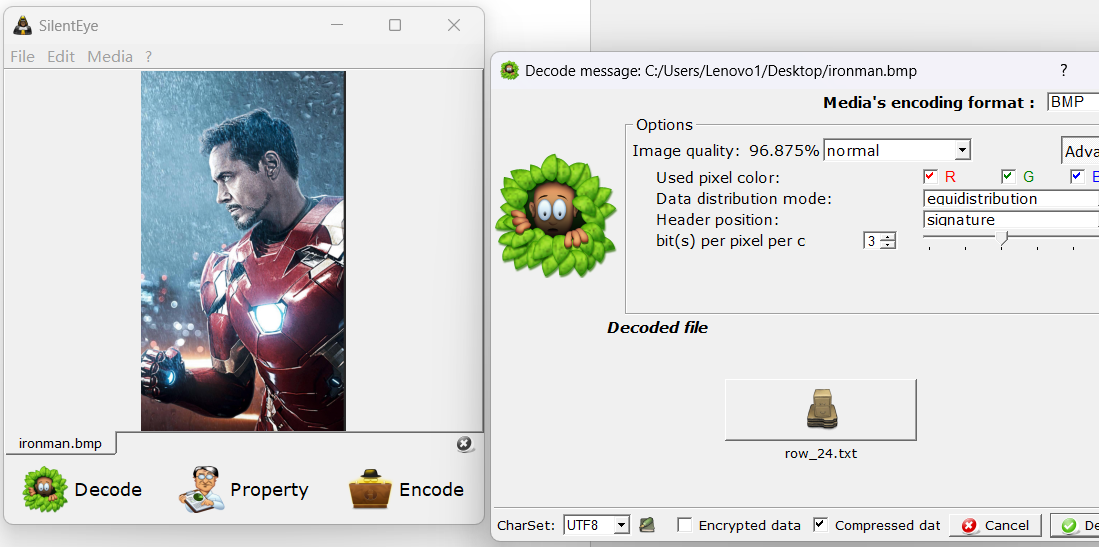
# ISCC2024 WriteUp

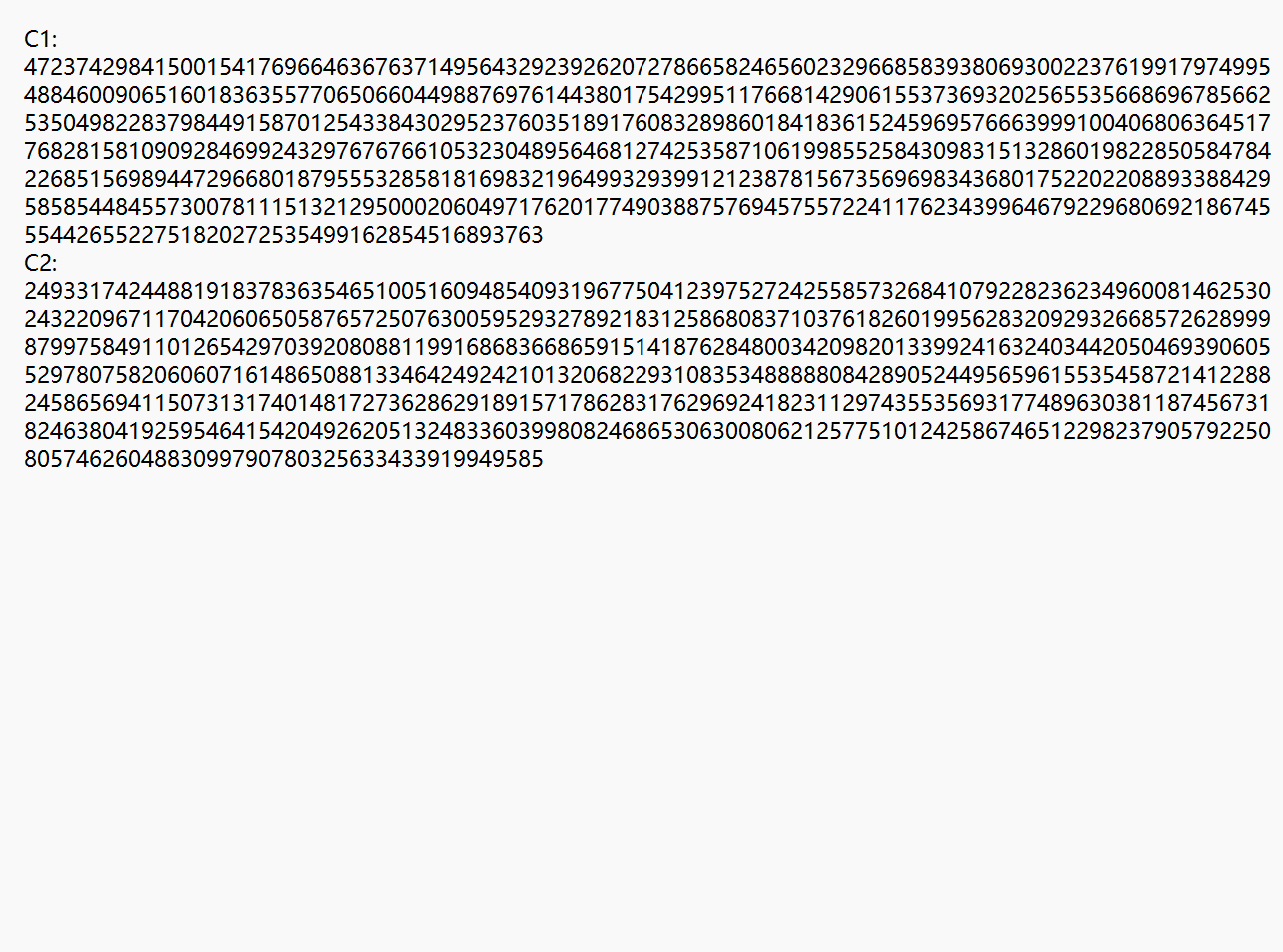
Whooops+李卓航+925798691@qq.com

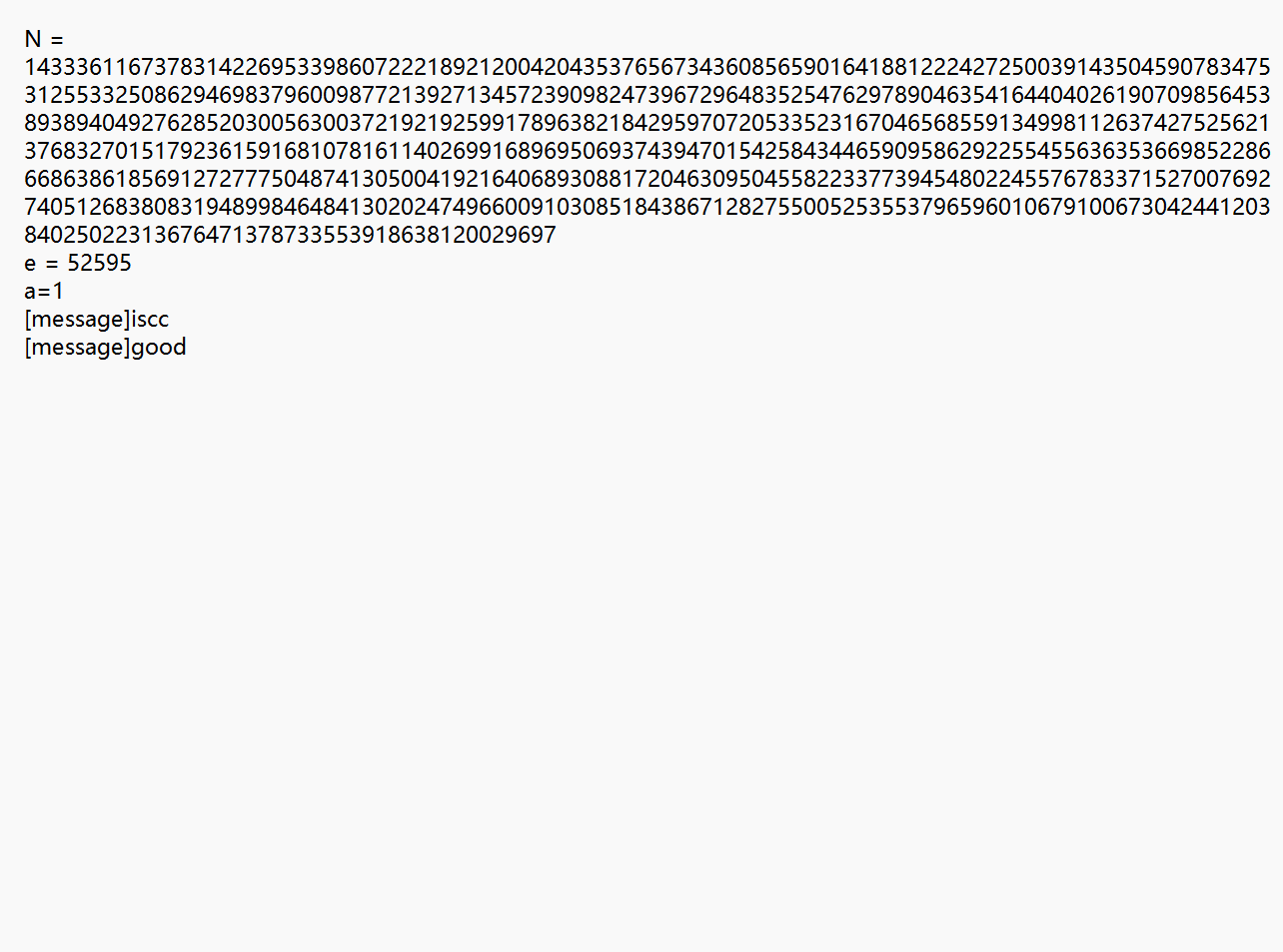
### MISC+钢铁侠在解密

### 解题思路



用工具提取，得到C1，C2





得到flag

### Exp

# 使用 SageMath 的 Python 解释器

from sage.all import \*

# 定义一个多项式计算函数

def calcuate(n1, n2):

# calculate the value

if 2 \* n2.degree() <= n1.degree() or n1.degree() == 1:

return 1, 0, 0, 1

# calculate the value

flag\_resdssss = n1.degree() // 2

# calculate the value

taa, baa = n1.quo\_rem(x ^ flag\_resdssss)

# calculate the value

tbb, bbb = n2.quo\_rem(x ^ flag\_resdssss)

reg0, reg2, reg3, reg4 = calcuate(taa, tbb)

n3 = reg0 \* n1 + reg2 \* n2

n4 = reg3 \* n1 + reg4 \* n2

n5, val222 = n3.quo\_rem(n4)

tdd, bdd = n4.quo\_rem(x ^ (flag\_resdssss // 2))

tee, bee = val222.quo\_rem(x ^ (flag\_resdssss // 2))

S00, S01, S10, S11 = calcuate(tdd, tee)

RET00 = S01 \* reg0 + (S00 - n5 \* S01) \* reg3

RET01 = S01 \* reg2 + (S00 - n5 \* S01) \* reg4

RET10 = S11 \* reg0 + (S10 - n5 \* S11) \* reg3

RET11 = S11 \* reg2 + (S10 - n5 \* S11) \* reg4

return RET00, RET01, RET10, RET11

# 定义一个求 GCD 的函数

def gcd\_function0(n1, n2):

# calculate the gcd

n5, n6 = n1.quo\_rem(n2)

if n6 == 0:

return n2

reg0, reg2, reg3, reg4 = calcuate(n1, n2)

n3 = reg0 \* n1 + reg2 \* n2

n4 = reg3 \* n1 + reg4 \* n2

if n4 == 0:

return n3.monic()

n5, n6 = n3.quo\_rem(n4)

if n6 == 0:

return n4

return gcd\_function0(n4, n6)

# 定义多项式环

NNNNNNNN = 14333611673783142269533986072221892120042043537656734360856590164188122242725003914350459078347531255332508629469837960098772139271345723909824739672964835254762978904635416440402619070985645389389404927628520300563003721921925991789638218429597072053352316704656855913499811263742752562137683270151792361591681078161140269916896950693743947015425843446590958629225545563635366985228666863861856912727775048741305004192164068930881720463095045582233773945480224557678337152700769274051268380831948998464841302024749660091030851843867128275500525355379659601067910067304244120384025022313676471378733553918638120029697

PR = PolynomialRing(Zmod(NNNNNNNN))

x = PR.gen()

# 定义输入值

num1 = 4723742984150015417696646367637149564329239262072786658246560232966858393806930022376199179749954884600906516018363557706506604498876976144380175429951176681429061553736932025655356686967856625350498228379844915870125433843029523760351891760832898601841836152459695766639991004068063645177682815810909284699243297676766105323048956468127425358710619985525843098315132860198228505847842268515698944729668018795553285818169832196499329399121238781567356969834368017522022088933884295858544845573007811151321295000206049717620177490388757694575572241176234399646792296806921867455544265522751820272535499162854516893763

num2 = 2493317424488191837836354651005160948540931967750412397527242558573268410792282362349600814625302432209671170420606505876572507630059529327892183125868083710376182601995628320929326685726289998799758491101265429703920808811991686836686591514187628480034209820133992416324034420504693906055297807582060607161486508813346424924210132068229310835348888808428905244956596155354587214122882458656941150731317401481727362862918915717862831762969241823112974355356931774896303811874567318246380419259546415420492620513248336039980824686530630080621257751012425867465122982379057922508057462604883099790780325633433919949585

val222 = 52595

val1 = 1769169763

val0 = 1735356260

global0 = (x \* 2^32 + val1) ^ val222 - num1

global1 = (x \* 2^32 + val0) ^ val222 - num2

# 计算 GCD

resultttt = gcd\_function0(global0, global1)

# 打印 flag

flag\_resdssss = -resultttt.monic().coefficients()[0]

print(bytes.fromhex(hex(flag\_resdssss)[2:]).decode())

ISCC{xuan\_zhi\_you\_xuan\_250}