IceCTF - RSA -WP

原创

网安小小白 于 2022-03-25 17:39:21 发布

分类专栏： CTF 文章标签： 信息安全 CTF writeup

本文链接：https://blog.csdn.net/u013671216/article/details/123741569

IceCTF - RSA

难度：简单

考点：基础知识

```
N=0x1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a0334d9fe0726f8b057c4412cfbff75967a91a370
a1c1bd185212d46b581676cf750c05bbd349d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a47099342
89dc0bc5cdc2aa97ce62a6ca6ba25fca6ae38c0b9b55c16be0982b596ef929b7c71da3783c1f20557e4803de7d2a91b5a6e85df64249f48b
4cf32aec01c12d3e88e014579982ecd046042af370045f09678c9029f8fc38ebaea564c29115e19c7030f245ebb2130cbf9dc1c340e2cf17
a625376ca52ad8163cfb2e33b6ecaf55353bc1ff19f8f4dc7551dc5ba36235af9758b

e=0x10001

phi=0x1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a0334d9fe0726f8b057c4412cfbff75967a91a3
70a1c1bd185212d46b581676cf750c05bbd349d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a470993
4289dc0bc5cdc2aa97ce62a6ca6ba25fca6ae366e86eed95d330ffad22705d24e20f9806ce501dda9768d860c8da465370fc70757227e729
b9171b9402ead8275bf55d42000d51e16133fec3ba7393b1ced5024ab3e86b79b95ad061828861ebb71d35309559a179c6be8697f8a4f314
c9e94c37cbbb46cef5879131958333897532fea4c4ecd24234d4260f54c4e37cb2db1a0

d=0x12314d6d6327261ee18a7c6ce8562c304c05069bc8c8e0b34e0023a3b48cf5849278d3493aa86004b02fa6336b098a3330180b9b9655
cdf927896b22402a18fae186828efac14368e0a5af2c4d992cb956d52e7c9899d9b16a0a07318aa28c8202ebf74c50ccf49a6733327dde11
1393611f915f1e1b82933a2ba164aff93ef4ab2ab64aacc2b0447d437032858f089bcc0ddeebc45c45f8dc357209a423cd49055752bfae27
8c93134777d6e181be22d4619ef226abb6bfcc4adec696cac131f5bd10c574fa3f543dd7f78aee1d0665992f28cdbcf55a48b32beb7a1c0f
a8a9fc38f0c5c271e21b83031653d96d25348f8237b28642ceb69f0b0374413308481

c=0x126c24e146ae36d203bef21fcd88fdeefff50375434f64052c5473ed2d5d2e7ac376707d76601840c6aa9af27df6845733b9e53982a8
f8119c455c9c3d5df1488721194a8392b8a97ce6e783e4ca3b715918041465bb2132a1d22f5ae29dd2526093aa505fcb689d8df5780fa174
8ea4d632caed82ca923758eb60c3947d2261c17f3a19d276c2054b6bf87dcd0c46acf79bff2947e1294a6131a7d8c786bed4a1c0b92a4dd4
57e54df577fb625ee394ea92b992a2c22e3603bf4568b53cceb451e5daca52c4e7bea7f20dd9075ccfd0af97f931c0703ba8d1a7e00bb010
437bb4397ae802750875ae19297a7d8e1a0a367a2d6d9dd03a47d404b36d7defe8469
```

```
import gmpy2
N = 0x1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a0334d9fe0726f8b057c4412cfbff75967a91a3
70a1c1bd185212d46b581676cf750c05bbd349d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a470993
4289dc0bc5cdc2aa97ce62a6ca6ba25fca6ae38c0b9b55c16be0982b596ef929b7c71da3783c1f20557e4803de7d2a91b5a6e85df64249f4
8b4cf32aec01c12d3e88e014579982ecd046042af370045f09678c9029f8fc38ebaea564c29115e19c7030f245ebb2130cbf9dc1c340e2cf
17a625376ca52ad8163cfb2e33b6ecaf55353bc1ff19f8f4dc7551dc5ba36235af9758b

e = 0x10001

phi = 0x1564aade6f1b9f169dcc94c9787411984cd3878bcd6236c5ce00b4aad6ca7cb0ca8a0334d9fe0726f8b057c4412cfbff75967a91
a370a1c1bd185212d46b581676cf750c05bbd349d3586e78b33477a9254f6155576573911d2356931b98fe4fec387da3e9680053e95a4709
934289dc0bc5cdc2aa97ce62a6ca6ba25fca6ae366e86eed95d330ffad22705d24e20f9806ce501dda9768d860c8da465370fc70757227e7
29b9171b9402ead8275bf55d42000d51e16133fec3ba7393b1ced5024ab3e86b79b95ad061828861ebb71d35309559a179c6be8697f8a4f3
14c9e94c37cbbb46cef5879131958333897532fea4c4ecd24234d4260f54c4e37cb2db1a0

d = 0x12314d6d6327261ee18a7c6ce8562c304c05069bc8c8e0b34e0023a3b48cf5849278d3493aa86004b02fa6336b098a3330180b9b96
55cdf927896b22402a18fae186828efac14368e0a5af2c4d992cb956d52e7c9899d9b16a0a07318aa28c8202ebf74c50ccf49a6733327dde
111393611f915f1e1b82933a2ba164aff93ef4ab2ab64aacc2b0447d437032858f089bcc0ddeebc45c45f8dc357209a423cd49055752bfae
278c93134777d6e181be22d4619ef226abb6bfcc4adec696cac131f5bd10c574fa3f543dd7f78aee1d0665992f28cdbcf55a48b32beb7a1c
0fa8a9fc38f0c5c271e21b83031653d96d25348f8237b28642ceb69f0b0374413308481

c = 0x126c24e146ae36d203bef21fcd88fdeefff50375434f64052c5473ed2d5d2e7ac376707d76601840c6aa9af27df6845733b9e53982
a8f8119c455c9c3d5df1488721194a8392b8a97ce6e783e4ca3b715918041465bb2132a1d22f5ae29dd2526093aa505fcb689d8df5780fa1
748ea4d632caed82ca923758eb60c3947d2261c17f3a19d276c2054b6bf87dcd0c46acf79bff2947e1294a6131a7d8c786bed4a1c0b92a4d
d457e54df577fb625ee394ea92b992a2c22e3603bf4568b53cceb451e5daca52c4e7bea7f20dd9075ccfd0af97f931c0703ba8d1a7e00bb0
10437bb4397ae802750875ae19297a7d8e1a0a367a2d6d9dd03a47d404b36d7defe8469

m = gmpy2.powmod(c, d, N)

m = binascii.unhexlify(hex(m)[2:])
print(m)
```