攻防世界 Crypto高手进阶区 4分题 best_rsa

原创

思源湖的鱼 于 2020-12-24 13:52:02 发布 299 收藏 2

分类专栏： ctf 文章标签： ctf 攻防世界 crypto rsa 共模攻击

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111625064

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

本篇是best_rsa的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

给了两个密文和两个密钥

提取公钥信息

```
from Crypto.PublicKey import RSA
import libnum
import gmpy2

c1=libnum.s2n(open('cipher1.txt','rb').read())
c2=libnum.s2n(open('cipher2.txt','rb').read())

pub1=RSA.importKey(open('publickey1.pem').read())
pub2=RSA.importKey(open('publickey2.pem').read())

n1 = pub1.n
e1 = pub1.e
n2 = pub2.n
e2 = pub2.e

print(n1)
print(n2)
print(e1)
print(e2)
```

得到

```
n1 = 13060424286033164731705267935214411273739909173486948413518022752305313862238166593214772698793487761875251
03042351699351971421530680867772410469247419921511938772574190607155343784025678622048458288469328614053749254 10
93086953005486704542435188521724013251087887351409946184501295224744819621937322469140771245380081663560150133 16
26921744986424745881684441675336212598246405995300528278785584810361552227339861794875776933606973901523709017 46
11265375833845608344087872600722930783003780868105030299041123866672760825345257369690408313386609379198556511 80
32742893247076947480766837941319251901579605233916076425572961
n2 = 13060424286033164731705267935214411273739909173486948413518022752305313862238166593214772698793487761875251
03042351699351971421530680867772410469247419921511938772574190607155343784025678622048458288469328614053749254 10
93086953005486704542435188521724013251087887351409946184501295224744819621937322469140771245380081663560150133 16
26921744986424745881684441675336212598246405995300528278785584810361552227339861794875776933606973901523709017 46
11265375833845608344087872600722930783003780868105030299041123866672760825345257369690408313386609379198556511 80
32742893247076947480766837941319251901579605233916076425572961
e1 = 117
e2 = 65537
```

两个文件的模数相同
共模攻击

```
from Crypto.PublicKey import RSA
import libnum
import gmpy2

c1=libnum.s2n(open('cipher1.txt','rb').read())
c2=libnum.s2n(open('cipher2.txt','rb').read())

pub1=RSA.importKey(open('publickey1.pem').read())
pub2=RSA.importKey(open('publickey2.pem').read())
n = pub1.n
e1= pub1.e
e2= pub2.e

s = gmpy2.gcdext(e1,e2)
s1 = s[1]
s2 = s[2]

if s1<0:
 s1 = -s1
 c1 = gmpy2.invert(c1, n)
elif s2<0:
 s2 = -s2
 c2 = gmpy2.invert(c2, n)

m = pow(c1,s1,n)*pow(c2,s2,n) % n
flag = libnum.n2s(m)
print(flag)
```

得到flag：`flag{interesting_rsa}`

结语

共模攻击