[ACTF新生赛2020]crypto-rsa3

原创

雨后初雾& 于 2022-04-24 15:29:46 发布 150 收藏
分类专栏： 密码学CTF 文章标签： CTF Crypt

题目描述

```
from Crypto.Util.number import *

import gmpy2

import random

e=65537

p = getPrime(512)

q = int(gmpy2.next_prime(p))

n = p*q

m = bytes_to_long(FLAG)

c = pow(m,e,n)

print(n)

print(c)

#n=17760650483649924697095903022687160888596932177821105108052463408451697333144164499389802955

#c=14573903785113823547710005409453611689847750526930736416823750714074908512897030709057495255
```

明显的RSA加密

因为p和q十分接近，所以可以使用yafu直接分解

yafu用于自动整数因式分解，在RSA中，当p、q的取值差异过大或过于相近的时候，使用yafu可以快速的把n值分解出p、q值，原理是使用Fermat方法与Pollard rho方法等。

```
from Crypto.Util.number import *
import gmpy2
e=65537
n=177606504836499246970959030226871608885969321778211051080524634084516973331441644993898029573612290095853
c=145739037851138235477100054094536116898477505269307364168237507140749085128970307090574952583048303598873
q=133269090503574476435265858368339693780781470577230547014328421929887176493857314300950556223035495772334
p=133269090503574476435265858368339693780781470577230547014328421929887176493857314300950556223035495772334
phi=(p-1)*(q-1)
d=inverse(e,phi)
m=pow(c,d,n)
print(m)
#m=893441512863695667867454629314548913750576288726628646106246575194731343607717680126106810553506844477705
#m=616374667b705f616e645f715f73686f756c645f6e6f745f62655f736f5f636c6f73655f696e5f76616c75657d
#m=actf{p_and_q_should_not_be_so_close_in_value}
```