2022 HGAME WEEK2 容世

Crypto

RSA Attack

```
import gmpy2
import libnum
#http://factordb.com/
p = 71580034751331403248303 7
q = 97878202387171695485721 1
e = 65537
n = 700612512827159827368074182577656505408114629807
c = 12262242551087017771517736804904996651956751270 8
d = gmpy2.invert(e, (p-1)*(q-1))
print(libnum.n2s(int(pow(c,d,n))))
```

常规RSA，如上

RSA Attack 2

part1

```
import re
from math import ceil
import libnum
import gmpy2

e = 65537
n1 =
14611545605107950827581005165327694782823188603151768169731431418361306231114985
03777591746143392530805439697080969080407398583537646462986060971029218136860061
86265904984918504045034434142414554873044483448923378774224657157091542386535051
41605904184985311873763495761345722155289457889686019746663293720106874227323699
28827779429220895717244652342059639111489155953781102947315012364162410810367651
67544494928051266425527512783096348467776360421141359905162459075173773201900914
00729277307636724890592155256437996566160995456743018225013851937593886086129131
35158295881100359644580606149295251385193223856362719455 3
```

```
c1 =
96507580355493298866427181643918380232881201369420374132076310537603691258499503
16476723484681113104236808581019906700670653062375961216648843536799876895323054
37801346923070145524106271337770666947677115752724993307387122132705797012726237
07355066941911004630825740848453506351567806677768101721151098142927334692802297
11494110645562250012873991413061360817224710750324230796929083802671602141437205
16748000734987068685104675254411687005690312116824966036851568223828884335112144
63726809039715853293714112265407595273005233157398070113637821200295671929519273
39556733152342740645199576701998951005086235618385104 79
n2 =
20937478725109983803079185450449616567464596961348727453817249035110047585580142
82355128957714595812712158679287850938608517845217111245589042947445779721920282
70308842622730613347524934967979353466315098066855891796183674539927497533182738
34113016237120686880514110415113673431170488958730203963489455418967544128619234
39491582039290842297407593275183801218554296884269182420320651779569389386394510
06619409884556959235117773065664193733940919073494316866464855163255754949026823
37518438042711296437513221448397034813099279203955535025939120139680604495486980
76591089243828494545073337515693386315080836979683089236 3
c2 =
11536506945313747180442473461658912307154460869003392732178457643224057969838224
60105983686088371845998600310697037577844372574860708562093878771408132131581714
44141155899522374924484834389103788653592395751693261166680304632758176098276260
48962304593324479546453471881099976644410889657248346038986836461779780183411686
26075677671172057705331950469137355010752529656093646743528381249339648667817802
02924333658980325970273388760451827434928318141756738341983453375140655963964777
09839868387265840430322983945906464646824470437783271607499089791869398590557314
71309467420826176129989470577251344094813942901142594809 0
q=gmpy2.gcd(n1,n2)
p=n1//q
r=n2//q
d1 = gmpy2.invert(e, (p-1)*(q-1))
d2 = gmpy2.invert(e, (r-1)*(q-1))
print(libnum.n2s(int(pow(c1,d1,n1))))
print(libnum.n2s(int(pow(c2,d2,n2))))

#hgame{RsA@hAS!a&VArIETY?of.
```

part2

```
import gmpy2
import os
from functools import reduce
import libnum
e = 7
n =
14157878492255346300993349653813018105991884577529909522555551468374307942096214
96460417273438191305127374522829393083231448346692252924095899489769747593986702
55613480427259196635469490150246939526419364818415527514846041230971480718004166
08762258562797116583678332832015617217745966495992049762530373531163821979627361
20092154422357817071874134824201216411559377770090395440910311009292157882104893
33468932128050716822355758137241139783415928859577673775874922027401859708286297
67501662195356276862585025913615910839679860669917255271734413865211340126544199
76062844505413166148418487667962694636075300951263434953 7
```

```
c =
10262871020519116406312674685238364023536657841034751572844570983750295909492149
10150086980641860373218135008257644759476658757235024667544550893157767015829555
86412195827293455816974482311163180804561125167007179847316559007263881858669059
89088504004805024490513718243036445638662260558477697146032055765285263446084259
81456019754901804409993515835193188515761652723528322906614539096409492900705694
63320513644745284539709042510506056315148690078906 25

def CRT(items):
    N = reduce(lambda x, y: x * y, (i[1] for i in items))
    result = 0
    for a, n in items:
        m = N // n
        d, r, s = gmpy2.gcdext(n, m)
        if d != 1:
            raise Exception("Input not pairwise co-prime")
        result += a * s * m
    return result % N, N


m = gmpy2.iroot(gmpy2.mpz(c), e)[0].digits()
print(libnum.n2s(int(m)))

#AttacK^mEThodS^whAT:other!A
```

part3

```
from gmpy2 import invert
import libnum
def gongmogongji(n, c1, c2, e1, e2):
    def egcd(a, b):
        if b == 0:
            return a, 0
        else:
            x, y = egcd(b, a % b)
            return y, x - (a // b) * y
    s = egcd(e1, e2)
    s1 = s[0]
    s2 = s[1]

    # 求模反元素
    if s1 < 0:
        s1 = - s1
        c1 = invert(c1, n)
    elif s2 < 0:
        s2 = - s2
        c2 = invert(c2, n)
    m = pow(c1, s1, n) * pow(c2, s2, n) % n
    return m
```

```
n =
188195091881062303634448133504681620561644346427294046329830825182253880695447773745441423176128584483453441373722229880333665280862366352137562278166108650459243572321887689136421584486033463304625356961217396227022005403441054641266954320117391815312175829498049395557207004573505128983223765918131353119219045803383402035695826818892434524953638495589559471249752937365094264004600839810788461387400506349068244386897127483243368787916226769743418146910412622806042773578898922117171243193296660528100291311722299307234779814687613695167717202505717130279720649749998021680179462747363831480018659297192481590757291
e1 = 2519901323
c1 =
323077972622554487253144116900930707207375457876188838798340320636454845149673651390546038190792810731003008634658935110580902859965030353960758140762781979794433739860140051056099246245504845132659399359508980015034299902187473474806669296236265054003600207374876650934764981813930436391408387991892987357770632359962803161864179307401830452124346048755136482329968505251885268570668780020950527742686914005105699624288213261625669518887078263431036297315376669828625894689686639667087245180311428084670957277978055848222339375947599910360770451061833225371050385756102561363259268293155222815017142384620387534487 0
e2 = 3676335737
c2 =
940818595622279161439836719641707846790294650888799822335007385854166736459283129434769062995122371073636785371800857633841379139761091890426137981113087519934854663776695944489430385663011713917022574342380155718317794204988626116362865144125136624722782309455452257758808172415884403909840651554485364309237853885251876941477098008690389600544398998669635962495989736021020715396415375890720335697504837045188626103142204474942751410819466379437091569610294575687793060945525108986660851277475079994466474859114092643797418927645726430175928247476884879817034346652560116597965191204061051401916282814886688467861

print(libnum.n2s(int(gongmogongji(n,c1,c2,e1,e2))))



#ttACK|METHOdS~do@you_KNOW}
```

公因数+低加密指数+共模，如上

`hgame{RsA@hAS!a&VArIETY?of.AttacK^mEThodS^whAT:other!AttACK|METHOdS~do@you_KNOW}`