i春秋第二届春秋欢乐赛 RSA？ writeup

原创

bingge15 于 2019-10-04 22:07:09 发布 374 收藏

分类专栏： CTF 文章标签： CTF RSA

本文链接：https://blog.csdn.net/hanjinrui15/article/details/102097362

i春秋第二届春秋欢乐赛 RSA？ writeup

第一步：将附件中给出的所有的16进制转换为10进制看看

N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb454a34dab7684589bc32b19eb27cfff8c07179e349ddb62898ae896f8c681796052ae1598bd41f35491175c9b60ae2260d0d4ebac05b4b6f2677a7609c2fe6194fe7b63841cec632e3a2f55d0cb09df08eacea34394ad473577dea5131552b0b30efac31c59087bfe603d2b13bed7d14967bfd489157aa01b14b4e1bd08d9b92ec0c319aeb8fedd535c56770aac95247d116d59cae2f99c3b51f43093fd39c10f93830c1ece75ee37e5fcdc5b174052eccadcadeda2f1b3a4a87184041d5c1a6a0b2eeaa3c3a1227bc27e130e67ac397b375ffe7c873e9b1c649812edcd

e=0x1

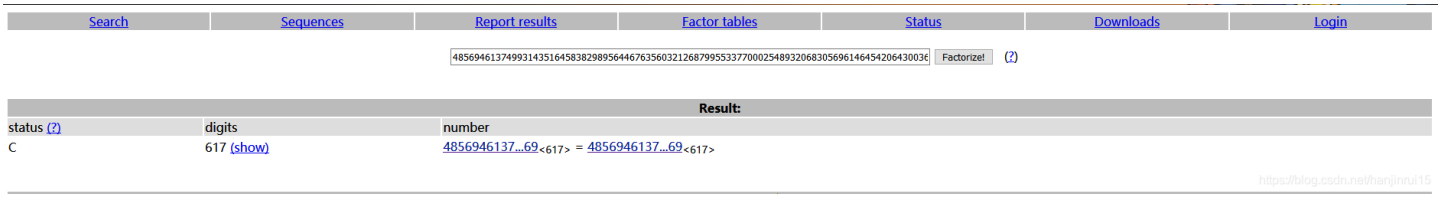
c=0x4963654354467b66616c6c735f61706172745f736f5f656173696c795f616e645f7265617373656d626c65645f736f5f637275646 56c797d

N=485694613749931435164583829895644676356032126879955337700025489320683056961464542064300369119705105010280933969616510401148602559910141372563787280664804020969280512071158330905770216594866346944742238142482480991957461376876971088566405131637916136826005702705815755524127055902306719846247358438871435086324937592950048568740577515404144759739459986931453772920933892683459272006547971748983521218203852501822200648011857893447378441128856653937916713800594000177004487872955499773224066737201036374231180266149992423369026210453796558894794872384502651294550841391647002612690670955948910192080286023855034022578 69

e=1

c=208364969187294709763110474149662765860879002985066102841653682079171655293372490251587249013853834399047472102123087558613560722225533

第二步：分解大整数



发现不太行，那么换种思路看看。

第三步：分析公式

m^e*d%n≡m就是我们需要的一个非对称加密的公式。m为明文，e和d分别对应的是公钥私钥。

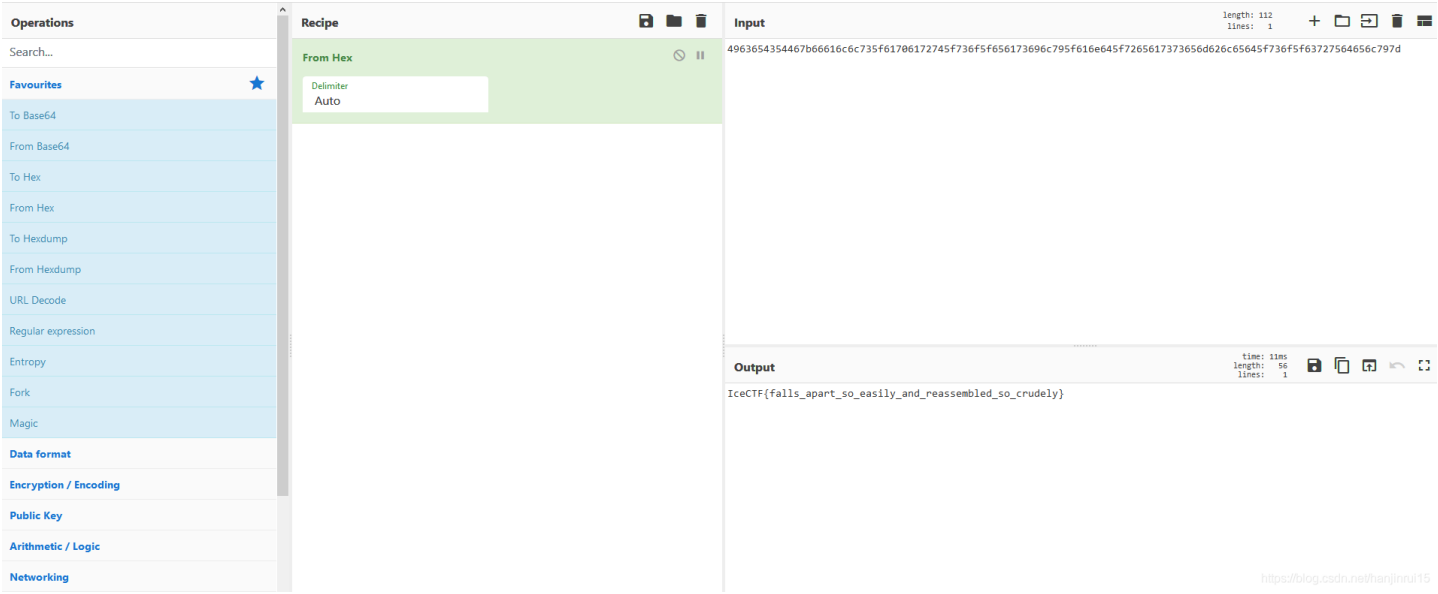
m^e%n=c 加密

c^d%n=m 解密

因此我们这道题目中:

c = m%N

我们试探着将c转换为字符串看看（我的理解没错的话c是密文，然后直接转换试一试）：



flag为：IceCTF{falls_apart_so_easily_and_reassembled_so_crudely}