




# BUUCTF RSAROLL

原创

宁嘉  于 2020-05-15 17:39:28 发布  1551  收藏

分类专栏: [RSA加密](#) 文章标签: [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/MikeCoke/article/details/106146568>

版权



[RSA加密](#) 专栏收录该内容

12 篇文章 9 订阅

订阅专栏

得到两个记事本:

```
data.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
{920139713,19}

704796792
752211152
274704164
18414022
368270835
483295235
263072905
459788476
483295235
459788476
663551792
475206804
459788476
428313374
475206804
459788476
425392137
704796792
458265677
341524652
483295235
534149509
425392137
178212271

第 1 行, 第 1 列    100%    Unix (LF)    https://blog.csdn.net/MikeCoke
```

```
题目.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
RSA roll! roll! roll!
Only number and a-z
(don't use editor
which MS provide)

https://blog.csdn.net/MikeCoke
```

把图一中的每行数据进行解密:

上脚本:

```

import gmpy2
N,p,q,e=920139713,18443,49891,19
d=gmpy2.invert(e,(p-1)*(q-1))
result=[]

with open("C:\\Users\\MIKEWYW\\Desktop\\data.txt","r") as f:
    for line in f.readlines():
        line=line.strip('\n')#去掉列表中每一个元素的换行符
        result.append(chr(pow(int(line),d,N)))

for i in result:
    print(i,end='')

```

注意读取的密文数据要新建一个文本：只保留卷轴数据



```

704796792
752211152
274704164
18414022
368270835
483295235
263072905
459788476
483295235
459788476
663551792
475206804
459788476
428313374
475206804
459788476
425392137
704796792
458265677
341524652
483295235
534149509
425392137
428313374
425392137
241524652

```

运行得到:

flag{13212je2ue28fy71w8u87y31r78eu1e2}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)