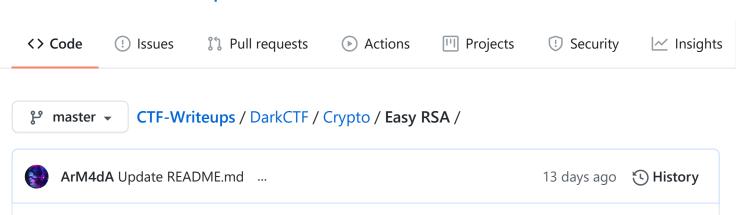
☐ t3rmin0x / CTF-Writeups



README.md

Easy RSA

README.md

Points: 407

Description

Just a easy and small E-RSA for you:)

File

Solution

A very simple RSA form :) The modulo N isn't given. Why?

Because we don't need it!

Assuming the N to be a big 2048-bit number (general format) and my plaintext (flag) to be relatively small it's clear that $(pt ^ e) < N$

This is the vulnerabilty as a mod b = a when a < b so $ct = (pt ^ e)$ mod N becomes equivalent to $ct = (pt ^ e)$.

Taking e-th root of ciphertext will retrieve the plaintext (flag).

13 days ago

```
#!/bin/env python3
from Crypto.Util.number import long_to_bytes
import gmpy2

ct = 7041534847151588467551026880218940076847782937458303730999688262671041368816140
e = 3

# Calculating e-th root of ciphertext
pt = gmpy2.iroot(ct,e)[0]
print("Flag is : " + str(long_to_bytes(pt).decode()))
```

Flag

darkCTF{5m4111111_3_4tw_xD}