Power Rsa

Challenge:
Something's not quite secure.
nc 34.92.214.217 8887
Flag format : shell{}
A python script was also provided

The netcat connection provided us with a public key

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA8a8ztJkOY8EW8YoQTj4x
Mz+hZHUVSF3hrJd99FTvAM/z4riW1lG5jTqOq1f0sF6J/kR1x8IoSma7CNM1tPUj
H5RZk1YswRecjIT254A2G1yirlLrH3uko0BBrZUM+WFuH92KW5bXpfcwV5HqQCJ1
I8adHlRLfdGOGy7jdqMvAEM9k5VzRGeTp9ll+RN2Rpb3FVHq2+OZlWpwJDZ107xk
WkefEPrc/9lo/Yc2LP/02j0eU3T+1o5RPTngO8UjGIAFIMJzP4zXJ2bEKX9TQI8v
hNHybBm6FGXzWhrnZywHt8TOnvx2tgwhIXlpEzzXMrdPS/ZLtpdvGx4LoUtTP368
AeOHwjqjnmwsZqiX5N2FJrWbbnALgXFT+c2uxpsq33sBJ2Mrh+PuGzY2JFubumoa
qeRMFFA2PmnrjzQUaHF+5Tj6ZbE6qha9Qhfx9ltQA7sZyQ+SHAwxfc1J2ArWaZCv
9uEmvrqZhSCdUOmo7DEY7YlTZGhQtoGFFCvmVmLiGF8c7jhdAQBPJskVmOjCRMYM
0jcMs9B1fHc9pnRI2E/43Wv1d2D+VSJIFDR/FsMSb8dWedUsC3tp9gyL4JSq33VD
n/xuwR9UyT5YUPWHNBUPremq18AVssgbkI2ko1asrkj6Kz984MHWb8rDU70bm0Ig
h8vS1kZS3FcJ6dIT+rTLx2ECAwEAAQ==
-----END PUBLIC KEY-----
```

and the encrypted flag in hex format

```
0xda59c6c774c32574d15113388407f0b09e8bb6c139ed8a41157eaa919bef24e9062069f742f4ad
dd248db2a2a942c08ff80203c953ee3d9209243a450c870142c052ed34276b119755c8c174a25e99
0278ca252430b7d9855dbe843fed7921f63213a2f501bc677025c0344051a2b88f5ba18ff974991d
4a61434cdffb30b2c88393d57cb2e28b089c54d470af1521d24a871a48997b3844250d5560e42fb9
09eb1524c8f09ea73eae541547e22e2236fdf03096530485db3aa7abf5734b1d51b6a71937b50324
3a223b9d83477fe229c4b4600c14a33795dd104c4326d16f3af319e1b1f22be71d41602adcb18316
3c1dec55707f8bb62fd0e3999a58873744edef3384dc6dc83ef295fc28582a6dcab31895a5300f2f
dea40805bdd81634fccf2e09fb3355466eeb95b42870ae25e9e6bcfbfe630590690f428fec1b3df7
f3d0ea1134097ab84e9eacbe365c7507056f7224471e3ce88d3dad990a226b31580021b96768c4fb
cb489a6d723c47b663865c9862d2647507ba3a2069ab41c13eecdcbb554fe578405726f90b79a904
e6e7f9b94a0742444090c70d23fbaf7fdc21e51fc2a89931466f08b5508a7a851193e4b92f8c1bb3
5c02524f48d13afd15823a704447441174815fa9884710565be73e5142ff3f185b072442d36511d4
b6ba34d48e4eaf862728c4d9f684d2a8dd77e71f73294ffc699824f2941c61c295
```

after reading the python script, i began the challenge by recovering the private key from the public key provided. This was done using the RsaCtfTool
`python3 RsaCtfTool.py --publickey '*.pub' --private`

After a few seconds i got the private key as

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEA8a8ztJkOY8EW8YoQTj4xMz+hZHUVSF3hrJd99FTvAM/z4riW
1lG5jTqOq1f0sF6J/kR1x8IoSma7CNM1tPUjH5RZk1YswRecjIT254A2G1yirlLr
H3uko0BBrZUM+WFuH92KW5bXpfcwV5HqQCJ1I8adHlRLfdGOGy7jdqMvAEM9k5Vz
RGeTp9ll+RN2Rpb3FVHq2+OZlWpwJDZ107xkWkefEPrc/9lo/Yc2LP/02j0eU3T+
1o5RPTngO8UjGIAFIMJzP4zXJ2bEKX9TQI8vhNHybBm6FGXzWhrnZywHt8TOnvx2
tgwhIXlpEzzXMrdPS/ZLtpdvGx4LoUtTP368AeOHwjqjnmwsZqiX5N2FJrWbbnAL
gXFT+c2uxpsq33sBJ2Mrh+PuGzY2JFubumoaqeRMFFA2PmnrjzQUaHF+5Tj6ZbE6
qha9Qhfx9ltQA7sZyQ+SHAwxfc1J2ArWaZCv9uEmvrqZhSCdUOmo7DEY7YlTZGhQ
toGFFCvmVmLiGF8c7jhdAQBPJskVmOjCRMYM0jcMs9B1fHc9pnRI2E/43Wv1d2D+
VSJIFDR/FsMSb8dWedUsC3tp9gyL4JSq33VDn/xuwR9UyT5YUPWHNBUPremq18AV
ssgbkI2ko1asrkj6Kz984MHWb8rDU70bm0Igh8vS1kZS3FcJ6dIT+rTLx2ECAwEA
AQKCAgEAuYjdcav6DvxhZ6WspNQ7ovMbK+pyHy7rGzrlF5fILuB1grxgF0F/53pn
ogQQtQCugML/hA16Lru0o6640SVLBGg3Z9NE4isFJB7DCK81WkYAIUFIfM/HcQfY
I7CD2EJCbzX8jBk9jYw40VET+o45TPChF3JwzbL8m8OgHShi4Zm9ALo/VekJwlYz
YUXei4xDPFu5p3qPIdQnKLWiOJyskV3gMAHVfJfjcJXHMj6AMrWuvTTYmc+BcDYo
/Nl2+sz0otSD8uplFTtgJdc4Cxygxx8BMpmBbz1g1vBGar6zYhE06Xo4i8K+AFub
HYicT7PHrTHzp8WTJscm+HjB/MGHA5JHPLzoIHbAtOoapCH4icEfqz0ZrBxgvPh4
BvmETAWJ+O2R7uW3P6iNrK8BRQnjE/EILSjp2SQsl/hkvq7zVQ65K4y5ySbeR7uQ
```

```
hJv6EOmv4DFHptt6Xoqpdg+CddgD2O0/z2uOEzUXKyNndo3+JsW/PWU5jkthWme6
cAFsjJ9FyHih1NnRk4FjNBmyzPrkW/M2YRSefGikGAXNvJ1CLNj0y6Ovb6x3GLXc
rwcIpcRKlmukShdnzHsesCNAnbiBEaDZja/ra9JPnMsdfI39uBwbaWXhQ5MzrNUy
eNnjX8LW5nFzuFSQB44DhZVkb4P/4kTFNWSsrSmdetSAW9LBHNECggEBAPi9PdbU
FT1xBfg7+VyG3AMaLB3cZtxnBZMEt2JV/GXe5gOh6kq4hNd5wxbGPyj+DUvqvqCk
LS3vCYoFGP6jiwzs/ntxiDDbYjyPg7UsL2Lt5baK6RByxhp6r9LRouX77njKnsBs
FPtZlQcQAA15ggTRF6DvGTV5kBUIJg8wxC+hvZfFlimgSIfNekpsdt/jxvFgjd82
yW3ysIpDmQXSJJYCnlvlJL8CovRCmF9NlLAzB2lpToKkQ//RdT/GA4MhpZJYahu4
OU4pjNHpWmCEmR+JTQlWdqUmqMCJYzfUxYNuMqG89XVmBTISBEGo4ERE0SjCP3rH
KNHz3HnhiAc3Yu0CggEBAPi9PdbUFT1xBfg7+VyG3AMaLB3cZtxnBZMEt2JV/GXe
5gOh6kq4hNd5wxbGPyj+DUvqvqCkLS3vCYoFGP6jiwzs/ntxiDDbYjyPg7UsL2Lt
5baK6RByxhp6r9LRouX77njKnsBsFPtZlQcQAA15ggTRF6DvGTV5kBUIJg8wxC+h
vZfFlimgSIfNekpsdt/jxvFgjd82yW3ysIpDmQXSJJYCnlvlJL8CovRCmF9NlLAz
B2lpToKkQ//RdT/GA4MhpZJYahu4OU4pjNHpWmCEmR+JTQlWdqUmqMCJYzfUxYNu
MqG89XVmBTISBEGo4ERE0SjCP3rHKNHz3HnhiAc3Y8UCggEAduzT8jC4bwXo2sSh
9tErw/fxe91y+JHxIlew7j06TeKCit4RTORn7zXyRqNGc2z0IoX72oZka3/MScci
Ki07QFTXX2HqwaFCmL3tNOQJS/1+RQapZAncGbDq+5rrjZYkcHA/8rQ6W+p6zEOk
Is0jkvX9nB51KRIUB1o8CCtCwZtNMJFxuDlANF3TyF2PgIBBEAsgCccCC6VrLtAf
C59riqV53WnzZbf2/V4RyA8ptgzP0GBe/ytWr6sPqgwchcfCh/Pp15L/IxXOlFZD
tb3wEBnvUTWbyF5xdIy7eWgrfyli392eZiD+/u+KRXJet4VHk3s8KpGqPKehlEx2
YyziCQKCAQEApFdEGEAfmGyoaQ4W/w8LJfGQ3FnWjCB1CmG/V/U/wX63sga0aZHo
EwWb49wvtsHDvzjlofVW9FZOkyYzEWq0YGHk8WJdfQo1qZWYi4cZ997+OtEkk32B
bdVJfZyMaC8/rAcTREckxby2PehQYJa7VLthRS80FKSwkXTE0JyDwoS2YyRkxjPk
N/WGqs1m7R3tP2Vv1t63zzDdezyWScZB7erk/gozcRAo4gFt8umrJ49PglHVUXN+
ifK16ODHSUhdwIcx9AaPthi1tarbz5FMKg3pHBZIZW1ZaXxcVXL63I9eXIYgFuTE
4gQNU+Rj6DcfijJtBo23ZqAcN1rPKRVrkQKCAQB7N9GYpFGh/eoRfIYxY/2Uf+2O
ys9mEdlHpLTqyWjh3wKI6RjNT42oXrAMd4n0TnFA3cRbbcXJt5jfoVcMXN3FN8Us
jsJHnBVnez2wRBw27rx1r3qQcb6UOmewus+ChRiAk8eHndY+4bWs+uOU5axCYtZf
IRvlKBIKayXRAaOOHSiV2ZUNglzRfq0r+niEPd7+rqUYDhpM+8bcMhQZZunTysdV
0YLLqGrL9lKXgbDEUirIXaW03TljdyqsoOeqcKrofsLI/aEgyxnn++R5Syqq4aT5
9X+DlrTHrFqhlUCoN8YeV629thfoNfZBtgbMfCn7TUMAYEmN7iKM+ASRzAeG
-----END RSA PRIVATE KEY-----
```

i Used the Rsactftool to recover the values p,n,d,q,e from the private key

n:

```
985986258267031520013329314658188183291143245108756305222576271782834096595591056712152356203358708587278513447229834134580222578808711634843070310400903919482066953497904496339649434238616426213759937474638889604855498428428666704902099851027632260969911127732536270836797306775342428802743431072642521002593708649114725829965035508355122071694118204114014957673395287202592742031825755466393248047459504810017042028089824147253766745557379166908133225392710931899536522647813945557057628654982137455117745614321870334640214490738165959119780293316906675872973924155403033256142909216474580282528354533997876100860952846104660871910630495786775183925097778804003115905861572099236342210895869493101423271790652238189239890983023153254921383195720656654077747972231097815145069268241490574489758400005158471966825511578482285876999148359591014851496241035978675806056710623466964413616424897034646537055479318659923124042288334613157940559756581037495240541473524687981132094786218129263598244721756070811434305948199915898911024086426638979037908091210726656996816166962250545994737462723972580989226184481021282630563629912451643420867192175979393898026849401255642176831462465369783581346482380743874156563309438510363102476486497
```

e: 65537

d:

```
756915248480592990271001284003968837291311897167502913957810623154342832809264715416407482688361993800976079009469157653613463816812565284657364700651233304744835291475549279267346730640386819952705742012703620472555731593339253407850978006394116402668068400252554012574120104691613179356620302435200236113363322639815844045827103795731488266917966659553842967110276489531862054173416323348180580473865681164788858224746740660580805632478406141054901669327748900541641851029710963500329986957913946587491476564416247591529728721844574325484463224393348669756705236708767291852690936502892299137804355477973772746851583671323058306076325686966948121935729896362846396381846798830872052635316447038339039983524805525552397597874493528269162562806730364136116595621339115456220168963029129744030152906624
```

32829474539567439179855784057830628476159912412900033620940175288223009478941935
29115477135327983277807958255056381277804695063295520050459556304415835744560987
90388700491153060170635833162755562714770849419653770614823195111052014495053373
69262482393220128731619761664192402274410952542040385378657161371214402036443821
00745428576478831178318979081447745880415552889251161454207079281233860456543571
68824795722071702003119477811528 1
p:
31400418122487342445730822042567342665263376561154465849495129353599604576018172
12736819807591108333576520823822022521150685567068050806518089732856847560695933
65926383649327050754687969771357738168113024189683446751164086896934091272726880
75843569916042525045265302774889467280714573831747131238390535769565979999643135
70127777052808328055085975476073202530102507792227744445724652551437071329207242
99784481543039700322742954566661676020761977673906914732368709997234880278240431
12276838950695028166647622269207549198526071555671396171440709342216244068943168
33024452234638160774543884359269825969499267648860608177 3
q:
31400418122487342445730822042567342665263376561154465849495129353599604576018172
12736819807591108333576520823822022521150685567068050806518089732856847560695933
65926383649327050754687969771357738168113024189683446751164086896934091272726880
75843569916042525045265302774889467280714573831747131238390535769565979999643135
70127777052808328055085975476073202530102507792227744445724652551437071329207242
99784481543039700322742954566661676020761977673906914732368709997234880278240431
12276838950695028166647622269207549198526071555671396171440709342216244068943168
33024452234638160774543884359269825969499267648860608198 9

i used p and q to decode the flag which was formatted in utf-16 which i decoded to

Flag: shell{entr0py_1s_th3_k3y_L9mlIsTtB557I/Nh4gqL87MxcugLIfZI}