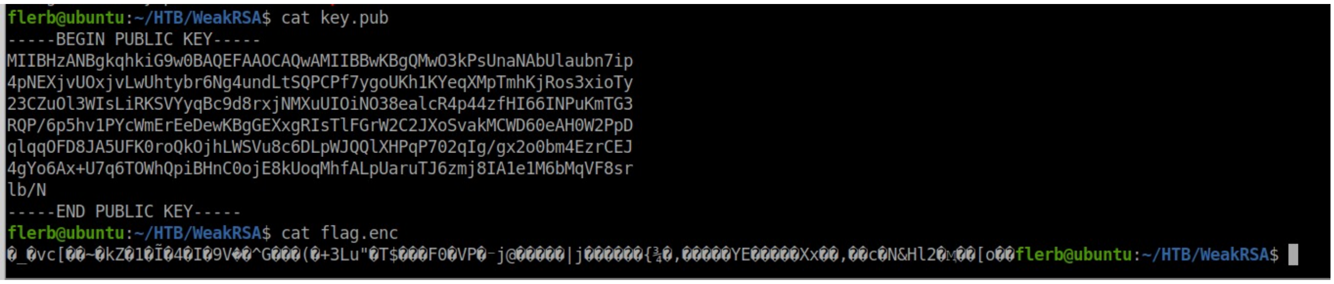
Weak RSA



```
flerb@ubuntu:~/HTB/WeakRSA$ cat key.pub
-----BEGIN PUBLIC KEY-----
MIIBHzANBgkqhkiG9w0BAQEFAAOCAQwAMIIBBwKBgQMwO3kPsUnaNAbUlaubn7ip
4pNEXjvUOxjvLwUhtybr6Ng4undLtSQPCPf7ygoUKh1KYeqXMpTmhKjRos3xioTy
23CZuOl3WIsLiRKSVYyqBc9d8rxjNMXuUIOiNO38ealcR4p44zfHI66INPuKmTG3
RQP/6p5hv1PYcWmErEeDewKBgGEXxgRIsTlFGrW2C2JXoSvakMCWD60eAH0W2PpD
qlqqOFD8JA5UFK0roQkOjhLWSVu8c6DLpWJQQlXHPqP702qIg/gx2o0bm4EzrCEJ
4gYo6Ax+U7q6TOWhQpiBHnC0ojE8kUoqMhfALpUaruTJ6zmj8IA1e1M6bMqVF8sr
lb/N
-----END PUBLIC KEY-----
flerb@ubuntu:~/HTB/WeakRSA$ cat flag.enc
�_�vc[��~�kZ�1�Ĩ�4�I�9V��^G���(�+3Lu"�T$���F0�VP�-j@�����|j������{¾�,�����YE�����Xx��,��c�N&Hl2�M��[o��flerb@ubuntu:~/HTB/WeakRSA$ 
```

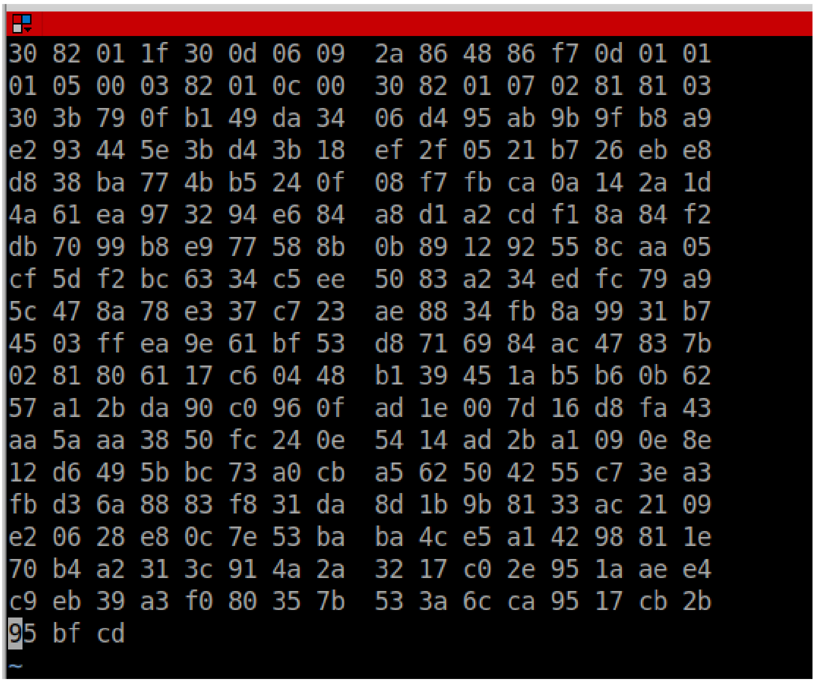
https://security.stackexchange.com/questions/177829/how-weak-rsa-key-is-decrypted

https://crypto.stackexchange.com/questions/6713/low-public-exponent-attack-for-rsa

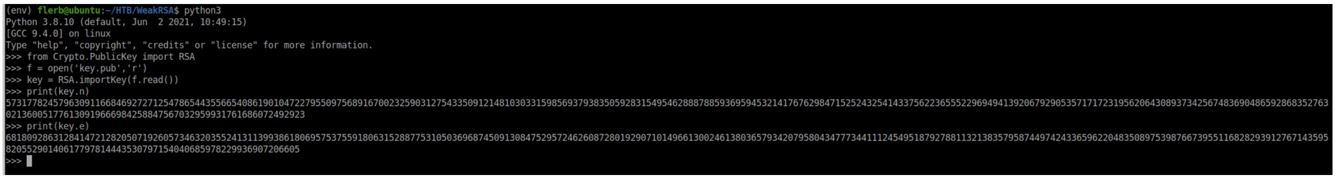
https://crypto.stackexchange.com/questions/18031/how-to-find-modulus-from-a-rsa-public-key

https://base64.guru/converter/decode/hex + vim to break it into hex.

The public key is only 388 characters long.



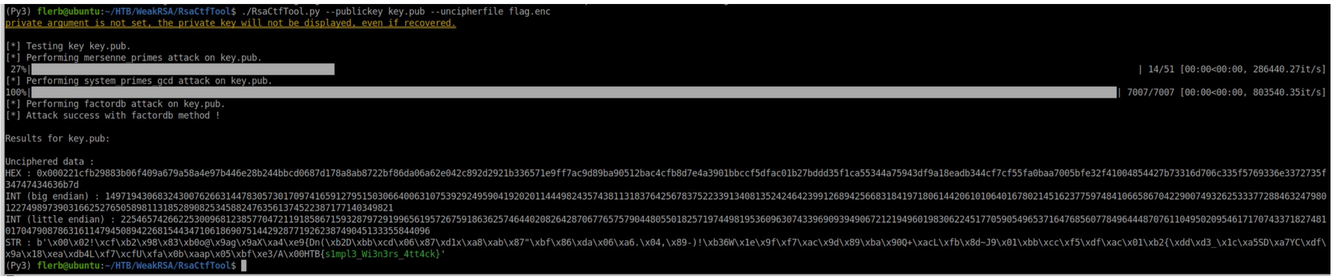
```
30 82 01 1f 30 0d 06 09  2a 86 48 86 f7 0d 01 01
01 05 00 03 82 01 0c 00  30 82 01 07 02 81 81 03
30 3b 79 0f b1 49 da 34  06 d4 95 ab 9b 9f b8 a9
e2 93 44 5e 3b d4 3b 18  ef 2f 05 21 b7 26 eb e8
d8 38 ba 77 4b b5 24 0f  08 f7 fb ca 0a 14 2a 1d
4a 61 ea 97 32 94 e6 84  a8 d1 a2 cd f1 8a 84 f2
db 70 99 b8 e9 77 58 8b  0b 89 12 92 55 8c aa 05
cf 5d f2 bc 63 34 c5 ee  50 83 a2 34 ed fc 79 a9
5c 47 8a 78 e3 37 c7 23  ae 88 34 fb 8a 99 31 b7
45 03 ff ea 9e 61 bf 53  d8 71 69 84 ac 47 83 7b
02 81 80 61 17 c6 04 48  b1 39 45 1a b5 b6 0b 62
57 a1 2b da 90 c0 96 0f  ad 1e 00 7d 16 d8 fa 43
aa 5a aa 38 50 fc 24 0e  54 14 ad 2b a1 09 0e 8e
12 d6 49 5b bc 73 a0 cb  a5 62 50 42 55 c7 3e a3
fb d3 6a 88 83 f8 31 da  8d 1b 9b 81 33 ac 21 09
e2 06 28 e8 0c 7e 53 ba  ba 4c e5 a1 42 98 81 1e
70 b4 a2 31 3c 91 4a 2a  32 17 c0 2e 95 1a ae e4
c9 eb 39 a3 f0 80 35 7b  53 3a 6c ca 95 17 cb 2b
95 bf cd
~
```



```
(env) flerb@ubuntu:~/HTB/WeakRSA$ python3
Python 3.8.10 (default, Jun  2 2021, 10:49:15)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from Crypto.PublicKey import RSA
>>> f = open('key.pub','r')
>>> key = RSA.importKey(f.read())
>>> print(key.n)
573177824579630911668469272712547865443556654086190104722795509756891670023259031275433509121481030331598569379383505928315495462888788593695945321417676298471525243254143375622365552296949413920679290535717172319562064308937342567483690486592868352763
021360051776130919666984258847567032959931761686072492923
>>> print(key.e)
681809286312841472128205071926057346320355241311399386180695753755918063152887753105036968745091308475295724626087280192907101496613002461380365793420795804347773441112454951879278811321383579587449742433659622048350897539876673955116828293912767143595
820552901406177978144435307971540406859782299369072066O5
>>> █
```

As riveting as finding primes might be, others have already done the work:

https://github.com/Ganapati/RsaCtfTool

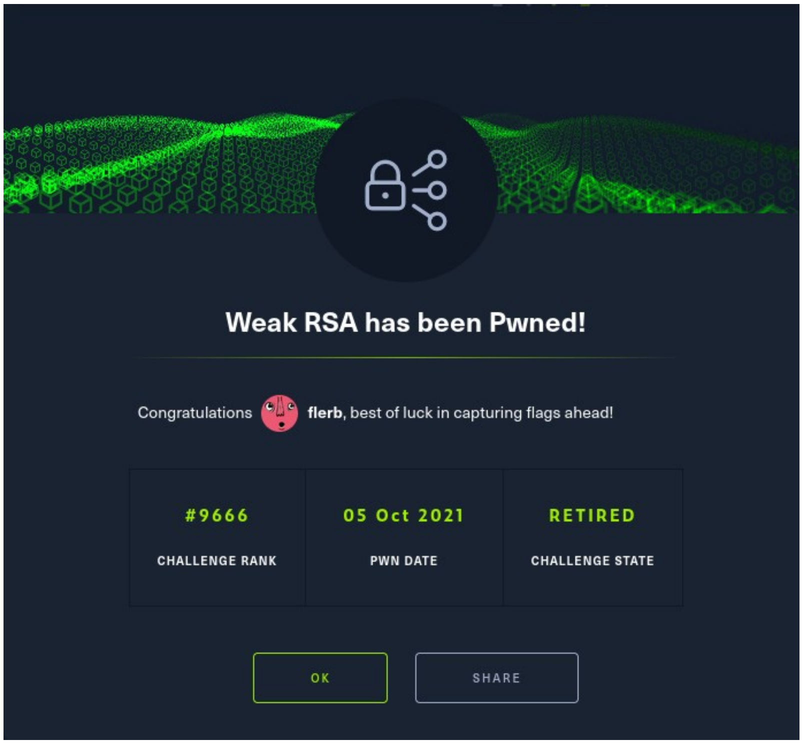


```
(Py3) flerb@ubuntu:~/HTB/WeakRSA/RsaCtfTool$ ./RsaCtfTool.py --publickey key.pub --uncipherfile flag.enc
private argument is not set, the private key will not be displayed, even if recovered.

[*] Testing key key.pub.
[*] Performing mersenne_primes attack on key.pub.
 27%|█████████████                                                     | 14/51 [00:00<00:00, 286440.27it/s]
[*] Performing system_primes_gcd attack on key.pub.
100%|██████████████████████████████████████████████████████████████████| 7007/7007 [00:00<00:00, 803540.35it/s]
[*] Performing factordb attack on key.pub.
[*] Attack success with factordb method !

Results for key.pub:

Unciphered data :
HEX : 0x000221cfb29883b06f409a679a58a4e97b446e28b244bbcd0687d178a8ab8722bf86da06a62e042c892d2921b336571e9ff7ac9d89ba90512bac4cfb8d7e4a3901bbccf5dfac01b27bddd35f1ca55344a75943df9a18eadb344cf7cf55fa0baa7005bfe32f41004854427b73316d706c335f5769336e3372735f
34747434636b7d
INT (big endian) : 14971943068324300762663144783057301709741659127951503066400631075392924959041920201144498243574381131837642567837522339134081352424642399126894256683184197180614420610106401678021451623775974841066586704229007493262533377288463247980
1227498973903166252765058981131852890825345882476356137452238717714O349821
INT (little endian) : 22546574266225300968123857704721191858671593287972919965619572675918636257464402082642870677657579044805501825719744981953609630743396909394906721219496019830622451770590549653716476856077849644487076110495020954617170743371827481
017047908786316114794508942268154434710618690751442928771926238749045133355844096
STR : b'\x00\x02!\xcf\xb2\x98\x83\xb0o@\x9ag\x9aX\xa4\xe9{Dn(\xb2D\xbb\xcd\x06\x87\xd1x\xa8\xab\x87"\xbf\x86\xda\x06\xa6.\x04,\x89-)!\xb36W\x1e\x9f\xf7\xac\x9d\x89\xba\x90Q+\xacL\xfb\x8d~J9\x01\xbb\xcc\xf5\xdf\xac\x01\xb2{\xdd\xd3_\x1c\xa5SD\xa7YC\xdf\
x9a\x18\xea\xdb4L\xf7\xcfU\xfa\x0b\xaap\x05\xbf\xe3/A\x00HTB{s1mpl3_Wi3n3rs_4tt4ck}'
(Py3) flerb@ubuntu:~/HTB/WeakRSA/RsaCtfTool$ █
```



Weak RSA has been Pwned!

Congratulations flerb, best of luck in capturing flags ahead!

#9666	05 Oct 2021	RETIRED
CHALLENGE RANK	PWN DATE	CHALLENGE STATE