i春秋第二届春秋欢乐赛 RSA2 writeup

原创

bingge15 于 2019-10-06 21:22:54 发布 212 收藏

分类专栏： CTF 文章标签： CTF RSA

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/hanjinrui15/article/details/102253455

版权


CTF 专栏收录该内容

17 篇文章 1 订阅

订阅专栏

i春秋第二届春秋欢乐赛 RSA2 writeup

第一步：题目中数据

我将题目给出的数据转换为10进制后，d是我根据代码算出来的：

N=0xee290c7a603fc23300eb3f0e5868d056b7deb1af33b5112a6da1edc9612c5eeb4ab07d838a3b4397d8e6b6844065d98543a977ed40ccd8f57ac5bc2daee2dec301aac508f9befc27fae4a2665e82f13b1ddd17d3a0c85740bed8d53eeda665a5fc1bed35fbbcedd4279d04aa747ac1f996f724b14f0228366aeae34305152e1f430221f9594497686c9f49021d833144962c2a53dbb47bdbfd19785ad8da6e7b59be24d34ed201384d3b0f34267df4ba8b53f0f4481f9bd2e26c4a3e95cd1a47f806a1f16b86a9fc5e8a0756898f63f5c9144f51b401ba0dd5ad58fb0e97ebac9a41dc3fb4a378707f7210e64c131bca19bd54e39bbfa0d7a0e7c89d955b1c9f

e=0x10001

c=0x3dbf00a02f924a70f44bdd69e73c46241e9f036bfa49a0c92659d8eb0fe47e42068eaf156a9b3ee81651bc0576a91ffed48610c158dc8d2fb1719c7242704f0d965f8798304925a322c121904b91e5fc5eb3dc960b03eb8635be53b995217d4c317126e0ec6e9a9acfd5d915265634a22a612de962cfaa2e0443b78bdf841ff901423ef765e3d98b38bcce114fede1f13e223b9bd8155e913c8670d8b85b1f3bcb99353053cdb4aef1bf16fa74fd81e42325209c0953a694636c0ce0a19949f343dc229b2b7d80c3c43ebe80e89cbe3a3f7c867fd7cee06943886b0718a4a3584c9d9f9a66c9de29fda7cfee30ad3db061981855555eeac01940b1924eb4c301

N=3006495847118014135296325596432072776494108785495738556267282166231985402139510096882334110807502
092854243744699399411986390256587435529618849830476138933643842188963640956193614198578680100292375
262729379026535172379596841277426808646711426376794769331044493431620539081418580251751469452850133
385125508465392518172697873480480670774044475590839875196489914349452278140545710369737386897283620
151142436360149090308648850698548952691031447424510633858562357136954938843486556795198686644530684
050539726828188988673801589198216237141313688598974693192978776561783875038122603678412249814317285
4419447324975505933540511
e=65537
c=7794723418575865133221710844957533763600341922604517613342495747603012554180094280541823023634873
599126585279853308940496678282266476710442981516354722804125430496779901585048718048185233664790252
394684332465074382441230073678600882729934579182285214951880877250418707254283530428901115269852700
826395665491878667661628136001999399484533201783253765516767750014674954245926135408324886326143714
299876277011335423927566142213389260930015587242338816401180184690143281167398845157288962617745058
933037815909282349958256327539704772842249498887000705177364153517572284141825022022854893024073953
342334031407154501829377
d=1837101646654330021334186119294464323271335067640889565288798233066764055246273964902495027269081
468226245929422594887355458300487700527530984887299126086512901816283167797670757789128155575526655
142965391073938191935665011393391864595977421356116881630040488071625667285775949189306748553109965
784308414810049800063607595379401147252533924504434160563528696033912002168260793067068899596593414
660684055973639147294546386601729796653637944962320635485114150256161704522591047690895368014581357
897787319758779861571557338924793938832827214946623022405976300732812023851872150290863864453083938
6083428373445455039926609

第二步：计算

```
N=30064958471180141352963255964320727764941087854957385562672821662319854021395100968823341108075020928542437446993994119863902565874355296188498304761389336438421889636409561936141985786801002923752627293790265351723795968412774268086467114263767947693310444934316205390814185802517514694528501333851255084653925181726978734804806707740444755908398751964899143494522781405457103697373868972836201511424363601490903086488506985489526910314474245106338585623571369549388434865567951986866445306840505397268281889886738015891982162371413136885989746931929787765617838750381226036784122498143172854419447324975505933540511
e=65537
c=7794723418575865133221710844957533763600341922604517613342495747603012554180094280541823023634873599126585279853308940496678282266476710442981516354722804125430496779901585048718048185233664790252394684332465074382441230073678600882729934579182285214951880877250418707254283530428901115269852700826395665491878667661628136001999399484533201783253765516767750014674954245926135408324886326143714299876277011335423927566142213389260930015587242338816401180184690143281167398845157288962617745058933037815909282349958256327539704772842249498887000705177364153517572284141825022022854893024073953342334031407154501829377
d=18371016466543300213341861192944643232713350676408895652887982330667640552462739649024950272690814682262459294225948873554583004877005275309848872991260865129018162831677976707577891281555755266551429653910739381919356650113933918645959774213561168816300404880716256672857759491893067485531099657843084148100498000636075953794011472525339245044341605635286960339120021682607930670688995965934146606840559736391472945463866017297966536379449623206354851141502561617045225910476908953680145813578977873197587798615715573389247939388328272149466230224059763007328120238518721502908638644530839386083428373445455039926609

m=pow(c,d,N)
print(m)
```

第三步：得到结果并转换为16进制后进行字符串转换

```
10进制：740261076214546811794112860369189341361210008008941391371580225182119664940497198386254540499525825894954797334654641533
```

```
16进制：4963654354467b6e6578745f74696d655f636865636b5f796f75725f6b6579735f6172656e745f666163746f7261626c657d
```

```
flag为：IceCTF{next_time_check_your_keys_arent_factorable}
```