

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

《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)	715800347513314032483037 978782023871716954857211
Modulus(N)	700612512827159827368074182577656505408114629807
Public(E)	65537
Private(D)	536622767389183848122360417472562479020563323833
密文(C)	122622425510870177715177368049049966519567512708
明文(M)	hgame {SHorTesT!fLAg}

+++欢迎关注bilibili:风二西+++

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 n_1, n_2 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

《爱我中华》+++轩禹+++CTF_RSA工具2.1 By:风二西 2022.01.16

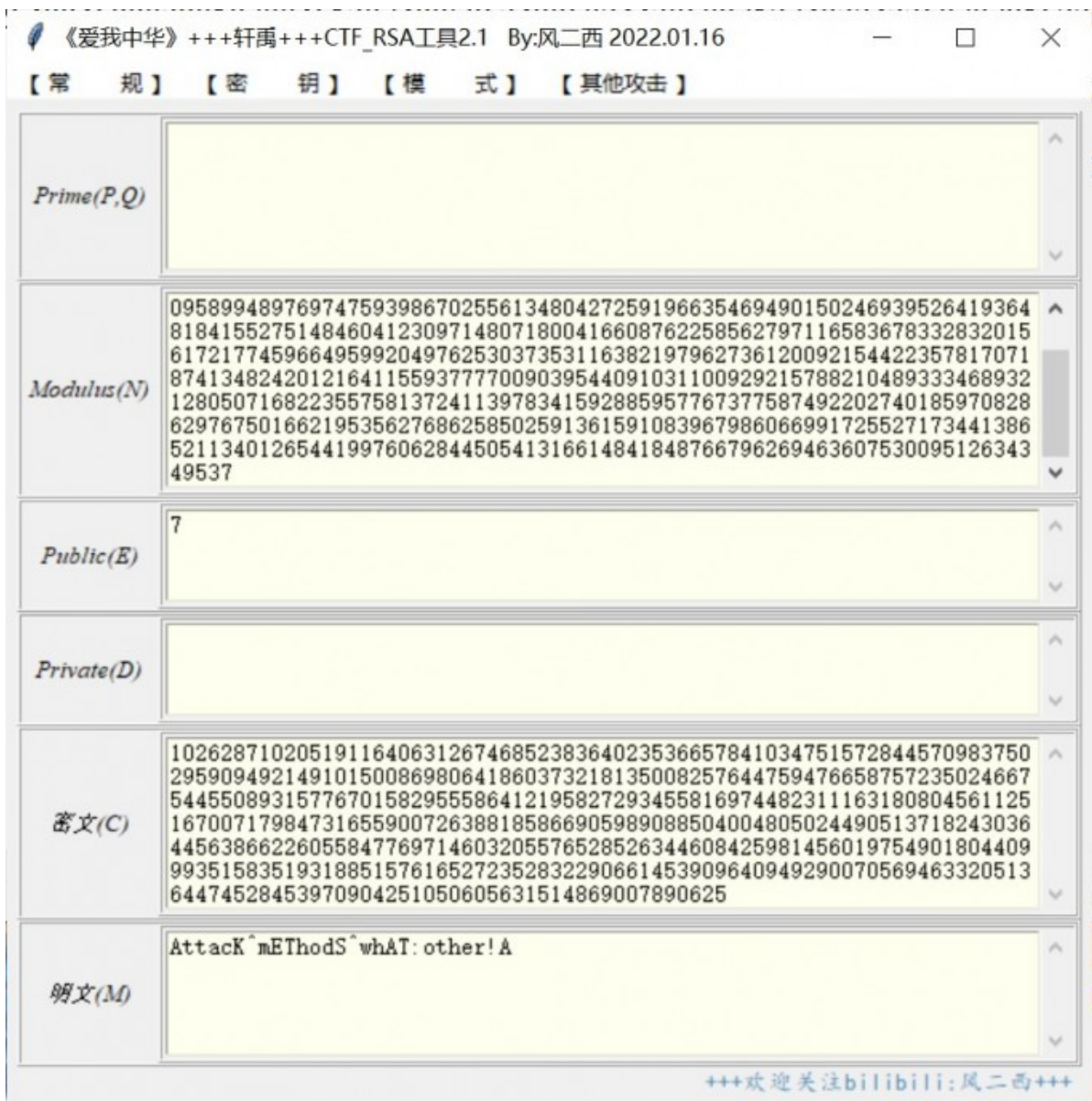
【 常 规 】 【 密 钥 】 【 模 式 】 【 其他攻击 】

Prime(P,Q)	1555575923412045644028857989016603411 11810617170951861319033738012072163909610943387175855148175055962860 78415251999333964010458573138419626670876810000779085753498562031979 89280137518119610447265022793158335778819939567162786340083036604758 38039417583009128994267731094096270635401836263248840410297634444690 3748276214668285468119214940392725123
Modulus(N)	14611545605107950827581005165327694782823188603151768169731431418361 30623111498503777591746143392530805439697080969080407398583537646462 98606097102921813686006186265904984918504045034434142414554873044483 44892337877422465715709154238653505141605904184985311873763495761345 72215528945788968601974666329372010687422732369928827779429220895717 24465234205963911148915595378110294731501236416241081036765167544494 92805126642552751278309634846777636042114135990516245907517377320190 09140072927730763672489059215525643799656616099545674301822501385193
Public(E)	65537
Private(D)	12054519550436801888179956166424123800565850762091792443978806383080 68885215870441159144155675129275914193715638095064459270741942924896 78701107132776547940476104780886380587663101864927982850453223000276 65465903601881042408264160116308615224931687862944380157630722932457
密文(C)	96507580355493298866427181643918380232881201369420374132076310537603 69125849950316476723484681113104236808581019906700670653062375961216 64884353679987689532305437801346923070145524106271337770666947677115 75272499330738712213270579701272623707355066941911004630825740848453 50635156780667776810172115109814292733469280229711494110645562250012 87399141306136081722471075032423079692908380267160214143720516748000 73498706868510467525441168700569031211682496603685156822382888433511
明文(M)	hgane {RsA@hAS! a&VArIETy?of.

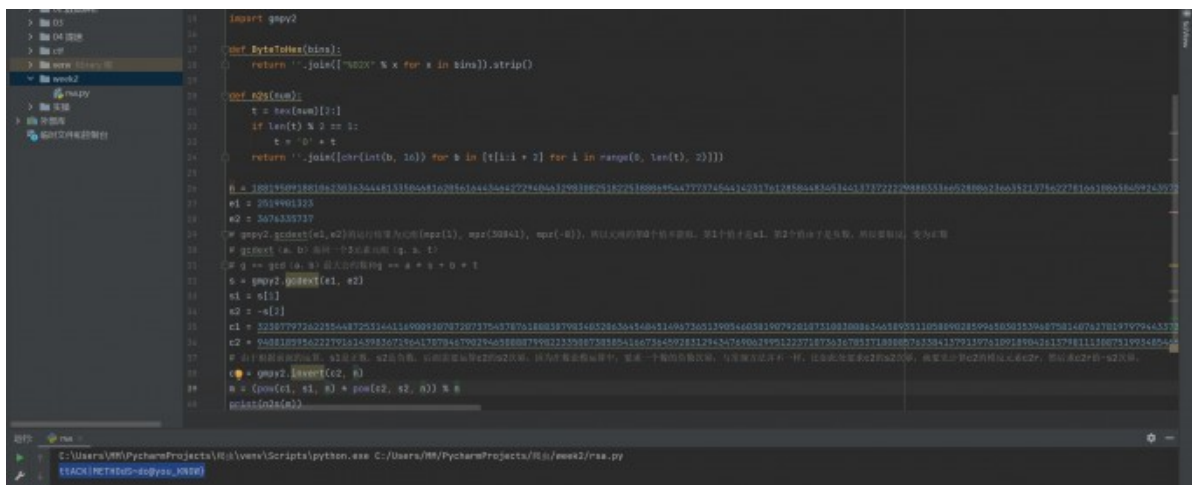
+++欢迎关注bilibili:风二西+++

然后第二部分, 这个好啊, 都不用算pq了

直接丢进小工具里



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。