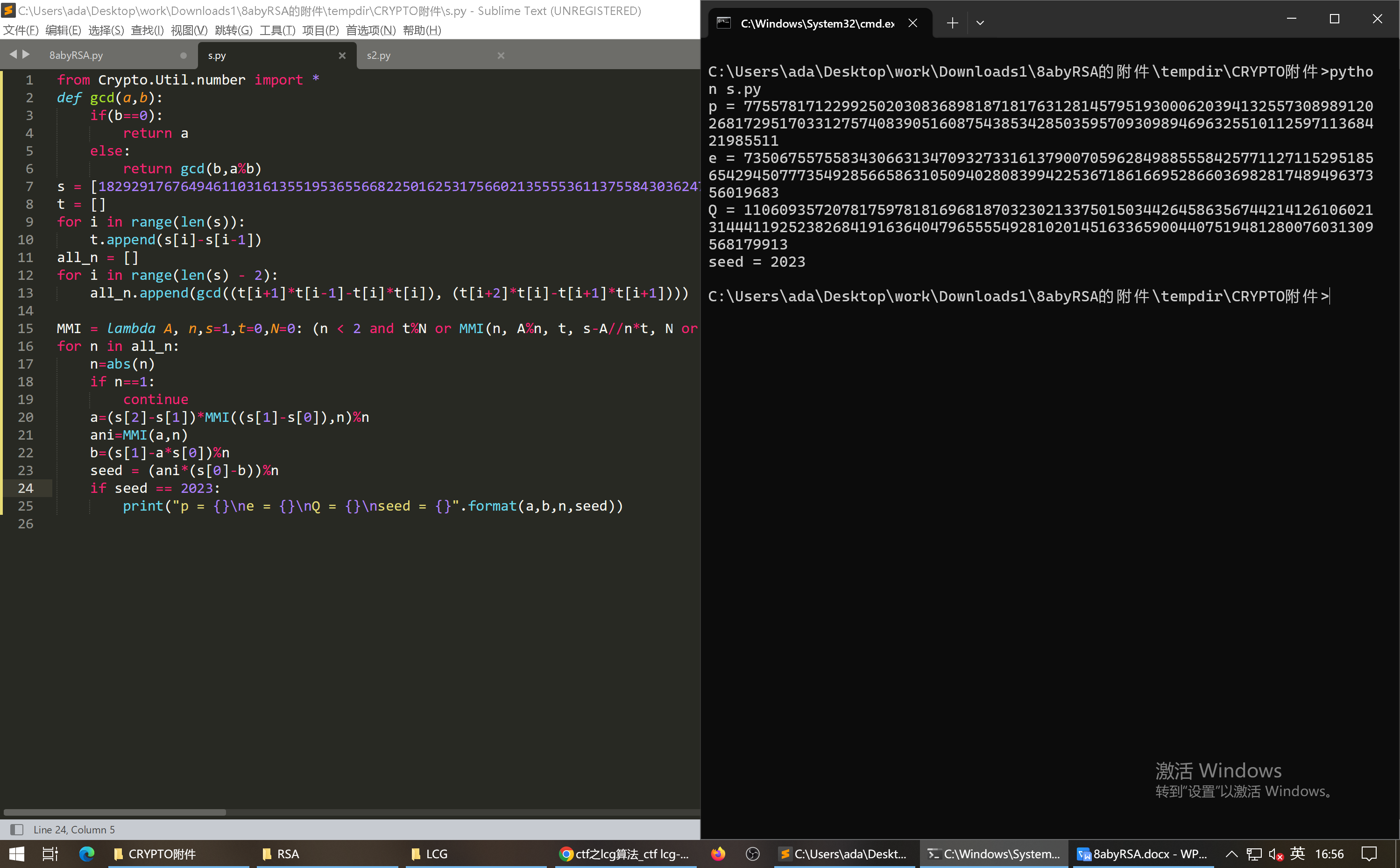
8abyRSA

LCG把输出跑脚本，获得lcg的三个参数，有个很恶心的事，他用了自己写的库LCGRandom，但是又没给出源码，四个参数代表什么纯靠蒙。



然后解出来的实际上是Q（Q = pow(q, 2, p)）而不是RSA里的q，这里用到了e=2时的RSA衍生算法RABIN，但是又不符合RABIN要求的模四余三……坑一大堆

RABIN强行按照p=p q=1解密后，获得可能的q值，再把pq带入到RSA中解密，得到FLAG

