

BUUCTF (RSA1)

原创

Bigotry77 于 2021-07-27 22:24:13 发布 488 收藏

分类专栏: [ctf](#) 文章标签: [密码学](#)

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/Bigotry77/article/details/119153634>

版权



[ctf](#) 专栏收录该内容

22 篇文章 1 订阅

订阅专栏

The screenshot shows the BUUCTF website interface. A modal window titled '题目 解题快手榜' is open, displaying the challenge 'RSA 1'. The challenge text reads: '注意: 得到的 flag 请将 noxCTF 替换为 flag, 格式为 flag{} 提交。' Below the text is a download button labeled '70a2f2f0-d...'. In the background, a sidebar menu is visible with categories like Basic, Crypto, Misc, N1BOOK, Pwn, Real, Reverse, and Web. A table on the right shows challenge statistics, including 'Quoted-printable' with 4087 solves and 1 point.

题目.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

在一次RSA密钥对生成中, 假设 $p=473398607161$, $q=4511491$, $e=17$
求解出 d 作为flag提交

<https://blog.csdn.net/Bigotry77>

看到题目第一眼能想到的就是RSA算法了, 然后百度RSA算法的原理和具体描述, emmm.....发现不是很懂

RSA公开密钥密码体制的原理是: 根据数论, 寻求两个大素数比较简单, 而将它们的乘积进行因式分解却极其困难, 因此可以将乘积公开作为加密密钥。

可以使用这个工具: RSA-Tool2 by tE 具体下载需要自己去百度找一下哈, 我自己也是在学长给的工具包里找到的。。。其中Number Base为10, Public Exponent(E)为11, 只是针对这一题, 别的题目可能不一样。

还有一种方法就是用python写代码

```
def getEuler(prime1, prime2):
    return (prime1 - 1) * (prime2 - 1)

def getDkey(e, Eulervalue):
    k = 1
    while True:
        if ((Eulervalue * k) + 1) % e == 0:
            (d, m) = divmod(Eulervalue * k + 1, e)
            return d
        k += 1

def Ming(c, d, n):
    return pow(c, d, n)

if __name__ == '__main__':
    p = 473398607161
    q = 4511491
    d = getDkey(17, getEuler(p, q))
    print('私钥为: %d' % d)
```

最后也可求出d