

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](#)

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/102097362>

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 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=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb454a34dab7684589bc32b19eb27cfff8c07179e349ddb62898ae896f8c681796052ae1598bd41f35491175c9b60ae2260d0d4ebac05b4b6f2677a7609c2fe6194fe7b63841cec632e3a2f55d0cb09df08eacea34394ad473577dea5131552b0b30efac31c59087bfe603d2b13bed7d14967bfd489157aa01b14b4e1bd08d9b92ec0c319aeb8fedd535c56770aac95247d116d59cae2f99c3b51f43093fd39c10f93830c1ece75ee37e5fcdc5b174052eccadcaded2f1b3a4a87184041d5c1a6a0b2eeaa3c3a1227bc27e130e67ac397b375ffe7c873e9b1c649812edcd
```

e=0x1

```
c=0x4963654354467b66616c6c735f61706172745f736f5f656173696c795f616e645f7265617373656d626c65645f736f5f63727564656c797d
```

```
N=48569461374993143516458382989564467635603212687995533770002548932068305696146454206430036911970510501028093396961651040114860255991014137256378728066480402096928051207115833090577021659486634694474223814248248099195746137687697108856640513163791613682600570270581575552412705590230671984624735843887143508632493759295004856874057751540414475973945998693145377292093389268345927200654797174898352121820385250182220064801185789344737844112885665393791671380059400017700448787295549977322406673720103637423118026614999242336902621045379655889479487238450265129455084139164700261269067095594891019208028602385503402257869
```

e=1

```
c=208364969187294709763110474149662765860879002985066102841653682079171655293372490251587249013853834399047472102123087558613560722225533
```

第二步: 分解大整数

Search	Sequences	Report results	Factor tables	Status	Downloads	Login
48569461374993143516458382989564467635603212687995533770002548932068305696146454206430036 Factorize! (?)						
Result:						
status (?)	digits	number				
C	617 (show)	4856946137...69<617> = 4856946137...69<617>				

<https://blog.csdn.net/hanjin15>

发现不太行，那么换种思路看看。

第三步：分析公式

$m^e \cdot d \% n = m$ 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）：

The screenshot shows a web interface for converting hex to text. On the left is a sidebar with 'Operations' including 'From Hex'. The main area has a 'Recipe' section with 'From Hex' selected and 'Delimiter' set to 'Auto'. The 'Input' field contains the hexadecimal string: 4963654354467b66616c6c735f6172745f736f5f656173696c795f616e645f7265617373656d626c65645f736f5f63727564656c797d. The 'Output' field displays: IceCTF{falls_apart_so_easily_and_reassembled_so_crudely}. Metadata for the input shows length: 112, lines: 1. Metadata for the output shows time: 11ms, length: 56, lines: 1.

flag为: IceCTF{falls_apart_so_easily_and_reassembled_so_crudely}