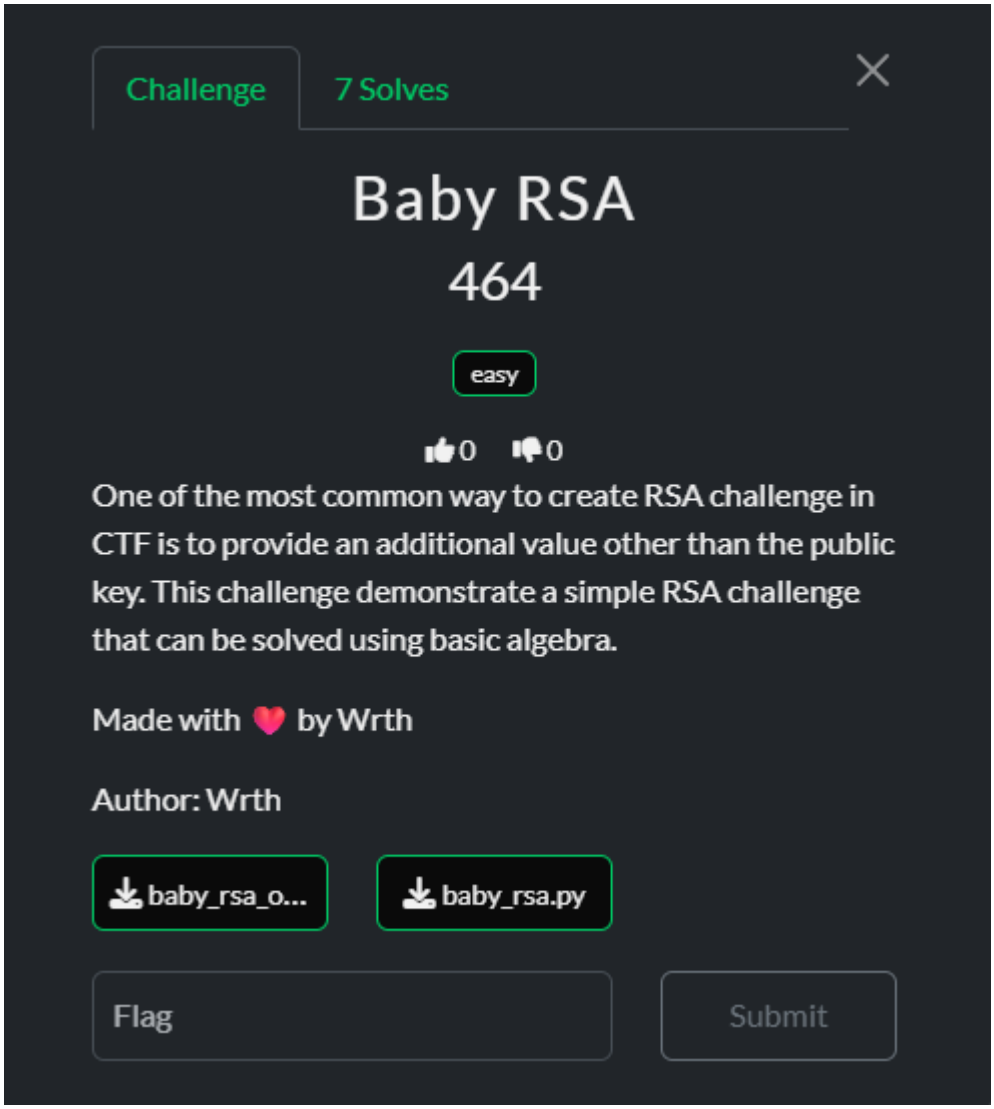
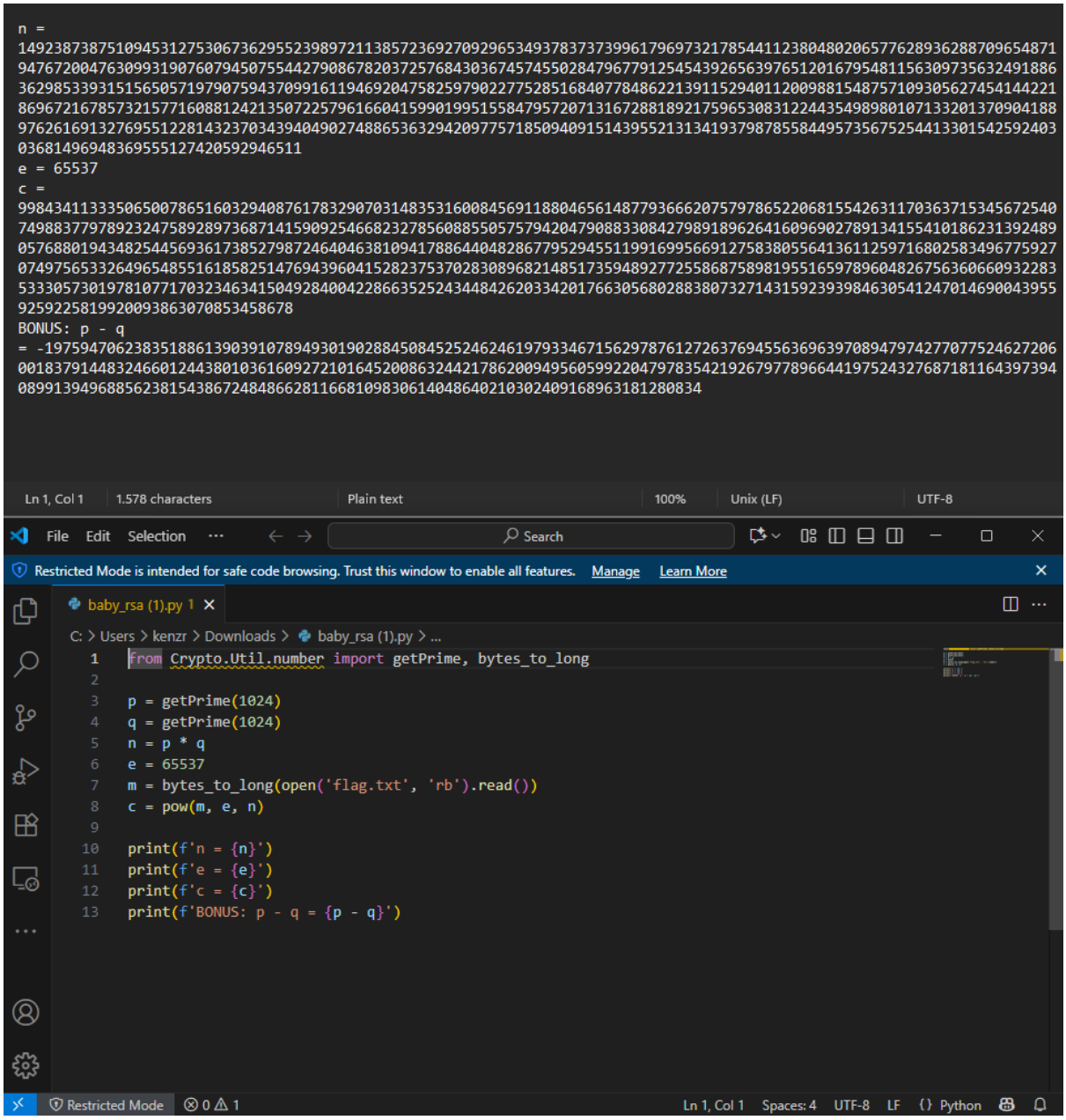
Baby RSA

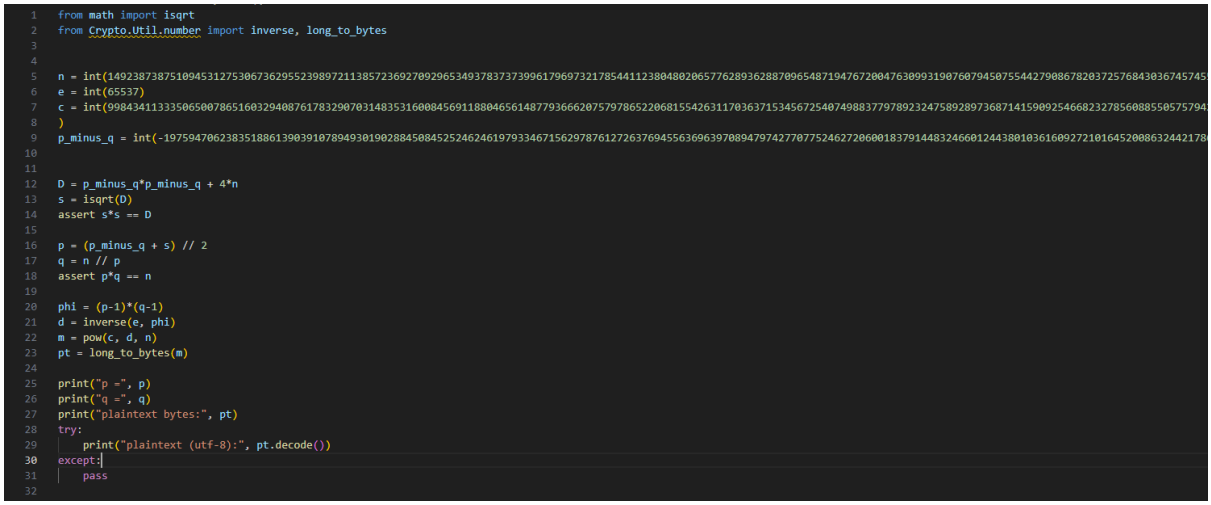
WriteUp by KxnZ



Lets download the files shall we



This is what inside the file. It includes the output and the algorithm of the output, now lets make an algorithm to compile and produce the plain text.



```python
from math import isqrt
from Crypto.Util.number import inverse, long_to_bytes


n = int(14923873875109453127530673629552398972113857236927092965349378373739961796973217854411238048020657762893628870965487194767200476309931907607945075544279086782037257684303674574
e = int(65537)
c = int(998434113335065007865160329408761783290703148353160084569118804656148779366620757978652206815542631170363715345672540749883779789232475892897368714159092546682327856088550575794
)
p_minus_q = int(-197594706238351886139039107894930190288450845252462461979334671562978761272637694556369639708947974277077524627206001837914483246601244380103616092721016452008632442178


D = p_minus_q*p_minus_q + 4*n
s = isqrt(D)
assert s*s == D

p = (p_minus_q + s) // 2
q = n // p
assert p*q == n

phi = (p-1)*(q-1)
d = inverse(e, phi)
m = pow(c, d, n)
pt = long_to_bytes(m)

print("p =", p)
print("q =", q)
print("plaintext bytes:", pt)
try:
    print("plaintext (utf-8):", pt.decode())
except:
    pass
```

PETIR{saya_bisa_RSA_dan_aljabar_yeyeyyyy}