README.md

CTFNAME

RSA

Cyrptography / 60pts

Description

This time John managed to use RSA " correctly "&ellipsis; I think he still made some mistakes though. flag.txt

Solution

First of all: WTF?! Why am i so...

WTF#1: " correctly " - it is correctly, at least every provided string is correct, I spent so much time to check them

WTF#2: &ellipsis; - is it "..." or is it "elliptic attack"

Well both WTF took so much time from me before I got that 60pts chall can't be so difficult

Success:

They provided everything we need in flag file. Even more:

- N - which is modulus
- c - whichi is encrypted test
- d - which is private exponent
- e - anyway it can only 3 or 65537, so not a big deal to have it
- Phi - which is phi(N) = (p-1)*(q-1) ... and we do not need this!!!

All we really need are N, c, d

m=c^mod(N)

Using Python `_pow(c,d,N)_` function:

```
c=0x126c2...
d=0x12314...
N=0x1564a...
print (hex((pow(c,d,N)))[2:][:-1].decode('hex'))
```

first we use pow to decrypt message, it will be provided in INT, INT will be converted to HEX, HEX to string and we have flag

Flag

IceCTF{rsa_is_awesome_when_used_correctly_but_horrible_when_not}