

zh3r0 2020 Crypto - RSA warmup

deuterium — 2020-06-18

Canonical HTML: <https://deut-erium.github.io/WriteUps/2020/zh3r0/crypto/RSA-Warmup/2020-06-18-zh3r0-2020-RSA-warmup.html>

Abstract

CTF writeup: SymPy finds the small prime that skipped leg day in zh3r0 CTF 2020's RSA Warmup. Factor the modulus, then decrypt with the recovered key.

RSA-Warmup

Description

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret.

You all know this :p
here is a warmup question.

```
nc crypto.zh3r0.ml 8451
```

Author : Finch

Lets quickly net cat

```
nc crypto.zh3r0.ml 8451
```

N:

```
43548487870732371760955890842849173208020062049622270622561208147070504533882656873883
95034418958102598296848051946357195851407739670247559761851352621870245520928144557235
95911873136367728098843543576413761698077300341835156919036506196997741966308833553400
592985253519980085783152705343962743180838960657525326043909
```

e 65537

CT:

```
34457418037424162484870593462086954519073633790726625231891117138329024389712986206231
30268311871869767041773055906260824999945000755707381822840396512563974378680017489700
87145045390243038430722206063983740148183702626114632523965797127289304488799040619348
710378056179517002039171315275774158768719676479442190241480
```

We have N, we have e, we have CT, No other information, This is most likely to be the generic RSA challenge where N is some special case factorizable. OKAY lets do this

```
from pwn import remote
from sympy import factorint

HOST, PORT = "crypto.zh3r0.ml", 8451
REM = remote(HOST, PORT)

n = int(REM.recvline().strip()[2:])
e = int(REM.recvline().strip()[2:])
```

```
c = int(REM.recvline().strip()[3:])

p, q = factorint(n)
phi = (p-1)*(q-1)
d = pow(e, -1, phi)
m = pow(c, d, n)

print(bytes.fromhex(hex(m)[2:]).decode())
# zh3r0{RSA_1s_Fun}
```

And we get our flag, just like that.

Checking why was it easily factorizable?

```
p,q =
(2942026403,
13457507041793036403600372774137668561581246195435048456970843701466799468071381378146
81839833862340119620701466842340112806277859554029313398803396891458368205227266305620
36268896319664602063579145594582463191728917055827142635500611088623983035188866470062
494891880603875253301899285045944864340088876075089)
```

Since p was small, RSA makes no promise 😞

zh3r0-RSA_1s_Fun"

Interactive controls are omitted from this PDF. See the canonical HTML version.