Hgame week1 ---Conner

CRYPTO

1.RSA Attack

2.RSA Attack2

CRYPTO

1.RSA Attack

www,过年摸了，只会做RSA。

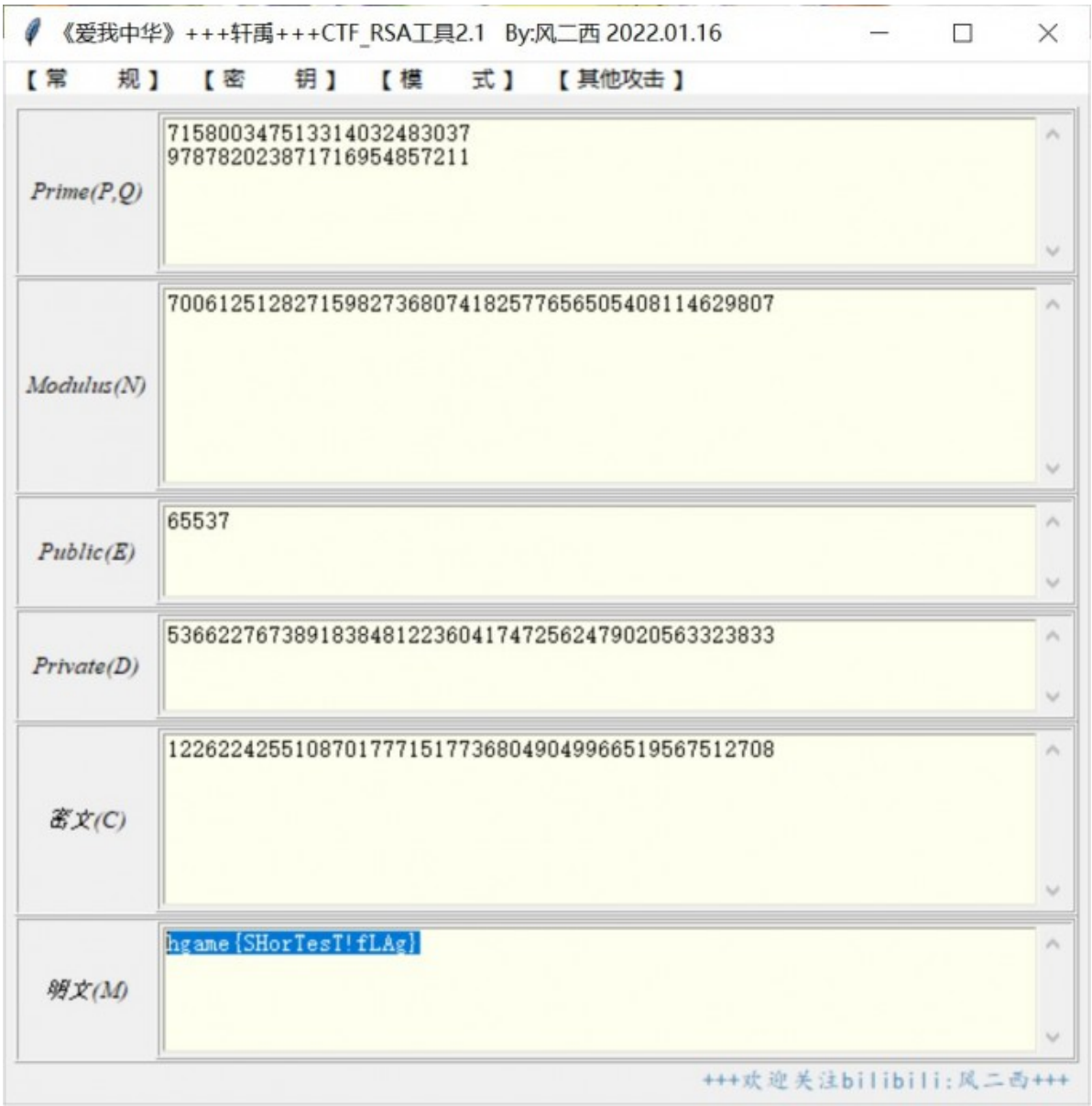
先看题目，只给了e,n,c没什么套路，题目说暴力，我们就暴力把p,q弄出来

Result:

tatus (?)	digits	number
F	48 (show)	700612512827159827368074182577656505408114629807<48> = 715800347513314032483037<24> · 978782023871716954857211<24>

放到网站上，运气好直接得到了p,q 之后就是RSA的常见套路了

直接用小工具

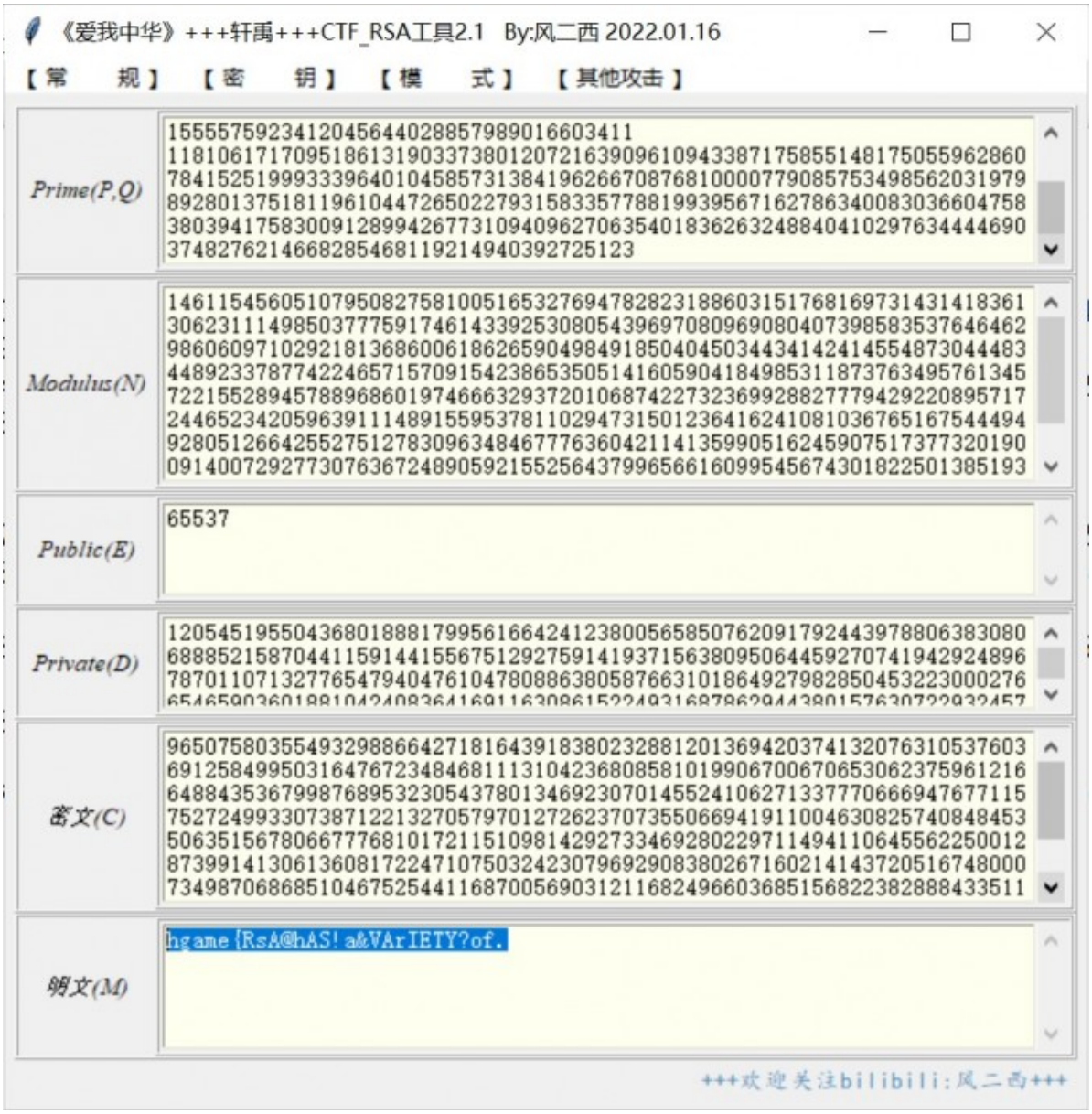


2.RSA Attack2

www,这题就RSA大杂烩了,一瞅这n都好几行，给我小网站都整懵了

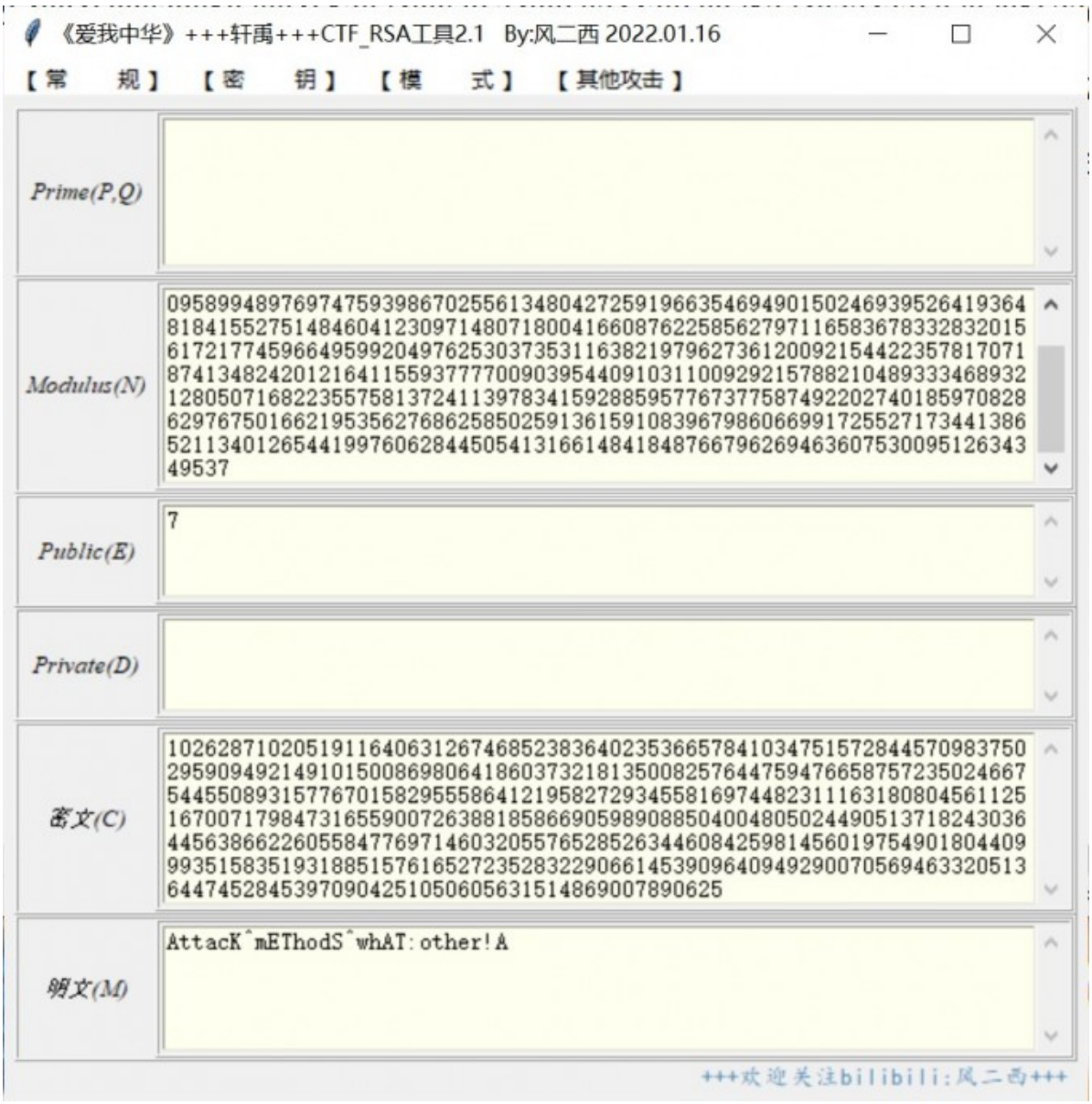
经过学习，了解到第一段属于模不互素，第二段是小e攻击，第三段是共模攻击

进行具体操作，第一段先找出n1,n2的公因数作为q，然后用一组,n,e,p,c，求出剩下的q和m就好了

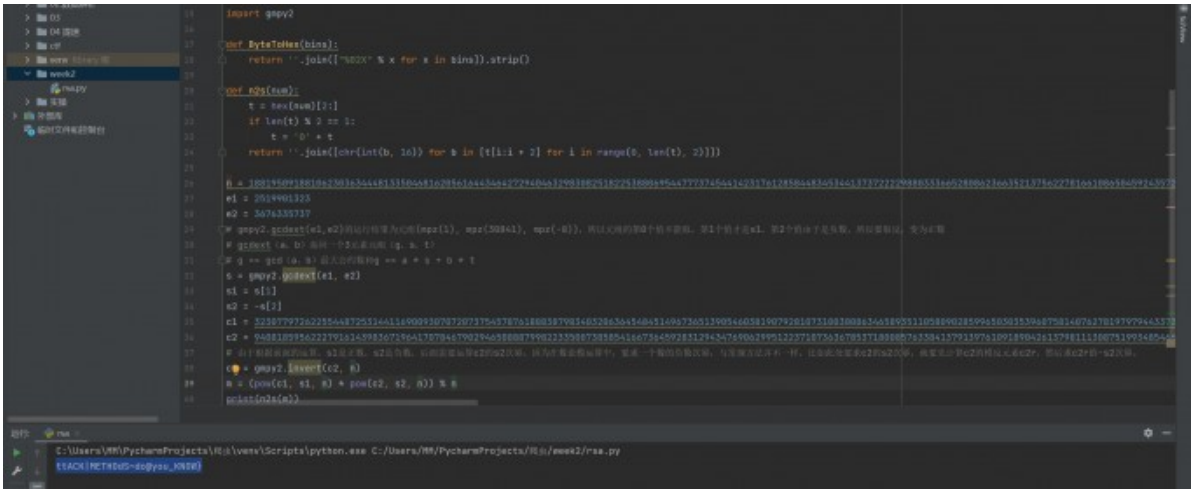


然后第二部分，这个好啊，都不用算pq了

直接丢进小工具里


《爱我中华》+++轩禹+++CTF_RSA工具2.1 By:风二西 2022.01.16
【常 规】 【密 钥】 【模 式】 【其他攻击】
Prime(P,Q)
Modulus(N)
0958994897697475939867025561348042725919663546949015024693952641936481815527514846041230971480718004166087622585627971165836783328320156172177459664959920497625303735311638219796273612009215442235781707187413482420121641155937777009039544091031100929215788210489333468932128050716822355758137241139783415928859577673775874922027401859708286297675016621953562768625850259136159108396798606699172552717344138652113401265441997606284450541316614841848766796269463607530095126343 49537
Public(E)
7
Private(D)
密文(C)
1026287102051911640631267468523836402353665784103475157284457098375029590949214910150086980641860373218135008257644759476658757235024667544550893157767015829555864121958272934558169744823111631808045611251670071798473165590072638818586690598908850400480502449051371824303644563866226055847769714603205576528526344608425981456019754901804409993515835193188515761652723528322906614539096409492900705694633205136447452845397090425105060563151486900789062 5
明文(M)
AttacK^mEThodS^whAT:other!A
+++欢迎关注bilibili:风二西+++

最后第三段，共模攻击，用Py脚本跑了一下，



拼接一下，终于结束了。