攻防世界 Crypto高手进阶区 4分题 RSA256

原创

思源湖的鱼 于 2020-12-17 13:02:04 发布 171 收藏

分类专栏： ctf 文章标签： rsa 攻防世界 ctf crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111312804

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

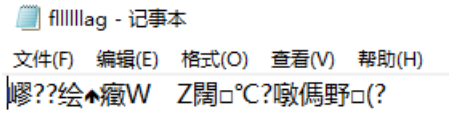
本篇是RSA256的writeup

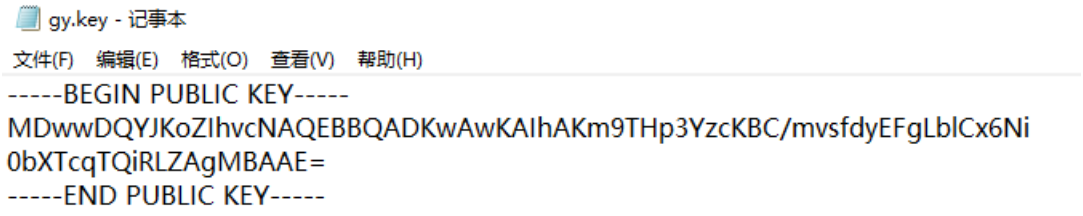
发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到两个文件





扔进openssl

```
cy@kalifisher:~/ctf$ openssl rsa -pubin -text -modulus -in gy.key
RSA Public-Key: (256 bit)
Modulus:
    00:a9:bd:4c:7a:77:63:37:0a:04:2f:e6:be:c7:dd:
    c8:41:60:2d:b9:42:c7:a3:62:d1:b5:d3:72:a4:d0:
    89:12:d9
Exponent: 65537 (0x10001)
Modulus=A9BD4C7A7763370A042FE6BEC7DDC841602DB942C7A362D1B5D372A4D08912D9
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAKm9THp3YzcKBC/mvsfdyEFgLblCx6Ni
0bXTcqTQiRLZAgMBAAE=
-----END PUBLIC KEY-----
```

得到`n=767753333402239611394270507078404178111569780851469703123158866715466662591 61`

素数分解

767753333402239611394270507078404178111569780851469703123158866715466662591 61 Factorize! (?)

Result:		
status (?)	digits	number
FF	77 (show)	7677533334...61<77> = 27382110802096828837291142451920104433 3<39> · 28038500718631511582848300086755998351 7<39>

得到

```
p =  27382110802096828837291142451920104433 3
q =  28038500718631511582848300086755998351 7
```

脚本

```
#coding:utf-8
import gmpy2
import rsa
p = 27382110802096828837291142451920104433 3
q = 28038500718631511582848300086755998351 7
n = 767753333402239611394270507078404178111569780851469703123158866715466662591 61
e = 65537
d = int(gmpy2.invert(e,(p-1)*(q-1)))
privatekey = rsa.PrivateKey(n,e,d,p,q)
with open("E:\\fllllllag.txt","rb") as f:
    print(rsa.decrypt(f.read(),privatekey).decode())
```

得到：`flag{2o!9_CTF_ECUN}`

但实际的flag是`flag{2o!9CTFECUN}`

结语

RSA