Hgame week1 ---Conner

CRYPTO

1. Block Cipher
2. Multi Prime RSA
3. RSA Attack3

呜呜呜，我想做出一道web。。。。。

crypto

1.Block Cipher

www,先去搜一搜block cipher是什么意思，得知是块加密，题目把加密用的Iv，key以及加密后的结果告诉我们，理清题目使用xor加密，那就用再和相应的元素xor回去就行了，贴下解密的代码

```
iv = b'Up\x14\x98r\x14%\xb9'
key = b'\r\xe8\xb86\x9c33^'
parts = [b'0\xff\xcd\xc3\x8b\\T\x8b', b'RT\x1e\x89t&\x17\xbd', b'\x1a\xee\x8d\xd6\x9b>w\x8c', b'9CT\xb3^pF\xd0']
yi=xor(b'0\xff\xcd\xc3\x8b\\T\x8b',b'\r\xe8\xb86\x9c33^')
er=xor(b'RT\x1e\x89t&\x17\xbd',b'\r\xe8\xb86\x9c33^')
san=xor(b'\x1a\xee\x8d\xd6\x9b>w\x8c',b'\r\xe8\xb86\x9c33^')
si=xor(b'9CT\xb3^pF\xd0',b'\r\xe8\xb86\x9c33^')
print(yi,er,san,si)
si=xor(si,b'\x1a\xee\x8d\xd6\x9b>w\x8c')
san=xor(san,b'RT\x1e\x89t&\x17\xbd')
er=xor(er,b'0\xff\xcd\xc3\x8b\\T\x8b')
yi=xor(yi,iv)
print(yi,er,san,si)
```

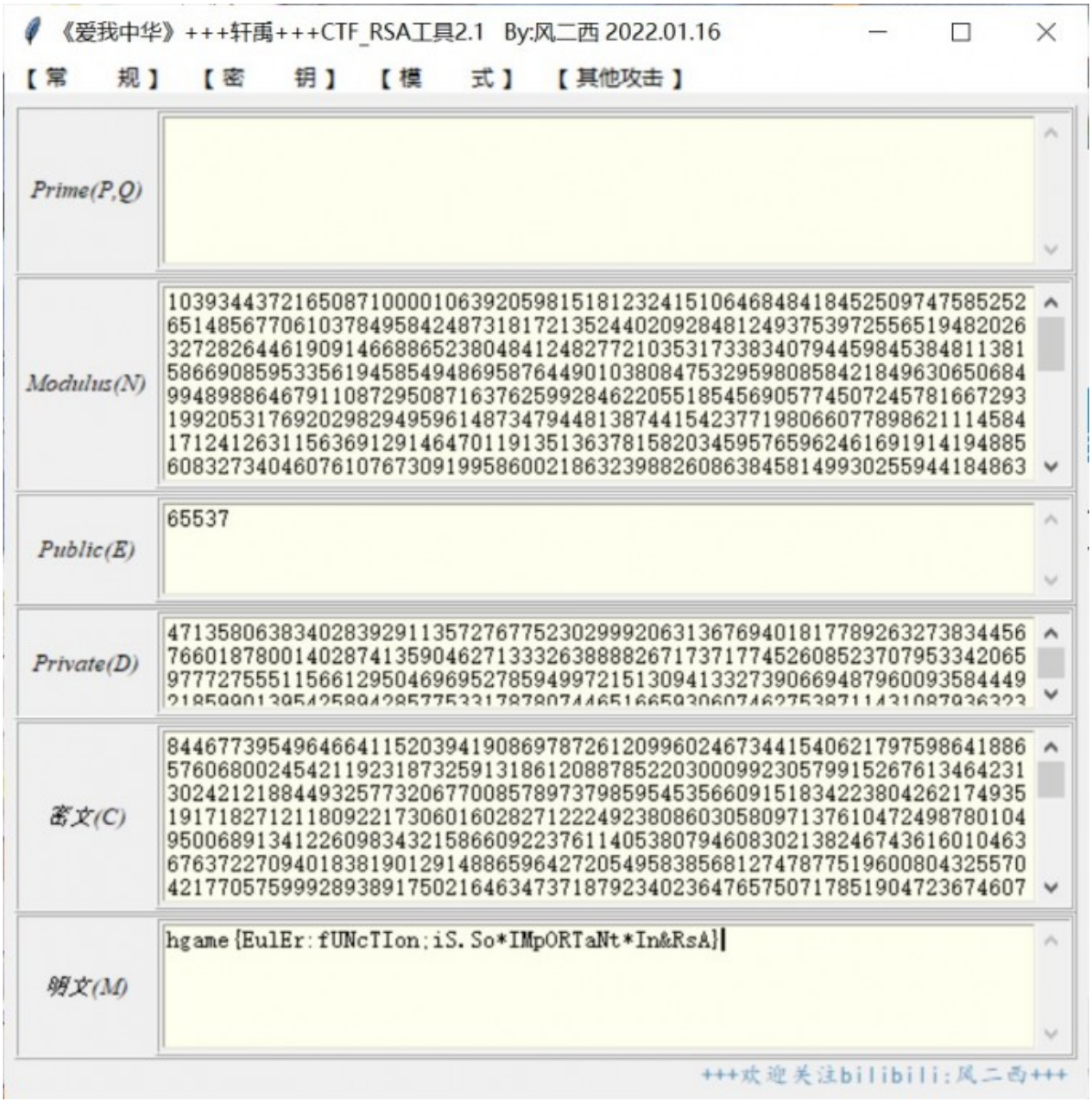
就是都先和key xor，然后再结果4和parts3....依次类推结果四和iv xor,就得出结果啦

```
b'=\x17u\xf5\x17og\xd5' b'_\xbc\xa6\xbf\xe8\x15$\xe3' b'\x17\x065\xe0\x07\rD\xd2' b'4\xab\xec\x85\xc2Cu\x8e'
b'hgame{Bl' b'oCk|cIph' b'ER+is+So' b'.EaSY}\x02\x02'
```

2.Multi Prime RSA

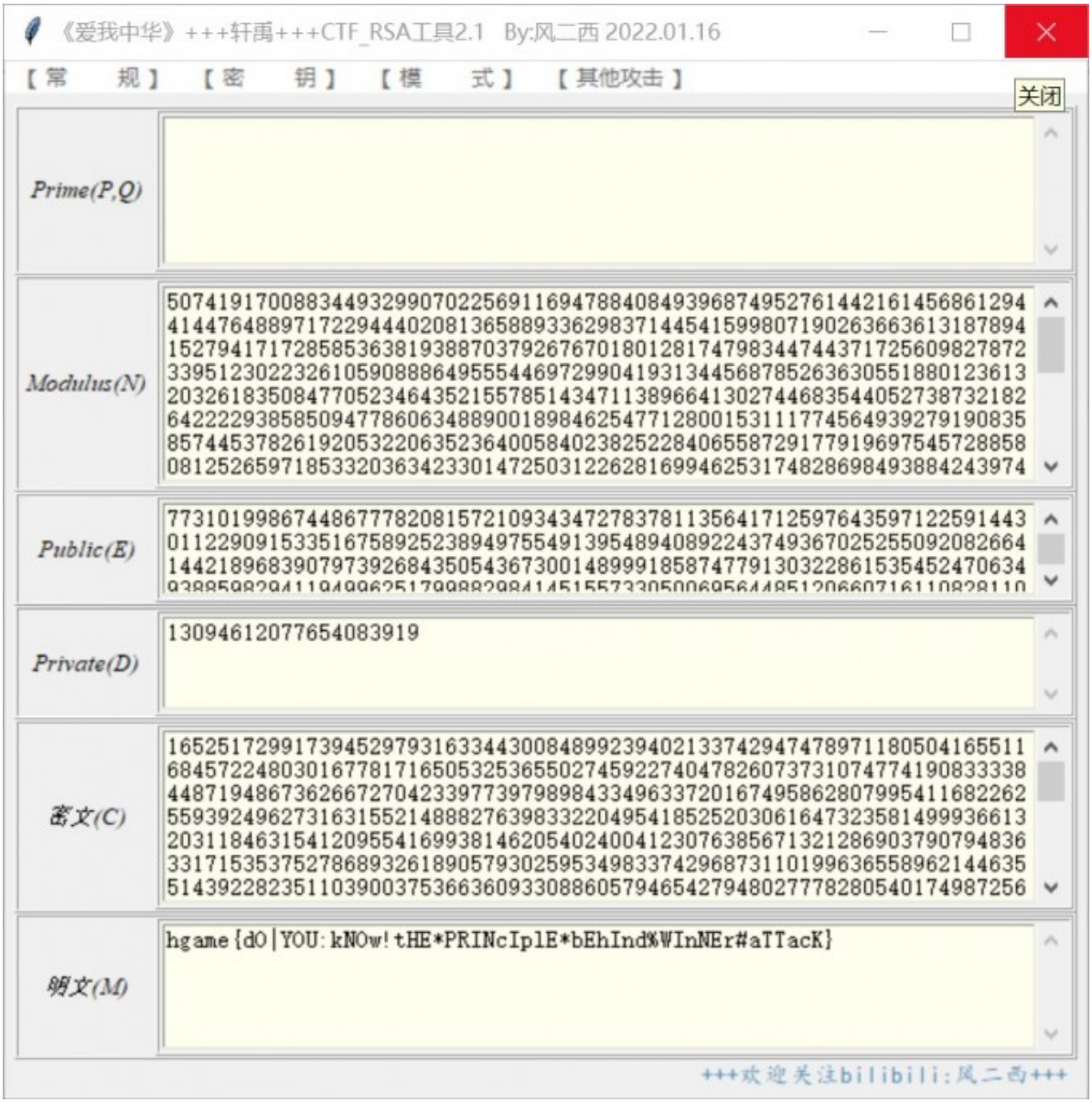
这题一开始看不会，呜呜呜大素数有点多呀，不好用工具，过了两天，再看RSA算法，进一步了解了d的生成，先算出来n的欧拉函数，再算出e模反元素d，得出d，就好做了，套个工具就好了。

```
import libnum
p = 6178993214871947738402745833338056897805628613613782909295231730771190835347 7
q = 9120796935333576368563328437883350631979471450702753292929070174872753419386 1
r = 1054712996073753886223472724792079445096705028356512509452853975300108618093 67
s = 8515323874890377244811383075055797992771626521512444773914651305042671718814 37
n = 1039344372165087100001063920598151812324151066684841845259974758525265148567706103786958426873181721552460289284812493755972556519482026527282644619891466886523804 84
e = 65537
c = 8446773954964666411520394190869778726209960246734415406217975986618865760688024542119231873259151861208878522030809923057991526761346423158242121884493257732867708857 7
# 2,3,5,7
phi=p*(p-1)*q**2*(q-1)*r***6*(r-1)*s***6*(s-1)
d = libnum.invmod(e, phi)
print(d)
```



3.RSA Attcak3

这题就好多了，这条件多淳朴啊，e不就大了点嘛，e大加密系数d就小，也好做，


《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】
关闭
Prime(P,Q)
Modulus(N)
507419170088344932990702256911694788408493968749527614421614568612944144764889717229444020813658893362983714454159980719026366361318789415279417172858536381938870379267670180128174798344744371725609827872339512302232610590888649555446972990419313445687852636305518801236132032618350847705234643521557851434711389664130274468354405273873218264222293858509477860634889001898462547712800153111774564939279190835857445378261920532206352364005840238252284065587291779196975457288580812526597185332036342330147250312262816994625317482869849388424397 4
Public(E)
773101998674486777820815721093434727837811356417125976435971225914430112290915335167589252389497554913954894089224374936702525509208266414421896839079739268435054367300148999185874779130322861535452470634
Private(D)
1309461207765408391 9
密文(C)
165251729917394529793163344300848992394021337429474789711805041655116845722480301677817165053253655027459227404782607373107477419083333844871948673626672704233977397989843349633720167495862807995411682262559392496273163155214888276398332204954185252030616473235814999366132031184631541209554169938146205402400412307638567132128690379079483633171535375278689326189057930259534983374296873110199636558962144635514392282351103900375366360933088605794654279480277782805401749872569 1
明文(M)
hgame{dO|YOU:kNOw!tHE*PRINcIplE*bEhInd%WInNEr#aTTacK}
+++欢迎关注bilibili:风二西+++