小指数rsa 多线程版writeup

原创

lulu_ctf 于 2016-08-17 14:58:00 发布 776 收藏

下载flag.enc 和pubkey.pem文件

将pem文件拖入**openssl**得到n(modulus)和e(exponent)

```
 openssl rsa -pubin -text -modulus -in pubkey.pem
```

需从github下载libnum,gmpy

```
from multiprocessing import Pool
from libnum import s2n
import gmpy
workerCount=4
n=0xB0BEE5E3E9E5A7E8D00B493355C618FC8C7D7D03B82E409951C182F398DEE3104580E7BA70D383
e=3
f=open('exp/flag.enc','rb')
c=f.read()
c=s2n(c)
f.close()
def worker(workerID):
    global workerCount
    print("[%d] " % workerID, "Worker start, workerID =", workerID, ",workerCount =", workerCount)
    ibase = 0
    i = ibase + workerID
    while True:
        gTempC = gmpy.mpz(c + i * n)
        (M, flag) = gmpy.root(gTempC, e)
        if flag == True :
            print("[%d] " % workerID, "Found! i =", i, "; M = ", M)
            break
        ibase = ibase + workerCount
        i = ibase + workerID




if __name__ == '__main__':
    pool = Pool(workerCount)
    pool.map(worker, range(workerCount))
    pool.close()
    pool.join()
```