# WEEK 4

## {Crypto}

### [easy_rsa]

共模攻击，但 gcd 不等于 1，最后要开三次方，脚本如下。

```
from Crypto.Util.number import *
import sympy

def gcd(a,b):
    if a < b:
        a,b = b,a
    while b != 0:
        tem = a % b
        a = b
        b = tem
    return a

def egcd(a, b):
  if a == 0:
    return (b, 0, 1)
  else:
    g, y, x = egcd(b % a, a)
    return (g, x - (b // a) * y, y)

e1=0x33240
e2=0x3e4f
n=0x9439682bf1b4ab48c43c524778c579cc844b60872275725c1dc893b5bcb358b9f136e4dab2a06318bb0c80e202a14bc54ea334519bec023934e01e9378abf329893f3870979e9f2f2be8fff4df931216a7
c1=0x7c7f315a3ebbe305c1ad8bd2f73b1bb8e300912b6b8ba1b331ac2419d3da5a9a605fd6291bc11f8921c450525d2efda7d48f1e503041498f4f0676760b43c770ff2968bd942c7ef95e401dd7facbd4e54
c2=0xf3a8b9b739196ba270c8896bd3806e9907fca2592d28385ef24afadc2a408b7942214dad5b9e14808ab988fb15fbd93e725edcc0509ab0dd1656557019ae93c38031d2a7c84895ee3da1150eda04cd281

GCD=gcd(e1,e2)
s = egcd(e1, e2)
s1 = s[1]
s2 = s[2]

if s1<0:
    s1 = - s1
    c1 = inverse(c1, n)
elif s2<0:
    s2 = - s2
    c2 = inverse(c2, n)

m = pow(c1,s1,n)*pow(c2,s2,n) % n
m = sympy.root(m, GCD)
print(m)
```

最后 flag 为

```
hrh@hrh-study ~/Desktop python same_n.py
59594981651654789
```