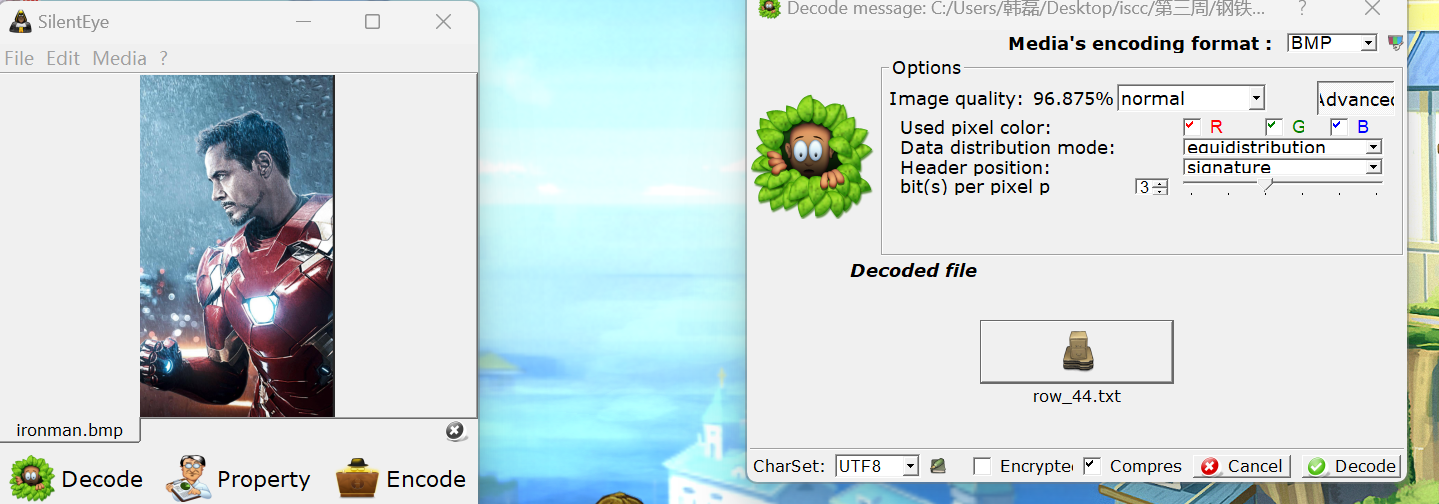
Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

解题思路：

用SilentEye打开编bmp图片，decode导出txt文件，里面就是C1，C2



C1: 1162797362182632315489493439549530976777216093849560582772806719287573117469830157624914515330060819525432527310801624863160104643652764731338368873882358035577052526369249946658924141054408779040649418882864608759191848998798846475105250295276212217100661538083321077886292295982406776886337185220495130052878311569859761370345903727203154897385622251882768913482936840355865390735120866983727655790181591836701128398697666391928396207069002156037576310389446946225071520199214523092989861037572488274140229592283543261828500258528551418215207788809122760664866741354030292230337773808300384176968678738275160380495

C2: 4466686121174334155570089799611784372774397257371734918336364554636262644574583919803122195820670031732645556342545656406559494182025855503979550373128121812161993773292865937270848588725314339313945268501890789135262698413881037808102143530184070176869883076331764741302499796348010791849345625650200157305035283376831490882304097433619169088569451761703571839636830528950801722726518020911873431262901349822311896835013780620481320187198137980995488273661654351834126328333858488378120661518956920727581960037420407773595604189317444161728645428863450152591807025084520229599122231883268428193349434464266426757816

打开一张小纸条.txt，里面是

N = =s14333611673783142269533986072221892120042043537656734360856590164188122242725003914350459078347531255332508629469837960098772139271345723909824739672964835254762978904635416440402619070985645389389404927628520300563003721921925991789638218429597072053352316704656855913499811263742752562137683270151792361591681078161140269916896950693743947015425843446590958629225545563635366985228666863861856912727775048741305004192164068930881720463095045582233773945480224557678337152700769274051268380831948998464841302024749660091030851843867128275500525355379659601067910067304244120384025022313676471378733553918638120029697

e = 52595

a=1

[message]iscc

[message]good

直接写脚本解密就行了，具体在下面

然后sage跑车flag:



Exp：

from sage.all import PolynomialRing, Zmod

def half\_gcd(poly\_a, poly\_b):

    if 2 \* poly\_b.degree() <= poly\_a.degree() or poly\_a.degree() == 1:

        return 1, 0, 0, 1

    m = poly\_a.degree() // 2

    a\_high, a\_low = poly\_a.quo\_rem(x ^ m)

    b\_high, b\_low = poly\_b.quo\_rem(x ^ m)

    R00, R01, R10, R11 = half\_gcd(a\_high, b\_high)

    c = R00 \* poly\_a + R01 \* poly\_b

    d = R10 \* poly\_a + R11 \* poly\_b

    q, e = c.quo\_rem(d)

    d\_high, d\_low = d.quo\_rem(x ^ (m // 2))

    e\_high, e\_low = e.quo\_rem(x ^ (m // 2))

    S00, S01, S10, S11 = half\_gcd(d\_high, e\_high)

    ret00 = S01 \* R00 + (S00 - q \* S01) \* R10

    ret01 = S01 \* R01 + (S00 - q \* S01) \* R11

    ret10 = S11 \* R00 + (S10 - q \* S11) \* R10

    ret11 = S11 \* R01 + (S10 - q \* S11) \* R11

    return ret00, ret01, ret10, ret11

def gcd\_polynomial(poly\_a, poly\_b):

    q, r = poly\_a.quo\_rem(poly\_b)

    if r == 0:

        return poly\_b

    R00, R01, R10, R11 = half\_gcd(poly\_a, poly\_b)

    c = R00 \* poly\_a + R01 \* poly\_b

    d = R10 \* poly\_a + R11 \* poly\_b

    if d == 0:

        return c.monic()

    q, r = c.quo\_rem(d)

    if r == 0:

        return d

    return gcd\_polynomial(d, r)

ciphertext1 = 1162797362182632315489493439549530976777216093849560582772806719287573117469830157624914515330060819525432527310801624863160104643652764731338368873882358035577052526369249946658924141054408779040649418882864608759191848998798846475105250295276212217100661538083321077886292295982406776886337185220495130052878311569859761370345903727203154897385622251882768913482936840355865390735120866983727655790181591836701128398697666391928396207069002156037576310389446946225071520199214523092989861037572488274140229592283543261828500258528551418215207788809122760664866741354030292230337773808300384176968678738275160380495

ciphertext2 = 4466686121174334155570089799611784372774397257371734918336364554636262644574583919803122195820670031732645556342545656406559494182025855503979550373128121812161993773292865937270848588725314339313945268501890789135262698413881037808102143530184070176869883076331764741302499796348010791849345625650200157305035283376831490882304097433619169088569451761703571839636830528950801722726518020911873431262901349822311896835013780620481320187198137980995488273661654351834126328333858488378120661518956920727581960037420407773595604189317444161728645428863450152591807025084520229599122231883268428193349434464266426757816

modulus\_N = 14333611673783142269533986072221892120042043537656734360856590164188122242725003914350459078347531255332508629469837960098772139271345723909824739672964835254762978904635416440402619070985645389389404927628520300563003721921925991789638218429597072053352316704656855913499811263742752562137683270151792361591681078161140269916896950693743947015425843446590958629225545563635366985228666863861856912727775048741305004192164068930881720463095045582233773945480224557678337152700769274051268380831948998464841302024749660091030851843867128275500525355379659601067910067304244120384025022313676471378733553918638120029697

exponent\_e = 52595

padding1 = 1769169763

padding2 = 1735356260

PR.<x> = PolynomialRing(Zmod(modulus\_N))

g1 = (x \* 2^32 + padding1)^exponent\_e - ciphertext1

g2 = (x \* 2^32 + padding2)^exponent\_e - ciphertext2

known\_value\_X = 584734024210292804199275855856518183354184330877

result = gcd\_polynomial(g1, g2)

m = -result.monic().coefficients()[0]

print(bytes.fromhex(hex(m)[2:]).decode())