ichunqiu的RSA?的writeup，直接用Rsatool即可

原创

> John was messing with RSA again... he encrypted our flag! I have a strong feeling he had no idea what he was doing however, can you get the flag for us?

下载flag得到一个文件，里面有：

```
N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb454a34dab7684589bc32b19eb27cffff8c

e=0x1

c=0x4963654354467b66616c6c735f61706172745f736f5f656173696c795f616e645f7265617373656d626c65645f736f5f6372756
```

这个用RSAtool即可，安装教程参见：https://blog.csdn.net/dchua123/article/details/105176794

1、生成pubkey：

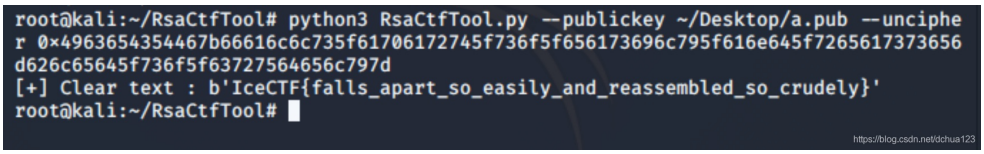
```
python3 RsaCtfTool.py -n 0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb454a34dab76
```

得key，保存成文件a.pub：

```
root@kali:~/RsaCtfTool# python3 RsaCtfTool.py -n 0x180be86dc898a3c3a710e52b31de460f
8f350610bf63e6b2203c08fddad44601d96eb454a34dab7684589bc32b19eb27cffff8c07179e349ddb
62898ae896f8c681796052ae1598bd41f35491175c9b60ae2260d0d4ebac05b4b6f2677a7609c2fe619
4fe7b63841cec632e3a2f55d0cb09df08eacea34394ad473577dea5131552b0b30efac31c59087bfe60
3d2b13bed7d14967bfd489157aa01b14b4e1bd08d9b92ec0c319aeb8fedd535c56770aac95247d116d5
9cae2f99c3b51f43093fd39c10f93830c1ece75ee37e5fcdc5b174052eccadcadeda2f1b3a4a8718404
1d5c1a6a0b2eeaa3c3a1227bc27e130e67ac397b375ffe7c873e9b1c649812edcd -e 0x1 --createp
ub
-----BEGIN PUBLIC KEY-----
MIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEBgL6G3ImKPDpxDlKzHeRg
+PNQYQv2PmsiA8CP3a1EYB2W60VKNNq3aEWJvDKxnrJ8//+MBxeeNJ3bYomK6Jb4
xoF5YFKuFZi9QfNUkRdcm2CuImDQ1OusBbS28md6dgnC/mGU/ntjhBzsYy46L1XQ
ywnfCOrOo0OUrUc1d96lExVSsLMO+sMcWQh7/mA9KxO+19FJZ7/UiRV6oBsUtOG9
CNm5LsDDGa64/t1TXFZ3CqyVJH0RbVnK4vmcO1H0MJP9OcEPk4MMHs517jfl/Nxb
F0BS7Mrcre2i8bOkqHGEBB1cGmoLLuqjw6Eie8J+Ew5nrDl7N1/+fIc+mxxkmBLt
zQIBAQ==
-----END PUBLIC KEY-----
root@kali:~/RsaCtfTool#
```

2、解密密文：

```
python3 RsaCtfTool.py --publickey ~/Desktop/a.pub --uncipher 0x4963654354467b66616c6c735f61706172745f736f5f
```



得flag：

```
IceCTF{falls_apart_so_easily_and_reassembled_so_crudely}
```