -370139595209929255588070, -962432985784022976320 76, -147418509953031495149107, -142420580762319461511905, -220220885324166314787414, -158559426488258540181363, 463284325188845362741382, -232262475174670986356214, -880635309473865894167559], [-428464900546510137815099, 488939030773129160583526, 322475282817920352111508, -596358860632714501363100, -400949057540391445997 63, -694834929584491010227089, -661215246983458452654 67, -408908826465025991892803, -381119631130559852291927, -132346968917899665024196, -266420324666947744570466, -432213050840729310682285, -191253296687462423534536, 246251105434083425592202, -676731509512094428459416, -274016891593309261757135], [377101903690726336428440, -121348429056019948756348 2, -119944930293834986346245, 993682750846327542155850, -133804394116386764954494, 350429537123313116358509, 2891017233717661907617 1, 30987401304741817593693 1, 309603390905461767438401, -35339866840394371367207, -782827714190406925465 8, 701824039617084839069700, -14943857202888661685509, -467319573429330488029667, 756675089135674827292532, 706329086618886945513777], [-411751102426003290528823, 118796995651614723728772 6, 235475859537686068112339, -108883656940095875023 8025, -335897139136652583526206, -932793706583567411518457, 322523667424362643617154, -162782353341095843772626, -448295308701753292448221, 760832611994927314253 11, -398519110414456088947307, -370974527022594189904817, -277982234288229036175712, 349221501728475467258847, -854671356322097731331054, -503211047890056756573535], [260103389907266010419999, 497482815124712787878785, -603404436457025164761159, -27598135404360340589 0189, -882838653923224322688 62, 563793885355446571903665, 194076686885406001721081, -119204654487124333496344, -819183778400907508672 87, 653217065068751276256615, 354313672101724378178902, -313373661870739312557900, -162365790623300182700178, 384067717888518559152686, -250271654153125485529265, 232872869544776709714256], [-105924021021792473628535, -100993814485279077416225 2, 699826823628869312022483, 546704213803931953657159, 6376887001610022884283 72, -756003374974648539209 87, -530011729285793080342278 0, -380893516802494799966449, -562965962970107808605 68, -658510890440934163516179, -137419759505589368298886, -3782334273407142548871, 492181102869721328564764, -585234162667732419933176, 387759085874407844007347, 194908154608499549504626], [68609176342043534801560, 325340345851827111385855, 816271118401232566998107, -778251962351209168411064, 340752924742993600725179, -506145633632314534111166, 337493299093437494024 23, -225037006081322766113402, -350012868674564395280364, -375093720776455428791822, -227061585718434106353247, -275589279332941918184381, -111730003990264503520486, 135520407342305598429366, -322899982486342867809124, -104725101019551432016 5048], [-145915184368335811921402, -696088642540606737699561, 490298502469692944755190, 869727194211386370086932, 2933436385739664623316 03, 345908180335332537027958, -550525127142679685092262, -529062392995153902294 66, 459916513588589162120878, -617467329992980365402877, 669360469725680555128677, -

```
832990223453050425906910, 565661804653032638500849, 123252277679173172504103, 40431
965095679690601983 3, -552152596574337200750560], [-
459645218170049580115865, 538894876344036905359839, -390300779885788579913007, -
265308257823211345667891, -227803474357837244551963, -311659128031512993594469, -
503201017816806838429903, 59823677463563421788377, 227599726018708673371881, -
288487681643490478 2883, -166627347653713953717374, 66496127776523952916412, -
314844001259578098227253, 501301227173207985011155, -369465618174550855548226, -
150468913674295330891271], [386019097599644261386778, -373695603546365614199766, -
314557657370679744704658, 645338711148100631865316, -
104479437292820314332209, 844350746948471932564321, 373815812953215870254497, 22124
686535445987011 3417, 246604387824137768390322, 210632309073279668260940, 6097423708
10337852963759, -154660881646591902221593, 357434304788917732008388, -
113908374884112943220 45, 501851124722832332948031, 187684269656752517311032]]
S4 = [[-369591703263854994635993815 90, -
464573149777744031482070366 73, 335643835572745621658818870 04, 560491691863195558037
2272213, 544201508130609161518767461 11, -306922878797042686481314699 54, -
416630124144139930599391686 94, -738366615841306237767461825 5, -
255411848826011420223492698 41, -186382159344353685172262930 85, -
393695968334502073493006601 28, 510571497062705464650321267 32, 103881481213671698451
43050263, -659776278155784117940693048 52, -
474229492765714528303042928 1, 469935078737376501171857970 39], [-
131105500129088272278101033 41, 153088191588886283790522807 74, 357853166058410941175
88896731, -441436844995796487320791907 01, 344374136122469178044278654 01, -
310615605497452840283308486 59, -276612911752687028084545000, -
161374621818048588424984319 83, -315408104137699418051843195 60, -
713998052668740087084414232 4, -
304105856304182474440132750 37, 269515705447436658941109379 5, 201636820248514477306 80918957, -147492630272197494673363404 55, -340361767257533346260586157 96, -
135677110432103356444534279 24], [257301072558539510642785726 27, 1042189921804032466
5343243028, -902249484061961527119316973 94, 465488561174213289135335687 77, -
533351256167974537155989581 70, 635111505450429829859137551 80, 157600946698951755737
99646808, 130847838593111494671527310 66, 439035975529763445751214335 41, 48821219382
503255362943307158, 481565549572938623520004629 42, -560892582675039787627783260 7, -
163288663918116606713069193 55, 270890802145228737820854171 77, 336121813739872429090
16042431, 441286678084858010659674948 99], [-780818358491118021914031468 5, -
118801045032027005563476676 17, 397742888223173232761194367 01, -
476112485086083260895081880 94, 568467582043534565798923694 28, -
220280511430551055868592783 67, -150056147274353434319230594 78, -
256539211615752106464415851 38, -422213673303912657122171870 35, -
215179608646599960010336547 84, -
432080526138188644307729844 00, 433883977854304544172666130 31, 196460987276234929069
32863570, -422015835018395584742715614 98, -
180970602962548298991718065 60, 221264940001882690039915300 9], [-
123947147018083355280806506 57, -130673442134268007699052997 27, -
```

```
33281612474658820098865843 72, 31854222835538190794693262 93, 225511988025998874564708306, 32759072768218076134983095 97, -2356305802340032696078741902 9, 24734824118048240449822799278, -13032709200034279280330170 53, -11814695574412724597108364949, -12456541908804237199919473603, 38814977670793151975268406890, -45646759925533952521375961 80, -14833948237553015680104635674, 771804708563195696423236419 1, 27253800102183406404925576303], [77246281962958865450162727 72, -12960978938450744967687361052, 60959173210903179123217354 17, 7359433135010825141264334944, 24013746770225604826149782 69, 5100448594747437337524071280, 315445241846655158067926881 5, -10294752871657525442406843623, -73034712576191184581094661 59, -77845001634065056475850098 18, 38156861207389220896582601 26, -48997230563676770272916596 70, -97635521069921589130892543 85, -10195556689607859813165680335, 11193540511980722548667482561, 815566494740640559755609411], [-25301034992803328656130386 99, 81737205219366097748919786 80, 13311945811259804649785226133, -11935369644927396474940501181, 15424956485588001425605032903, -13113389115765108199083972096, 38902693322871632849211937 16, -25095722386900886572476517250, -16227726046196414833989205276, 21910573828407439668739152953, -24794060391737699011326507 89, -32368504682180791216989396026, 11715822404124252911794735147, -33715678312847968055927383 75, -24796930861479631627875942687, 109717262244937441323031848 58], [-61954791346621085584739738 58, -85306004036763505755675916 36, -17322012970487256079563356582, 35377931512717042989122002078, -18144534444817748296507590484, 21920938105134741557174650494, 1304067576184172782942958 8917, -27193506340353961195591610390, 11090888759736815921362037436, 1201183583083204655137427435 19, 54240814328300125591779355906, -55169739610322443396471781992, 38323951766802116622605811 41, 7991319700346508180816411330, 57251461563134634649546596 59, -83374528395115938292861229 7], [35542167445834613751586422099, -16748283702267240040139775136, 39302339454043554908675878531, -28441099026577132652279810100, 12006988031502540056064358966, -64040498167177917423270233 10, 37124130367779112443067703 30, 57430130488884271740097797842, -11037464063795495534687763927, -21654410201378260800098693716, -48499811381733813231844034077, 80497774917762905275046088276, -63775318725541520638441668 39, -21243078661447680601600956613, 30410931109423736188783387283, -12808331247963413070539818281], [-308043782942620029567643861 53, -59491552415167670642784733 13, -37379270550433819278699862403, 35175887079524106692993498777, -62507311350231807851673989 38, 20586737921630487429501238105, 1836238228437830827042
```

```
3794027, -619207350770186131568956578 73, -
27712059470201878047447625 76, 156292688314102302972340494 82, 576340052389604453561 39221679, -52404289139473617945195774077, 159287514524447132812389809 32, -
20554310241586428582714618612, -
88890851986183477038133675 73, 280375597654210529997073877 10], [-
27576399090200262718156742374, 111808415745093264391535734 55, -
45397277789503783780996803678, 129630554827848631193233264 83, -
20159422891902349182474548226, -14734355821894290539725797798, -
77651412593969079483108470 44, 75830476141434274790972928 70, 963198866009146315846473 7872, 31071650725191658647486536724, -
10467540946103991753495022617, 165309087508530653529119276 50, -
28094314257356870095013551191, 638963385523454531392957533 1, -
22363232601626361114456362348, 444868989683960384922143053 67], [4069096258921797122 0172493143, -159355113328254018535020437 4, 628147695438092160228283739 12, -
76049243323636787077054330 03, 598348381105828083037748751 5, 208199653923535946135 31586314, -
10299347710079344758215585422, 442363320770559193123505894 96, 123404190661814783525 25976636, -30793699902740820451878007078, 152589586922460705675472923 80, -
34813286618846064971705343102, 230893114120427294009986624 06, 346822968244982846638 75602638, 29622277389248317925546932952, -72499320238716967615863537937], [-
88124785726974306874268983 26, 886119359606582134186774944, 335740753701995065900502 07720, 118448667259280107580606312 1, 228051335412945383139730246 61, -
21098518079058123247666422111, -79469578358909945309585194, -
33666550797921755471088406509, -56652938808165207392101930 69, -
15947816653608361766223612 75, 727805283349405481648243183 4, -
56053671752980683035253308839, 243717302912882037884897060 2, 647703555019532115675 046095, -18179236238778704162881285451, -
24845783680512977603510279509], [220164813942223831437950947 32, 4490283543646226728 5824905174, 409158642306342752560754277 53, -52088345395867412112720954129, -
12407536541048234638431784792, -
20940365997458256778948457792, 276957553827778084377008949, 255211860381471231293584 1989, -10179700771408244252599957 8, -20355310127221302146755308911, -
52757013690810924500013118 31, -53733472417389578241469789550, -
74663999429424101612078559 54, 718364204819279817891530984 59, -
25812201089044577460914900777, -91602502952251109448836029084], [-
92644185229477459052268394 16, -13519196789437163098611882188, -
43103758332219131197726325864, 369016750362569377791238041 93, -
24420912512782077597402341993, 119727933605723239531033207 88, 113935998363398053978 98134621, -
38493593004501188817472186738, 496996551497328523666629669 8, 205990189891315215095 14003878, 30717566852618065117706039017, -24495229330712678737721273484, -
23589858091404470680669685834, -
53652982086260788326969477 64, 290642262302738238246329913 1, 419689644588981475622794 90624], [-
```

```
311085719247179888742190130, 30186748668393702163029379040, 655544803944904529758819
90929, -538249931570148866833270642l4, 373369090833574899168064805 9, -
24888324452508818770784583248, -
125151450354524119350535759 79, 237138164242065253436137928 04, -
106875716596232161203859534 60, -45491274199951160570737239 40, -
46926312462960797156845210611, 45170086952750770396864519794, -
11283658829095717492073977940, 18681708462943418302564831958, -
24313596583134659993458057015, -17439658689483794363650458244]]
m = 16
S1 = matrix(ZZ, m, m, S1)
S2 = matrix(ZZ, m, m, S2)
S3 = matrix(ZZ, m, m, S3)
S4 = matrix(ZZ, m, m, S4)
A = (S3 - S1).inverse() * (S4 - S2)
e = int(A.LLL().determinant())
```

接出来发现 e 并不与 p-1 互质，发现它们有公因数 21，所以原来求 RSA 的方法失效，这边需要给它做变形：

我们先假设$\mathbf{gcd}(e,\varphi(n)) = a$，那么就可以将 e 写成$e = E \times a$的形式。再构造 d 使得$dE mod \varphi(n) = 1$。由于 RSA 的加密算法为$m^e mod n = c$，解密算法为$c^d mod n = m$其中$de mod \varphi(n) = 1$。

那么变形之后可得到：

$$c^d mod n = (m^e mod n)^d mod n = m^{ed} mod n = m^{aEd} mod n = m^{Ed^a} mod n = (m^{Ed} mod n)^a mod n = (m^{k\varphi(n)+1} mod n)^a mod n，\ k \in Z = \left((m^{k\varphi(n)} mod n) * (mmod n)\right)^a mod n，\ k \in Z = m^a mod n。$$

带入本题中的 a=21，就得到了一个新的 RSA 算式，$m^a mod n = cn$。

观察题目，发现 m 有嵌套一长串随机字符串，所以 m 是一个非常大的数字，不太能用低指数攻击，因而这边需要转化一下：设$mmodp = x1, mmodq = x2$，那么有$x1^a modp = cnmodp, x2^a modq = cnmodq$，这样做是为了将 x1 和 x2 的取值范围上限限制在 p 和 q。然后把 x1 和 x2 分别求出来，可能有多组解，分别用中国剩余定理爆破 m， sage 代码如下：

```
from Crypto.Util.number import *
n = 126930298936285661712486297662920895162569606037310367763354747221281175771655642407136326621695910623038808779778530112406355314071209370688157872928010633181351390724545013677593062556323119308457918805555312069055604237211117650220178416298165021603211366843640334616217695418858036626587483782452105122653
```

```
c = 113627841667808982839757084973426219545127121566516056267404541633803040730885409234473068650543791446730694746311695177758797711077000091232969424826171863685060090359260225102836081852105845748467870581394884564134418376982186965340367386781824886506478939204791426457255483148486730526127180397268053506840
h1 = 870216076700806567507281892028116473216648253220859674321468859955381400049015748306253479547243443315147318528737211001752996566181611738748187734156847397730556206732588489916937198475694895156422966500354656325679100045530543978946476972860444655674051421499263039682353625738210601059088561275681624529 12
h2 = 705288010000556186596383154631335041982385077227225701272150980170822059342908678166957376827388317172284707998269574907829487607968448815086320603120803312644749682667530696872870344530368542586182806257763466333400812173975024235301806475487471444019226607103236232128909234883394647593603047510174901446 95
m = 16
e = 183183094232895496570030296666322746922054965594187733500344545328263827233
p = gcd(h1+h2 , n)
q = n // p
phi = (p-1)*(q-1)
d = int(inverse(e//21, phi))
c = pow(c, d, n)
P.<x> = Zmod(p)[]
f = x**21 - c
res1 = f.roots()

P.<x> = Zmod(q)[]
f = x**21 - c
res2= f.roots()

for i in res1:
    for j in res2:
        m = crt([int(i[0]), int(j[0])], [int(p), int(q)])
        m = long_to_bytes(int(m))
        if b'flag{' in m:
            print(m)
# b'H\xc2K\x9d \x9fV\xa3i\xe1\xdd\xc6\x85\xf6\xc3\x96\xf0)5\xbbw\xa2*\x08\xe0\x12\t\xa7wWJ+\xfcSz\xc9\xc9\xf2\xf3\xc0\xae\xe8F\xd1xG\xf7:\xdb\xb2#7\xb1\xcb\x86-\x7f\\\xb0K\xc0\x0f\x10>\xcc\xc0b\x8e\xa7\x01\xc1\xf1z\xd1HfW\xaf\x19#@S(\x99\x7ffl ag{5a6814eb-8848-11ed-aee3-d812656dd8d8}'
```