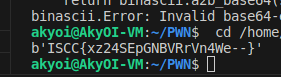
# ISCC2024 WriteUp

AkyOI 李承达 [3433778745@qq.com](mailto:3433778745@qq.com)

## Misc+RSA\_KU

## 解题思路

一道已知是n,(p-1)\*(q-2)和(p-2)\*(q-1)的RSA题目，直接写脚本就行



## Exp

import gmpy2

from Crypto.Util.number import \*

n = 129699330328568350681562198986490514508637584957167129897472522138320202321246467459276731970410463464391857177528123417751603910462751346700627325019668100946205876629688057506460903842119543114630198205843883677412125928979399310306206497958051030594098963939139480261500434508726394139839879752553022623977

e = 65537

c = 31650937211972318813128168239653816179644001565897609233771935181131001436964147248575202308685184523705281445274865352494075014090205778746752006666044591733979809458289439183822907915436022180381434273348701611989338558350485381102736760638968017295766407395945330037876472666238441594774035569377869600421

n1 = 129699330328568350681562198986490514508637584957167129897472522138320202321246467459276731970410463464391857177528123417751603910462751346700627325019668067056973833292274532016607871906443481233958300928276492550916101187841666991944275728863657788124666879987399045804435273107746626297122522298113586003834

n2 = 129699330328568350681562198986490514508637584957167129897472522138320202321246467459276731970410463464391857177528123417751603910462751346700627325019668066482326285878341068180156082719320570801770055174426452966817548862938770659420487687194933539128855877517847711670959794869291907075654200433400668220458

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

phi=n-ppq+1

d=gmpy2.invert(e,phi)

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

print(flag)