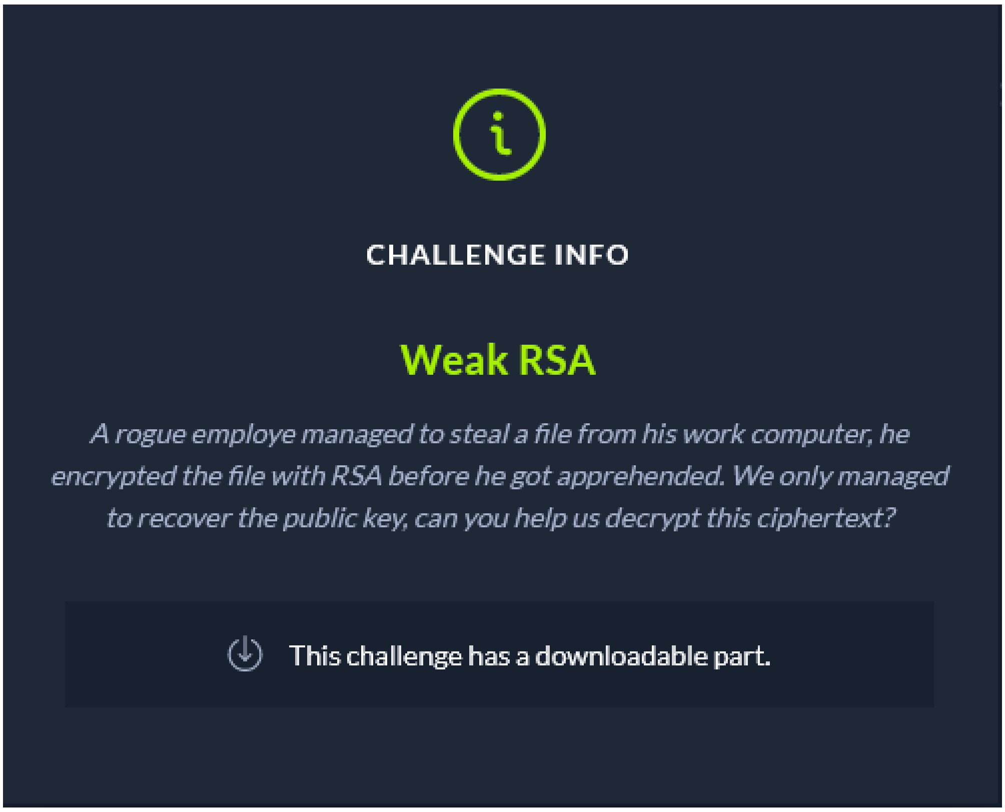
WEAK_RSA



CHALLENGE INFO

Weak RSA

A rogue employe managed to steal a file from his work computer, he encrypted the file with RSA before he got apprehended. We only managed to recover the public key, can you help us decrypt this ciphertext?

This challenge has a downloadable part.

MATERIAL:
flag.enc
pubkey.pem

FLAG:
HTB{b16_e_5m4ll_d_3qu4l5_w31n3r_4774ck}

SOLVER:
M1gnus

RSArmageddon

for this challenge I used my tool: RSArmageddon, it’s still a beta version and I have to discover and fix some bugs, but is really a valid tool to manage and attack RSA cryptosystem.

Foothold

The challenge provide an encrypted file and a RSA public key.
First let’s see what’s the values contained in the public key files using the flag:

```
C:\Users\Vittorio\RSArmageddon>python rsarmageddon.py pem --key %USERPROFILE%\Downloads\pubkey.pem --dumpvalues

______ _____  ___                                       _     _
| ___ \/  ___|/ _ \                                    | |   | |
| |_/ /\ `--./ /_\ \_ __ _ __ ___   __ _  __ _  ___  __| | __| | ___  _ __
|    /  `--. \  _  | '__| '_ ` _ \ / _` |/ _` |/ _ \/ _` |/ _` |/ _ \| '_ \
| |\ \ /\__/ / | | | |  | | | | | | (_| | (_| |  __/ (_| | (_| | (_) | | | |
\_| \_|\____/\_| |_/_|  |_| |_| |_|\__,_|\__, |\___|\__,_|\__,_|\___/|_| |_|
                                          __/ |
                                         |___/

Written by M1gnus && AquilaIrreale -- PGIATASTI

[*]n:
6099835333221774024685803141390900069398779553342450682614696778061694340400690697709285357010863649419834280909337
9574585389674645847262045749199349951179853674766819718685785088799081274685506241562671564522308941518609358972176
3366994454776521466115355580659841153428179997121984448771910872629371808169183
[*]e:
3878253927872009066766311989610980709123328654421375399194137147903101396537130775865576544095654597521334390092808
4396585678915196286019383025824442414923004683247595985277113450375477800713246546871778993660275533633298479062213
2641288576440161244396963980583318569320681953570111708877198371377792396775817
[*] d: None
[*] p: None
[*] q: None

[#] dp: None
[#] dq: None
[#] pinv: None
[#] qinv: None
```

Is possible to see that the public exponent “e” is really big, so it is reasonable to assume that the private exponent d is small. If “d” is small enough is possible to perform the wiener factorization attack against this public key and then use the recovered prime factors of “n” to obtain the private exponent “d” and decrypt the file “flag.enc”. RSArmageddon will do the dirty work for us.

Recover the flag

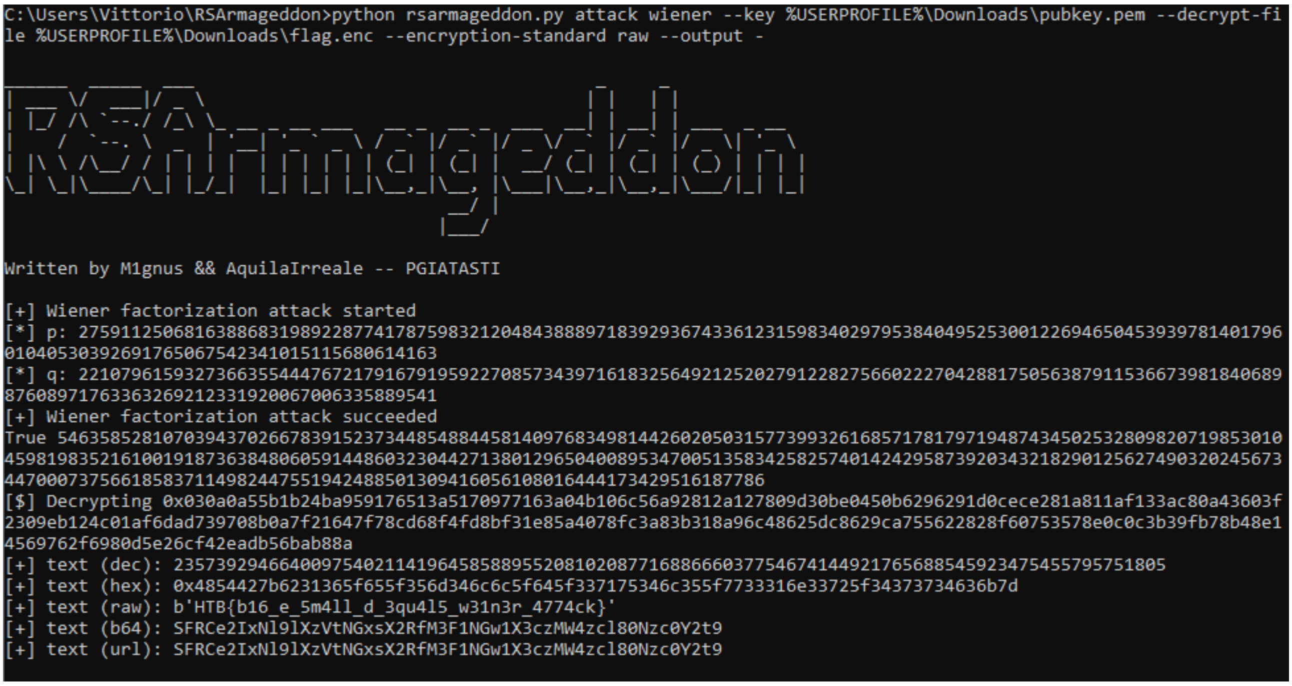
```
C:\Users\Vittorio\RSArmageddon>python rsarmageddon.py attack wiener --key %USERPROFILE%\Downloads\pubkey.pem --
decrypt-file %USERPROFILE%\Downloads\flag.enc --encryption-standard raw --output -

______  _____  ___                             _     _
| ___ \/  ___|/ _ \                           | |   | |
| |_/ /\ `--./ /_\ \_ __ _ __ ___   __ _  __ _  ___  __| | __| | ___  _ __
|    /  `--. \  _  | '__| '_ ` _ \ / _` |/ _` |/ _ \/ _` |/ _` |/ _ \| '_ \
| |\ \ /\__/ / | | | |  | | | | | | (_| | (_| |  __/ (_| | (_| | (_) | | | |
\_| \_|\____/\_| |_/_|  |_| |_| |_|\__,_|\__, |\___|\__,_|\__,_|\___/|_| |_|
                                          __/ |
                                         |___/

Written by M1gnus && AquilaIrreale -- PGIATASTI

[+] Wiener factorization attack started
[*]p:2759112506816388683198922877417875983212048438889718392936743361231598340297953840495253001226946504539397814
0179601040530392691765067542341015115680614163
[*]q:2210796159327366355444767217916791959227085734397161832564921252027912282756602227042881750563879115366739818
4068987608971763363269212331920067006335889541
[+] Wiener factorization attack succeeded
[$]Decrypting
0x030a0a55b1b24ba959176513a5170977163a04b106c56a92812a127809d30be0450b6296291d0cece281a811af133ac80a43603f2309eb12
4c01af6dad739708b0a7f21647f78cd68f4fd8bf31e85a4078fc3a83b318a96c48625dc8629ca755622828f60753578e0c0c3b39fb78b48e14
569762f6980d5e26cf42eadb56bab88a
[+] text (dec): 2357392946640097540211419645858895520810208771688666037754674144921765688545923475455795751805
[+] text (hex): 0x4854427b6231365f655f356d346c6c5f645f337175346c355f7733316e33725f34373734636b7d
[+] text (raw): b'HTB{b16_e_5m4ll_d_3qu4l5_w31n3r_4774ck}'
[+] text (b64): SFRCe2IxNl91XzVtNGxsX2RfM3F1NGw1X3czMW4zcl80Nzc0Y2t9
[+] text (url): SFRCe2IxNl91XzVtNGxsX2RfM3F1NGw1X3czMW4zcl80Nzc0Y2t9
```

Cheese!



```
C:\Users\Vittorio\RSArmageddon>python rsarmageddon.py attack wiener --key %USERPROFILE%\Downloads\pubkey.pem --decrypt-fi
le %USERPROFILE%\Downloads\flag.enc --encryption-standard raw --output -

______  _____  ___                             _     _
| ___ \/  ___|/ _ \                           | |   | |
| |_/ /\ `--./ /_\ \_ __ _ __ ___   __ _  __ _  ___  __| | __| | ___  _ __
|    /  `--. \  _  | '__| '_ ` _ \ / _` |/ _` |/ _ \/ _` |/ _` |/ _ \| '_ \
| |\ \ /\__/ / | | | |  | | | | | | (_| | (_| |  __/ (_| | (_| | (_) | | | |
\_| \_|\____/\_| |_/_|  |_| |_| |_|\__,_|\__, |\___|\__,_|\__,_|\___/|_| |_|
                                          __/ |
                                         |___/

Written by M1gnus && AquilaIrreale -- PGIATASTI

[+] Wiener factorization attack started
[*] p: 275911250681638868319892287741787598321204843888971839293674336123159834029795384049525300122694650453939781401796
01040530392691765067542341015115680614163
[*] q: 221079615932736635544476721791679195922708573439716183256492125202791228275660222704288175056387911536673981840689
87608971763363269212331920067006335889541
[+] Wiener factorization attack succeeded
True 54635852810703943702667839152373448548844581409768349814426020503157739932616857178179719487434502532809820719853010
4598198352161001918736384806059144860323044271380129650400895347005135834258257401424295873920343218290125627490320245673
447000737566185837114982447551942488501309416056108016444173429516187786
[$] Decrypting 0x030a0a55b1b24ba959176513a5170977163a04b106c56a92812a127809d30be0450b6296291d0cece281a811af133ac80a43603f
2309eb124c01af6dad739708b0a7f21647f78cd68f4fd8bf31e85a4078fc3a83b318a96c48625dc8629ca755622828f60753578e0c0c3b39fb78b48e1
4569762f6980d5e26cf42eadb56bab88a
[+] text (dec): 2357392946640097540211419645858895520810208771688666037754674144921765688545923475455795751805
[+] text (hex): 0x4854427b6231365f655f356d346c6c5f645f337175346c355f7733316e33725f34373734636b7d
[+] text (raw): b'HTB{b16_e_5m4ll_d_3qu4l5_w31n3r_4774ck}'
[+] text (b64): SFRCe2IxNl91XzVtNGxsX2RfM3F1NGw1X3czMW4zcl80Nzc0Y2t9
[+] text (url): SFRCe2IxNl91XzVtNGxsX2RfM3F1NGw1X3czMW4zcl80Nzc0Y2t9
```