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

本文链接：https://blog.csdn.net/Bigotry77/article/details/119153634

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