PUNY FACTORS

Challenge:
They are puny but in prime shape.
nc 34.92.214.217 8889
Flag format : shellctf{}
The netcat connection reveals the public key

```
"-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAgum2mNSsi6EomIAaLe8a
V9W4CMBQhDKaMr3IBF2pORy6F6XDfSzzY6XCJYqksXP4X6MdsV1jh92TckWAMDPl
8p4VejfXYD9m1m7PfRoEn/WNSDUyLjTc3g5x5PqEJWbSgbJ+If48kpEO+mCkAW+f
FYtq8n/xNDv5hw5merWgfeZ8hBsyQI9dUymE92gQWzNnAO4q/zYTpulqRxmggrHE
0krM1e2e9ZK2j4Oqra3nul27xDWhGORB0/ozbwj9ueWRhKaJF93QClNCAKkqMZ2A
xTmKBhprmjblPvWt7hIiODNMe9F6a6/holOcWe6p0guZ7+u+/hUMdalbpWkC9blL
4+vfoiTz7GLn8KPbli3c/wqffn0zTQMMtGflRZk4A+vm3d941GJqc+r/bbxy0laN
awntrHXIzjm3TsQ4uIvyG3nwcbzH8BVHLfpl1zuWVEy6UilkGGHAMB8QQLxwZRC5
FBlSZiX+2jXh3AqYhc8IJeNc/ov/3RmdlzZt6jQo3YyH144Xl9q/XufrwLbVRw8r
QigraNUQ1HXRvG0RgOCWRZl9Z5n7jyD+9N3SNqgmxMfYDvCkNbmZQvDsuyqrl8HM
jeE5EBlHJm/yskI9q+FbA4g4IVqmMdTGD+jwNpL2N5ktE+MMsspHhBce9jE43yV6
XWDXTSI/b5e6auV9z7XrSYkCAwEAAQ==
-----END PUBLIC KEY-----
"
```

 and the encrypted flag
 c =

```
21211558061350742464593109264579163290314727904974049724942506647661069745689064
```

```
21211558061350742464593109264579163290314727904974049724942506647661069745689064
34306267480202365585572342766700123162375139092716843615987041945569932625857101
53604992505184254630729965355726753897370357531531186983178350938959876192854093
84138834802738183683449610423714619460280425030685621435462176706692828285189870
62655352731939918113571425659093322615771864748508598576226945001877903957282628
72025310522896876451380974911185147747865515046069732547783629203831143343490433
32237884250728729384748362739830160778191086248616929932197303460255402659412475
19878727022058186978018179281427388156945989729879076319167605205025688588319711
44780767870322288072909372392706132679072831792852574481247918270109435897408919
48413036884447762560179656864607266565252513650891517008459414582885936004593284
94671054834008921283729564687086208415826825345663603051891151311816305832717902
29467949676085321827930184537521364736397693243462709841112359401859689117403139
12697566505306624332522574668368966049846568476559941604382869322395531297631116
18250404386108049031140996541804071164058072957002895819671187473321064555346721
47374965947669181982817129289680026846821518274365087976503227717518215311728143
815674804220080971433197879927960
```

using the rsactftool i recovered the value of n and e from the public key
RsaCtfTool.py --dumpkey --key '*.pub'
The value of n is therefore:

```
53407820913005177213886890439438317161237967464321515512085725915151221518769621
62816931281656882754980492016294849141352976479189845850739974634173910176775816
24808037260617353325934848594182129666199193944074969600485152222827449014215447
57847188079660311864702916135909106510840660895827827581319062884030791893240226
08605271762244897193878837332503961691864355449430056475463307268849609255817135
43981539062843029208057443938923630291991874352293827369233534768706318739264433
57629880504682765916461874692869962871171585465143640856085118351894255863198906
25790456471327871801792261390303340176842019899232115562858784004712576223506142
57933805478690247011109736939123686891473607167746038741230140594628700740877693
58043211377467679299060368277581742195649827870642334150728000377436840878025524
78089245345213860241259109934723959641377722580174401756189535467301706119017161
93226243872985551461621623631952665733750542017678338436848262409657294684350917
96879394201098901777128225708131850334397247368246442134738248348361061112320256
00405735607969346051635437508988251740623161578157903972486243295929062017007651
14040226180380486682498397818641564042670668460644404687564725489292554171505159
750643627096667997904648228522377
```

Working with C, n and e we can decrypt c by factorizing n and finding the values p and q which will be used to decrypt the key.
i opted for factordb but it had no clear results so i switched to X-RSA tool

which after some factorisation in the background it coughed the decrypted string
Here are the results:

```
PlainText in Decimal :
14693114728825226011632822880380453528800192955518694755520988729390788046278123
768934975357
PlainText in hex :
7368656c6c6374667b7072316d33735f6172335f73757033725f696e743372652474696e477d
PlainText in ascii : shellctf{pr1m3s_ar3_sup3r_int3re$tinG}
Flag: shellctf{pr1m3s_ar3_sup3r_int3re$tinG}
```