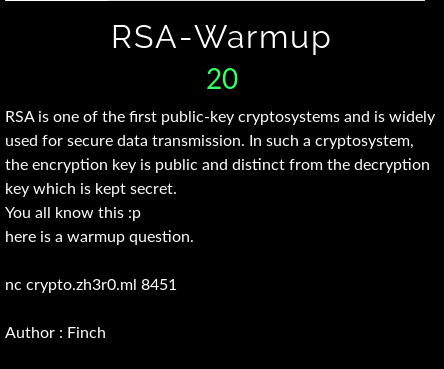
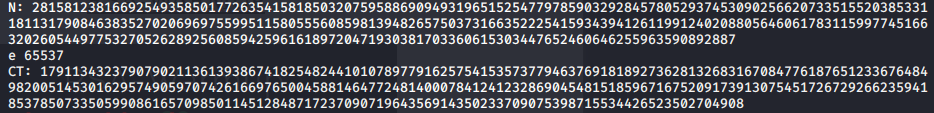
RSA-WARMUP



After connecting to the nc server we were given the following :



It was pretty clear that it was a basic RSA. So I used the below script to get the flag and factordb.com to factorise n.

import codecs

from Crypto.Util.number import inverse

e=65537

n=426170586976418962229011458970708252923025043289071857191581056716215298606831696791077188571747294507762971289979723847918632367644162991922549268089788338736085976580813825171464488038237345545058364522125692631870805592332041490963626738639469777998812448162740321472732632731547539479792931876065971079755195489033

c=41838780661995985319640505676973914831103480445491738783041720786087667747289932836131094568411194373215882728955077556833552062787399225144029055209846214288544951424360098553969789213310092936987038178881136510382270156481106421811732009521507510263268221047387582453730638327668360799064100530144810336295631704611

p=2397346271

q=177767639214943831628489624630745823919829161504167145486001866234456582015736556394642411076104113834026511929773587491866598343249581817262037599110682804960588013687411877919518322281711528999666299988636765703118073088880050858103020670658665052729386228979493267984703504991310260110435640891221913548823

phi=(p-1)\*(q-1)

d=inverse(e, phi)

m=pow(c, d, n)

#print(m)

hex\_ans= hex(m)[2:]

print(codecs.getdecoder("hex\_codec")(hex\_ans)[0])

The flag was : zh3r0{RSA\_1s\_Fun}