i春秋第二届春秋欢乐赛 RSA writeup

原创

bingge15 于 2019-10-05 20:35:58 发布 243 收藏

分类专栏： CTF 文章标签： CTF RSA

本文链接：https://blog.csdn.net/hanjinrui15/article/details/102170164

i春秋第二届春秋欢乐赛 RSA writeup

第一步：审题

本题我们发现给出的数据比上一道RSA题目的数据多一些：

N=0x1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a0334d9fe0726f8b057c4412cfbff75967a91a370a1c1bd185212d46b581676cf750c05bbd349d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a4709934289dc0bc5cdc2aa97ce62a6ca6ba25fca6ae38c0b9b55c16be0982b596ef929b7c71da3783c1f20557e4803de7d2a91b5a6e85df64249f48b4cf32aec01c12d3e88e014579982ecd046042af370045f09678c9029f8fc38ebaea564c29115e19c7030f245ebb2130cbf9dc1c340e2cf17a625376ca52ad8163cfb2e33b6ecaf55353bc1ff19f8f4dc7551dc5ba36235af9758b

e=0x10001

phi=0x1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a0334d9fe0726f8b057c4412cfbff75967a91a370a1c1bd185212d46b581676cf750c05bbd349d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a4709934289dc0bc5cdc2aa97ce62a6ca6ba25fca6ae366e86eed95d330ffad22705d24e20f9806ce501dda9768d860c8da465370fc70757227e729b9171b9402ead8275bf55d42000d51e16133fec3ba7393b1ced5024ab3e86b79b95ad061828861ebb71d35309559a179c6be8697f8a4f314c9e94c37cbbb46cef5879131958333897532fea4c4ecd24234d4260f54c4e37cb2db1a0

d=0x12314d6d6327261ee18a7c6ce8562c304c05069bc8c8e0b34e0023a3b48cf5849278d3493aa86004b02fa6336b098a3330180b9b9655cdf927896b22402a18fae186828efac14368e0a5af2c4d992cb956d52e7c9899d9b16a0a07318aa28c8202ebf74c50ccf49a6733327dde111393611f915f1e1b82933a2ba164aff93ef4ab2ab64aacc2b0447d437032858f089bcc0ddeebc45c45f8dc357209a423cd49055752bfae278c93134777d6e181be22d4619ef226abb6bfcc4adec696cac131f5bd10c574fa3f543dd7f78aee1d0665992f28cdbcf55a48b32beb7a1c0fa8a9fc38f0c5c271e21b83031653d96d25348f8237b28642ceb69f0b0374413308481

c=0x126c24e146ae36d203bef21fcd88fdeefff50375434f64052c5473ed2d5d2e7ac376707d76601840c6aa9af27df6845733b9e53982a8f8119c455c9c3d5df1488721194a8392b8a97ce6e783e4ca3b715918041465bb2132a1d22f5ae29dd2526093aa505fcb689d8df5780fa1748ea4d632caed82ca923758eb60c3947d2261c17f3a19d276c2054b6bf87dcd0c46acf79bff2947e1294a6131a7d8c786bed4a1c0b92a4dd457e54df577fb625ee394ea92b992a2c22e3603bf4568b53cceb451e5daca52c4e7bea7f20dd9075ccfd0af97f931c0703ba8d1a7e00bb010437bb4397ae802750875ae19297a7d8e1a0a367a2d6d9dd03a47d404b36d7defe8469

第二步：将这些数据先转换为10进制

N=432103260362901062510888102986679157020077445674678549881079372336228216717529305833785588083811970365429033965343373057234961071540503249535365309937442673860081206589102421439926567733607921826981422737611820470111192617799883774082088581095031774131945415245434478277778314099036647495205273755147486784621012614450399004089994299695107869604718871589576793371900915279133403833102258133221776576952569943150482709523150011005489495543239654046430052067327773613866235915444615337972636527805956392881588921222196267204814726164201180394366806472987147680717979412903070810100867296675525698283233540084413356742 51

e=65537

phi=432103260362901062510888102986679157020077445674678549881079372336228216717529305833785588083811970365429033965343373057234961071540503249535365309937442673860081206589102421439926567733607921826981422737611820470111192617799883774082088581095031774131945415245434478277778314099036647495205273755147486784616840011796810258362432726415200460011083944116083154239671701237095697019519175138479519249363475746712127896942227280870285190901941312509935851815969186416918772381571965768850857682010412345654770699579400102083775669592347658222662267708772769944632345948948573180038201798055771036509827994938283168 1952

d=367456229405453438757599764341571978867555063587609822573085670370060743917197053156667812000656251162031995986336220260704927757436186079666523939964196638533500859142527978877427826615948802954992273860759295946415566580332073828480750733197862441611938017951059010076401742547988318632265442680041499206253959252597156252484170784573171674585924445328250398280137681818603497051922466222404757111334440549853675205645424886971676064808382947477103964010265338201912991168911864742405202539533094741669639563344307988600840724503289317008812447173269029730616674404423153150845917668811883716689451353912904767581 45

c=372098770261388243023016972923193281858240599125066447190412738959727479266985566121944553671723682772688837741027191131948506740129999713375505610616978264584683635744283786791797216725305158817619492976139678126839486220680203827712056099752204071190229666006754690447328912107892482844107394828769378577260264315932839601622987078921439705138048922483704274553184724020115360958022551212849115178822680927852469859816879133109656287931787034989616176286611132772490714905847747645711708913913550800337917456621191391708345293065486447160690251619891038806715800752796564954722997474017946357818479015881560994950 17

第三步：常规操作分解N

	Result:
number	
4321032603...51<617> = 4321032603...51<617>	

发现不行，那么还是看定义，RSA的加密与解密：

m^e%n=c 加密
c^d%n=m 解密

第四步：用python将m（明文）计算出来

```
N=432103260362901062510888102986679157020077445674678549881079372336228216717529305833785588083811970365429033965343373057234961071540503249535365309937442673860081206589102421439926567733607921826981422737611820470111192617799883774082088581095031774131945415245434478277783140990366474952052737551474867846210126144503990040899942996951078696047188715895767933719009152791334038331022581332217765769525699431504827095231500110054894955432396540464300520673277361386623591544461533797263652780595639288158892122219626720481472616420118039436680647298714768071797941290307081010086729667552569828323354008441335674251
e=65537
phi=432103260362901062510888102986679157020077445674678549881079372336228216717529305833785588083811970365429033965343373057234961071540503249535365309937442673860081206589102421439926567733607921826981422737611820470111192617799883774082088581095031774131945415245434478277783140990366474952052737551474867846168400117968102583624327264152004600110839441160831542396717012370956970195191751384795192493634757467121278969422272808702851909019413125099935851815969186416918772381571965768859857682010412345654770699579400102083775669592347658222662267708772769944632345948948573180038201798055771036509827994938283168195 2
d=367456229405453438757599764341571978867555063587609822573085670370060743917197053156667812000656251162031995986336220260704927757436186079666523939964196638533500859142527978877427826615948802954992273860759295946415566580332073828480750733197862441611938017951059010076401742547988318632265442680041499206253959252597156252484170784573171674585924445328250398280137681818603497051922466222404757111334440549853675205645424886971676064808382947477103964010265338201912991168911864742405202539533094741669639563344307988600840724503289317008812447173269029730616674404423153150845917668811883716689451353912904767581455 c=372098770261388243023016972923193281858240599125066447190412738959727479266985566121944553671723682772688837741027191131948506740129999713375505610616978264584683635744283786791797216725305158817619492976139678126839486220680203827712056099752204071190229666006754690447328912107892482844107394828769378577260264315932839601622987078921439705138048922483704274553184724020115360958022551212849115178822680927852469859816879133109656287931787034989616176286611132772490714905847747645711708913913550800337917456621191391708345293065486447160690251619891038806715800752796564954722997474017946357818479015881560994950179
m=pow(c,d,N)
print(m)
```

*>m=384365526052440202360459651805033449148582243524328138349913683453506738455616163926510705066867828115177854736411335061889102850182140300335071766036185 3

第五步：转换为字符串

> IceCTF{rsa_is_awesome_when_used_correctly_but_horrible_when_not}