# ISCC2024 WriteUp

Whooops+李卓航+925798691@qq.com

### Misc+RSA\_KU

### 解题思路

已知n,(p-1)\*(q-2)和(p-2)\*(q-1)

RSA写脚本

### Exp

# 导入 gmpy2 库，用于高精度整数运算

import gmpy2

# 从 Crypto.Util.number 导入所有函数和类，用于处理数字和字节之间的转换

from Crypto.Util.number import \*

# 给定的 RSA 公钥的模数 (n)

n = 129699330328568350681562198986490514508637584957167129897472522138320202321246467459276731970410463464391857177528123417751603910462751346700627325019668100946205876629688057506460903842119543114630198205843883677412125928979399310306206497958051030594098963939139480261500434508726394139839879752553022623977

# 给定的 RSA 公钥的指数 (e)

e = 65537

# 加密的密文 (c)

c = 31650937211972318813128168239653816179644001565897609233771935181131001436964147248575202308685184523705281445274865352494075014090205778746752006666044591733979809458289439183822907915436022180381434273348701611989338558350485381102736760638968017295766407395945330037876472666238441594774035569377869600421

# 第一个类似模数的值 (n1)

n1 = 129699330328568350681562198986490514508637584957167129897472522138320202321246467459276731970410463464391857177528123417751603910462751346700627325019668067056973833292274532016607871906443481233958300928276492550916101187841666991944275728863657788124666879987399045804435273107746626297122522298113586003834

# 第二个类似模数的值 (n2)

n2 = 129699330328568350681562198986490514508637584957167129897472522138320202321246467459276731970410463464391857177528123417751603910462751346700627325019668066482326285878341068180156082719320570801770055174426452966817548862938770659420487687194933539128855877517847711670959794869291907075654200433400668220458

# 计算 ppq（可能是某种特殊的密钥参数），这里通过 n, n1, n2 的差值计算得出

ppq = (n - n1 + n - n2 + 4) // 3

# 计算 RSA 的 φ(n) 值，φ(n) = n - ppq + 1

phi = n - ppq + 1

# 使用 gmpy2 库计算私钥指数 d，d 是 e 在 φ(n) 模下的乘法逆元

d = gmpy2.invert(e, phi)

# 使用私钥 d 对密文 c 进行解密，得到明文

flag = long\_to\_bytes((pow(c, d, n)))

# 输出解密后的明文

print(flag)