# CTF之这次的题都不会

原创

soohyukkk 于 2021-04-26 20:48:04 发布 81 收藏

文章标签： 密码学



本文链接：https://blog.csdn.net/soohyukk/article/details/116169184

版权

4.20–4.26

这还只是题目，等我会做了再写！！

## 目录



---

## 一、bd

> 维纳攻击，首先从github上面下载攻击脚本：https://github.com/pablocelayes/rsa-wiener-attack

然后编写攻击脚本：

```
from Crypto.Util.number import *
import ContinuedFractions, Arithmetic, RSAvulnerableKeyGenerator

def hack_RSA(e,n):
    '''
    Finds d knowing (e,n)
    applying the Wiener continued fraction attack
    '''
    frac = ContinuedFractions.rational_to_contfrac(e, n)
    convergents = ContinuedFractions.convergents_from_contfrac(frac)

    for (k,d) in convergents:

        #check if d is actually the key
        if k!=0 and (e*d-1)%k == 0:
            phi = (e*d-1)//k
            s = n - phi + 1
            # check if the equation x^2 - s*x + n = 0
            # has integer roots
            discr = s*s - 4*n
            if(discr>=0):
                t = Arithmetic.is_perfect_square(discr)
                if t!=-1 and (s+t)%2==0:
                    print("Hacked!")
                    return d


if __name__ == "__main__":
    c = 37625098109081701774571613785279343908814425141123915351527903477451570893536663171806089364574293449414
561630485312247061686191366669404389142347972565020570877175992098033759403318443705791866939363061966538210758611679849037990315161035649389943256526167843576617469134413191950908582922902210791377220066
    e = 46867417013414476511855705167486515292101865210840925173161828985833867821644239088991107524584028941183216735115986313719966458608881689802377181633111389920813814350964315420422257050287517851213109465823444767895817372377616723406116946259672358254060231210263961445286931270444042869857616609048537240249
    N = 86966590627372918010571457840724456774194080910694231109811773050866217415975647358784246153710824794652840306389428729923771431340699346354646708396564203957270393882105042714920060055401541794748437242707186192941546185666953574082803056612193004258064074902605834799171191314001030749992715155125694272289
    d = hack_RSA(e, N)
    m = pow(c, d, N)
    flag = long_to_bytes(m).decode()
    print(flag)
```

运行后获得答案：

## 二、逆转思维

## 逆转思维？

实训描述：　你知道php伪协议、文件包含漏洞、反序列化吗？

实训环境：　创建环境



## 三、ezrsa

### ezrsa？

实训描述：　Related Message Attack，最后以SeBaFi{}的形式提交得到的{}中的内容。

实训附件：　下载



## 四、GM

### GM？

实训描述：　RSA题目，最后以SeBaFi{}的形式提交得到的{}中的内容。

实训附件：　下载