Week2

CRYPTO

signin

```
m = s2n(FLAG)
a = number.getPrime(1024)
p = number.getPrime(1024)

c = a ** p * m % p
```

易得 m = c * (a ^ p) ^ -1 % p,因为题中 a,p 均为质数,所以 a ^ p % p = a % p,而 a ^ -1 % p = a ^ (p - 2) % p, 所以 m = c * a ^ (p - 2) % p , 而 a , p , c 均已知， 计算可得 flag 。

WhitegiveRSA

已知 N , e , c ,需计算出 fi (N) , 进而算出 d 。借助网上工具 ，将 N 分解 , 得 N = 2 ^ 4 · 3 ^ 6 · 7 · 313 · 18755747 · 120652274417· 56078215438603 · 272140105763859736181 , 所以 fi (N) = (2 ^ 4 - 1) · (3 ^ 6 - 1) · (7 - 1) · (313 - 1) · (18755747 - 1) · (120652274417 - 1) · (56078215438603 - 1) · (272140105763859736181 - 1) , d = e ^ (fi (N) - 1) % fi (N) 。最后，通过 plaintext = c ^ d % N , 计算得出 flag 。