

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\r0\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 = 61789932148719477384027458333380568978056286156137829892952317507711908353477
q = 9120796935355576368563328457883506519794714507027532929298701748727534195861
r = 105471299607375388622347272479207944509670502835651250945203597530010861809367
s = 85153238748903772468138507505579799277162652151244477391465130504267171881437
n = 10193443721650871000010639205981518123243106468484184525097475852526514856778610578495862487518172155244020978481269375397255651948202632728764461989146688652580486
e = 65537
c = 844677395496464611520396190869787261209960246734615406217979986418865769680024542719251875259151861208878572030009925057991526761346425130242121884493257732067708857
# 2, 3, 5, 7
phi=(p-1)*(q-1)*(r-1)*(s-1)
d = libnum.invert(e, phi)
print(d)
```

《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)	10393443721650871000010639205981518123241510646848418452509747585252 65148567706103784958424873181721352440209284812493753972556519482026 32728264461909146688652380484124827721035317338340794459845384811381 58669085953356194585494869587644901038084753295980858421849630650684 99489886467911087295087163762599284622055185456905774507245781667293 19920531769202982949596148734794481387441542377198066077898621114584 17124126311563691291464701191351363781582034595765962461691914194885 60832734046076107673091995860021863239882608638458149930255944184863
Public(E)	65537
Private(D)	47135806383402839291135727677523029992063136769401817789263273834456 76601878001402874135904627133326388882671737177452608523707953342065 97772755511566129504696952785949972151309413327390669487960093584449 21850001305425804285775331787807446516650306074627538711431087036322
密文(C)	84467739549646641152039419086978726120996024673441540621797598641886 57606800245421192318732591318612088785220300099230579915267613464231 30242121884493257732067700857897379859545356609151834223804262174935 1917182712118092217306016028271224923808603058097137610472498780104 95006891341226098343215866092237611405380794608302138246743616010463 67637227094018381901291488659642720549583856812747877519600804325570 42177057599928938917502164634737187923402364765750717851904723674607
明文(M)	hgame {EulEr:fUNcTIon;iS. So*IMpORTaNt*In&RsA}

+++欢迎关注bilibili:风二西+++

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，

【常 规】 【密 钥】 【模 式】 【其他攻击】

关闭

$Prime(P,Q)$	
$Modulus(N)$	50741917008834493299070225691169478840849396874952761442161456861294 41447648897172294440208136588933629837144541599807190263663613187894 15279417172858536381938870379267670180128174798344744371725609827872 33951230223261059088864955544697299041931344568785263630551880123613 20326183508477052346435215578514347113896641302744683544052738732182 6422293858509477860634889001898462547712800153111774564939279190835 85744537826192053220635236400584023825228406558729177919697545728858 08125265971853320363423301472503122628169946253174828698493884243974
$Public(E)$	77310199867448677782081572109343472783781135641712597643597122591443 01122909153351675892523894975549139548940892243749367025255092082664 14421896839079739268435054367300148999185874779130322861535452470634 Q3R85Q82QA11QAQ862E17Q8882Q8A1A51E573305006Q56AA8E120660716110828110
$Private(D)$	13094612077654083919
密文(C)	16525172991739452979316334430084899239402133742947478971180504165511 68457224803016778171650532536550274592274047826073731074774190833338 44871948673626672704233977397989843349633720167495862807995411682262 55939249627316315521488827639833220495418525203061647323581499936613 20311846315412095541699381462054024004123076385671321286903790794836 33171535375278689326189057930259534983374296873110199636558962144635 51439228235110390037536636093308860579465427948027778280540174987256
明文(M)	hgame {d0 YOU: kN0w! tHE*PRINcIplE*bEhInd%WInNEr#aTTacK}

+++欢迎关注bilibili:风二西+++