github.com

CTFs/2019_picoCTF/miniRSA.md at master · Dvd848/CTFs

Dvd848

~3 minutes

miniRSA

Cryptography, 300 points

Description:

Lets decrypt this: ciphertext? Something seems a bit small

```
N:
2933192249979498578273597604559116493668305938055895038656
e: 3

ciphertext (c):
220531641393113403107460374692824779903015522125251987264
```

Solution:

This challenge is similar to last year's Safe RSA.

We'll reuse the script from the previous challenge:

```
import gmpy2

n =
2933192249979498578273597604559116493668305938055895038656016010574034320151336993900630753116592
e = 3
cipher_str =
2205316413931134031074603746928247799030155221252519872649602375643231006596573791863783976856797

gs = gmpy2.mpz(cipher_str)
gm = gmpy2.mpz(n)
ge = gmpy2.mpz(e)

root, exact = gmpy2.iroot(gs, ge)
print format(root, 'x').decode('hex')
```

Output:

```
root@kali:/media/sf_CTFs/pico/miniRSA# python solve.py
picoCTF{n33d_a_lArg3r_e_11db861f}
```