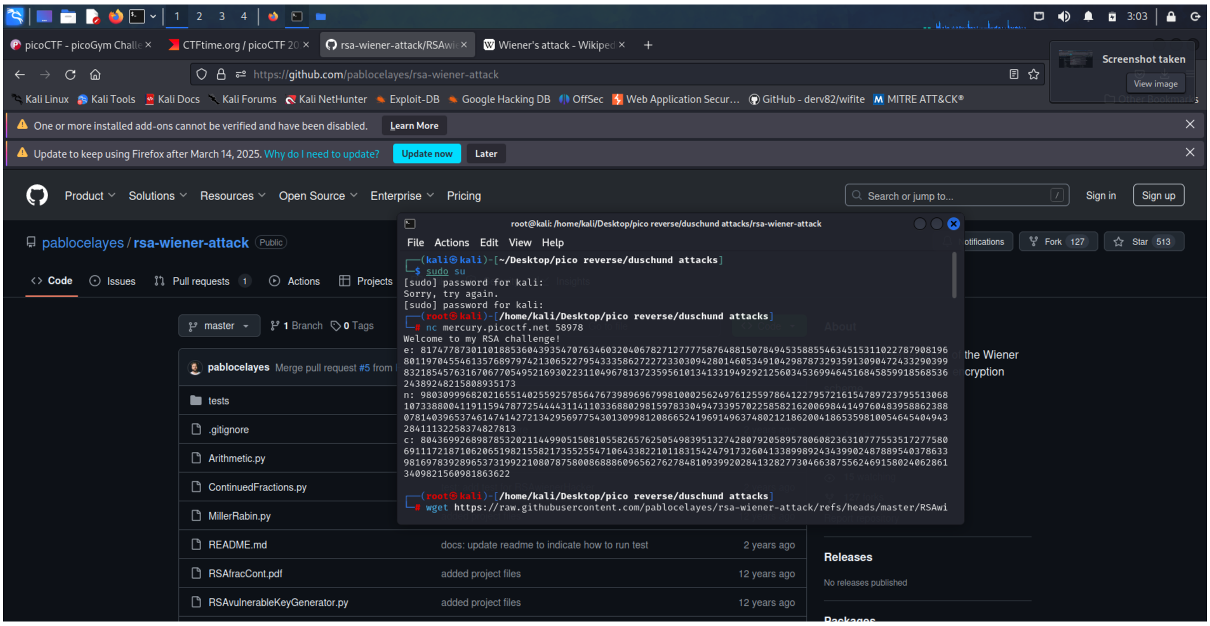
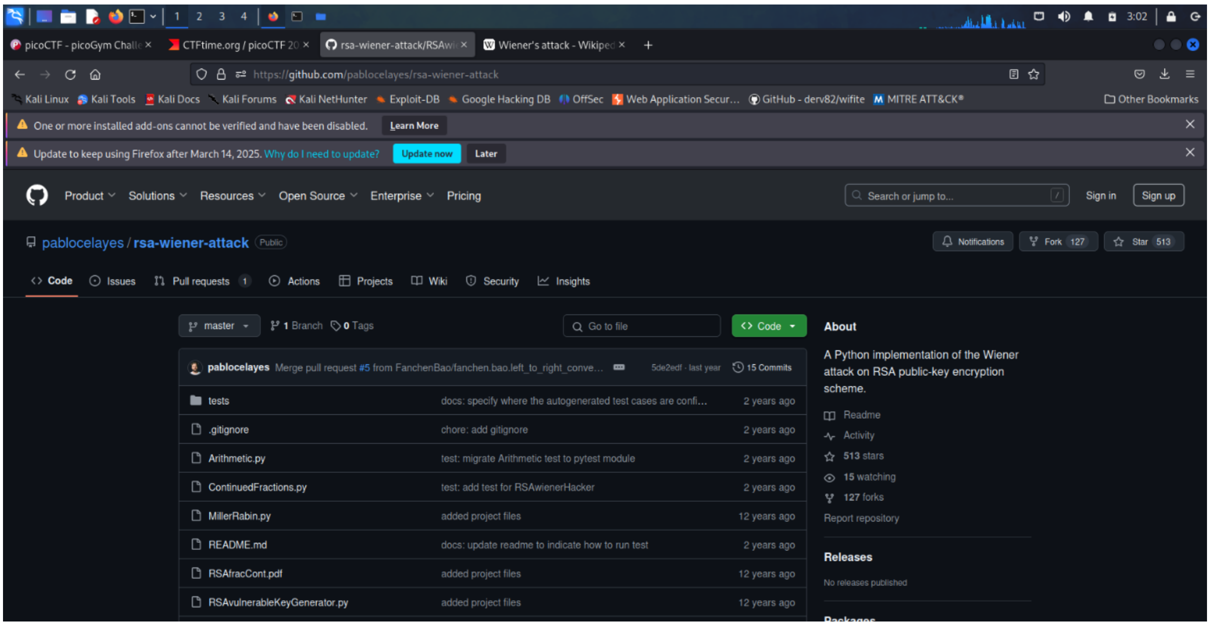
By using the nc mercury.picoctf.net 58978



```
┌──(kali㉿kali)-[~/Desktop/pico reverse/duschund attacks]
└─$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop/pico reverse/duschund attacks]
└─# nc mercury.picoctf.net 58978
Welcome to my RSA challenge!
e: 8174778730110188536043935470763460320406782712777758764881507849453588554634515311022787908196
8011970455461357689797421306522795433358627227233030942801460534910429878732935913090472433290399
8321854576316706770549521693022311049678137235956101341331949292125603453699464516845859918568536
2438924821580893517 3
n: 9803099968202165514025592578564767398969679981000256249761255978641227957216154789723795513068
1073388004119115947877254444311411033688029815978330494733957022585821620069844149760483958862388
0781403965374614741427213429569775430130998120866524196914963748021218620041865359810054645404943
284111322583748278 13
c: 8043699268987853202114499051508105582657625054983951327428079205895780608236310777553517277580
6911172187106206519821558217355255471064338221011831542479173260413389989243439902487889540378633
9816978392896537319922108078758008688860965627627848109399202841328277304663875562469158024062861
340982156098186362 2

┌──(root㉿kali)-[/home/kali/Desktop/pico reverse/duschund attacks]
└─# wget https://raw.githubusercontent.com/pablocelayes/rsa-wiener-attack/refs/heads/master/RSAwi
```

So next step is



pablocelayes / rsa-wiener-attack

pablocelayes Merge pull request #5 from FanchenBao/fanchen.bao.left_to_right_conve… 5de2edf · last year 15 Commits

tests	docs: specify where the autogenerated test cases are confi…	2 years ago
.gitignore	chore: add gitignore	2 years ago
Arithmetic.py	test: migrate Arithmetic test to pytest module	2 years ago
ContinuedFractions.py	test: add test for RSAwienerHacker	2 years ago
MillerRabin.py	added project files	12 years ago
README.md	docs: update readme to indicate how to run test	2 years ago
RSAfracCont.pdf	added project files	12 years ago
RSAvulnerableKeyGenerator.py	added project files	12 years ago

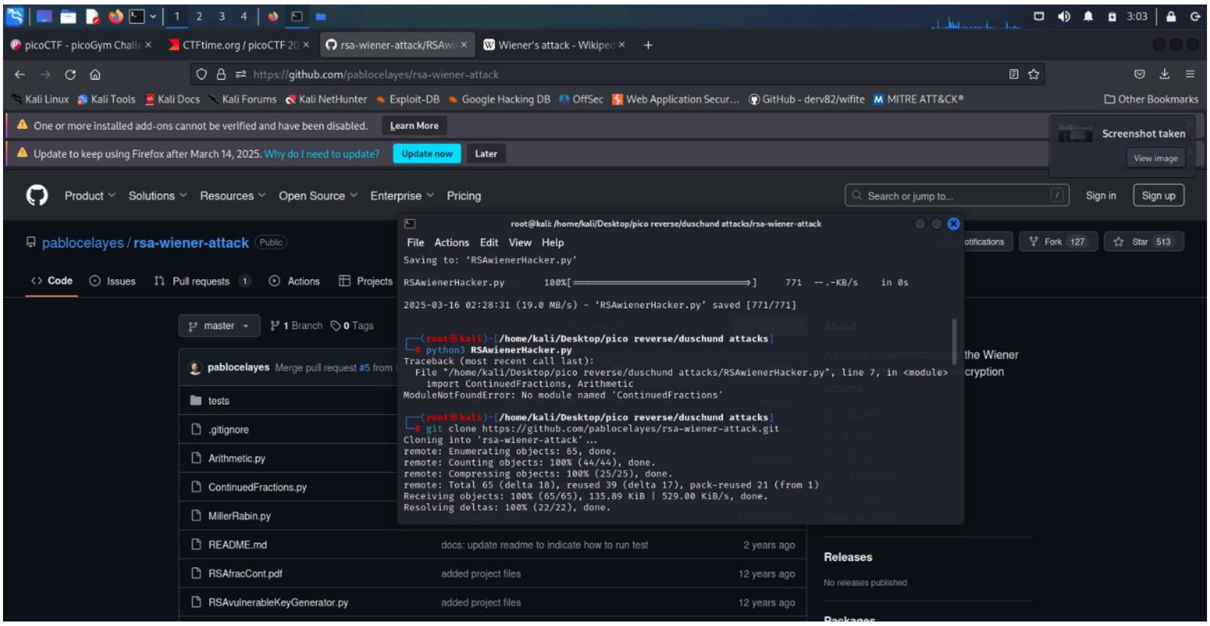
About

A Python implementation of the Wiener attack on RSA public-key encryption scheme.

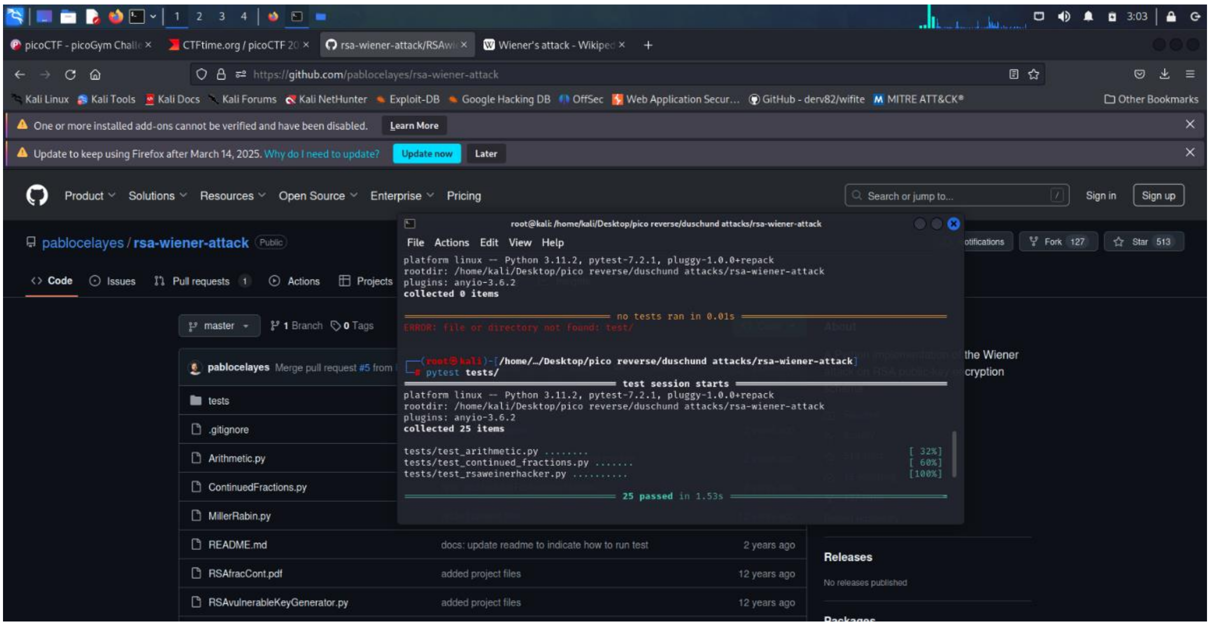
Use the the required github to use weiner attack against rsa cipher basically when d is too small it will create in secure cipher

https://github.com/pablocelayes/rsa-wiener-attack

read the readme in the directory of the github and do the required steps

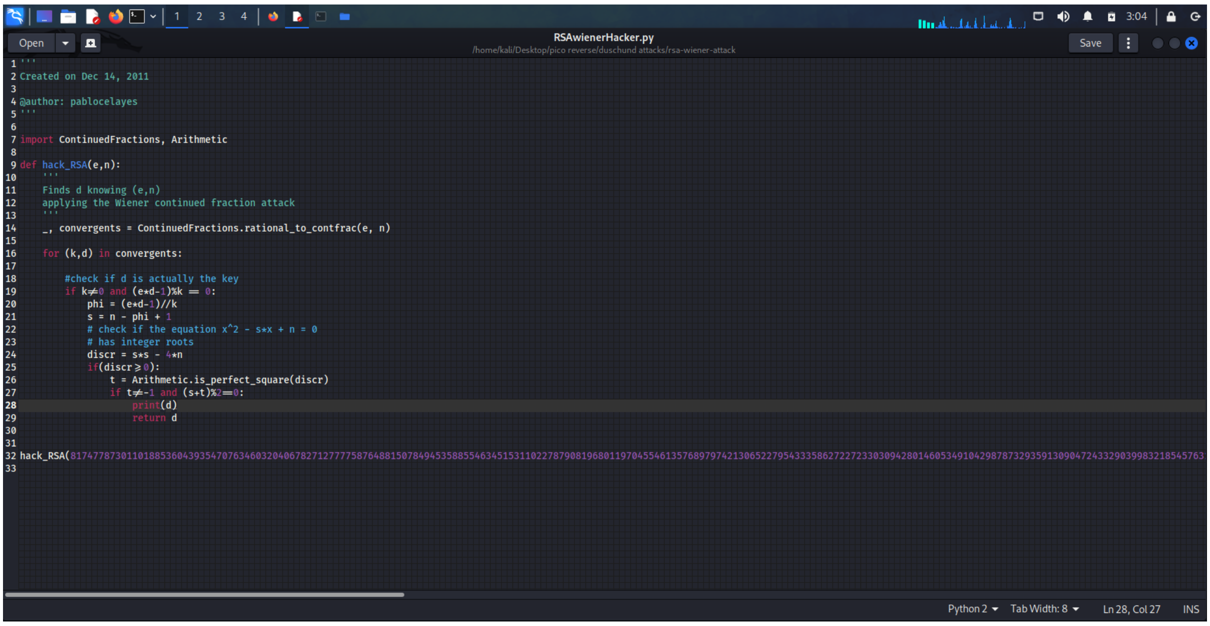


```
root@kali: /home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack
Saving to: 'RSAwienerHacker.py'

RSAwienerHacker.py        100%[==============================>]     771  --.-KB/s    in 0s

2025-03-16 02:28:31 (19.0 MB/s) - 'RSAwienerHacker.py' saved [771/771]


┌──(root㉿kali)-[/home/kali/Desktop/pico reverse/duschund attacks]
└─# python3 RSAwienerHacker.py
Traceback (most recent call last):
  File "/home/kali/Desktop/pico reverse/duschund attacks/RSAwienerHacker.py", line 7, in <module>
    import ContinuedFractions, Arithmetic
ModuleNotFoundError: No module named 'ContinuedFractions'

┌──(root㉿kali)-[/home/kali/Desktop/pico reverse/duschund attacks]
└─# git clone https://github.com/pablocelayes/rsa-wiener-attack.git
Cloning into 'rsa-wiener-attack'...
remote: Enumerating objects: 65, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 65 (delta 18), reused 39 (delta 17), pack-reused 21 (from 1)
Receiving objects: 100% (65/65), 135.89 KiB | 529.00 KiB/s, done.
Resolving deltas: 100% (22/22), done.
```



```
root@kali: /home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack
platform linux -- Python 3.11.2, pytest-7.2.1, pluggy-1.0.0+repack
rootdir: /home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack
plugins: anyio-3.6.2
collected 0 items

================================ no tests ran in 0.01s ================================
ERROR: file or directory not found: test/


┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# pytest tests/
================================ test session starts ================================
platform linux -- Python 3.11.2, pytest-7.2.1, pluggy-1.0.0+repack
rootdir: /home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack
plugins: anyio-3.6.2
collected 25 items

tests/test_arithmetic.py ........                                              [ 32%]
tests/test_continued_fractions.py .......                                      [ 60%]
tests/test_rsaweinerhacker.py ..........                                       [100%]

================================ 25 passed in 1.53s ================================
```

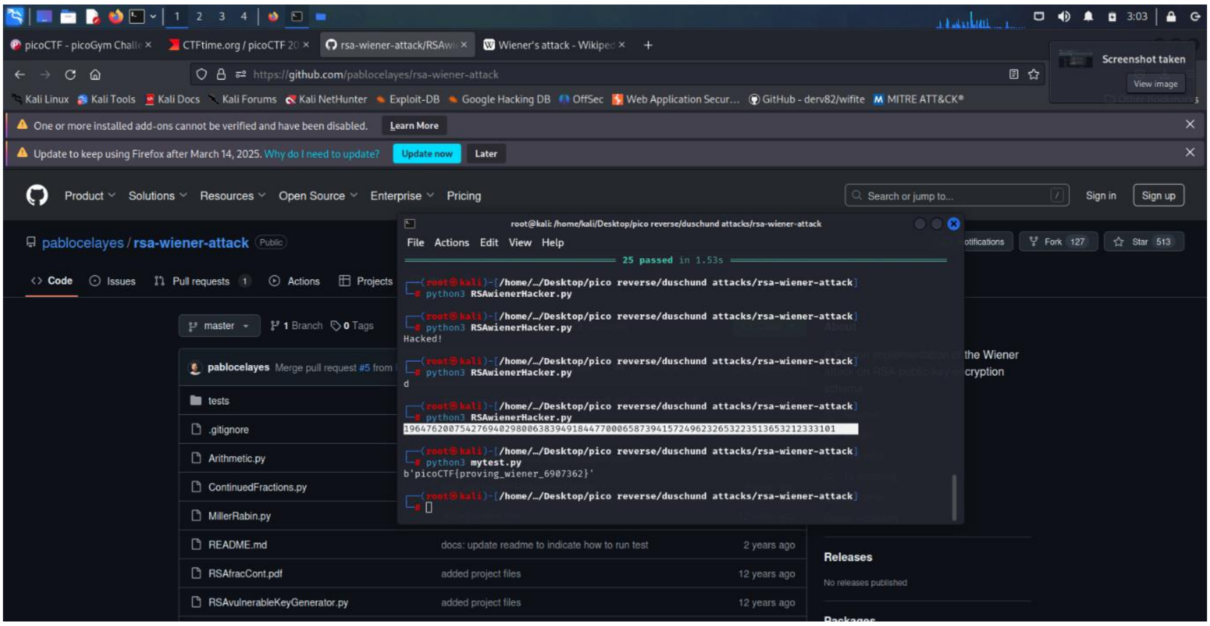
Now, change the program a little and print d nad write the function so that it can call



```python
'''
Created on Dec 14, 2011

@author: pablocelayes
'''

import ContinuedFractions, Arithmetic

def hack_RSA(e,n):
    '''
    Finds d knowing (e,n)
    applying the Wiener continued fraction attack
    '''
    _, convergents = ContinuedFractions.rational_to_contfrac(e, n)

    for (k,d) in convergents:

        #check if d is actually the key
        if k≠0 and (e*d-1)%k == 0:
            phi = (e*d-1)//k
            s = n - phi + 1
            # check if the equation x^2 - s*x + n = 0
            # has integer roots
            discr = s*s - 4*n
            if(discr≥0):
                t = Arithmetic.is_perfect_square(discr)
                if t≠-1 and (s+t)%2==0:
                    print(d)
                    return d


hack_RSA(8174778730110188536043935470763460320406782712777758764881507849453588554634515311022787908196801197045546135768979742130652279543335862722723303094280146053491042987873293591309047243329039983218545763

```

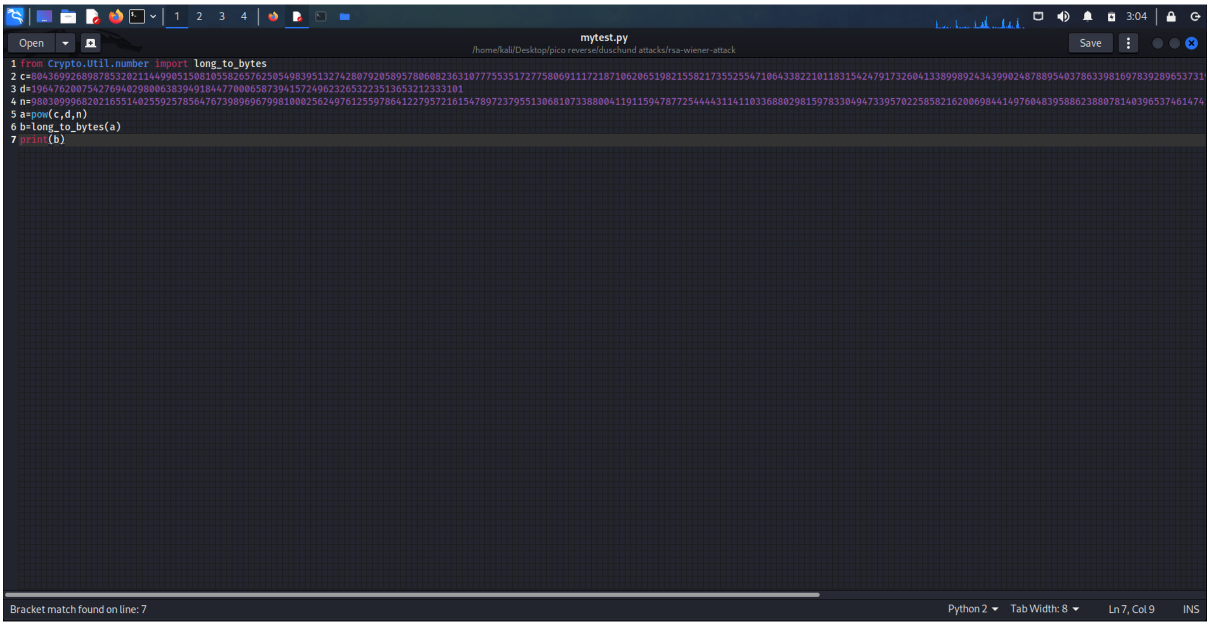
Open
RSAwienerHacker.py
/home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack
Save
Python 2
Tab Width: 8
Ln 28, Col 27
INS
3:04

And then you will find the d



```
root@kali: /home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack
══════════════════ 25 passed in 1.53s ══════════════════

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py
Hacked!

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py
d

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py
19647620075427694029800638394918447700065873941572496232653223513653212333101

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 mytest.py
b'picoCTF{proving_wiener_6907362}'

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# 
```

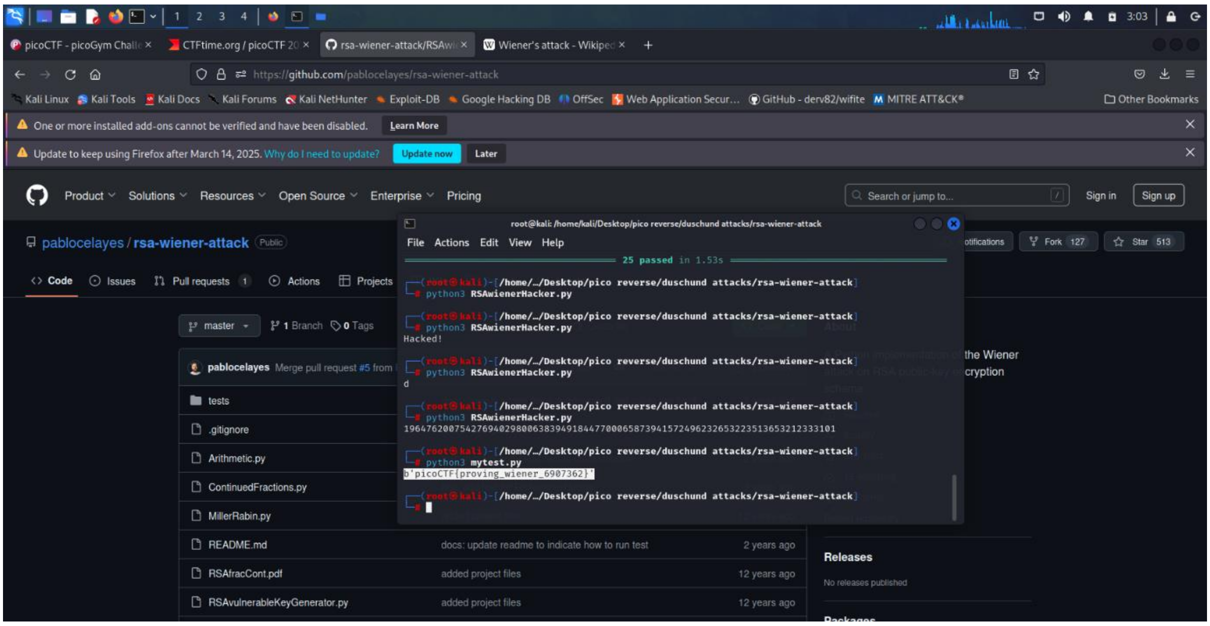
And use the d for your script


Open
mytest.py
/home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack
Save
Bracket match found on line: 7
Python 2
Tab Width: 8
Ln 7, Col 9
INS

```
from Crypto.Util.number import long_to_bytes
c=804369926898785320211449905150810558265762505498395132742807920589578060823631077755351727758069111721871062065198215582173552554710643382210118315424791732604133899892434399024878895403786339816978392896537319
d=19647620075427694029800638394918447700065873941572496232653223513653212333101
n=98030999682021655140255925785647673989696799810002562497612559786412279572161547897237955130681073388004119115947877254444311411033688029815978330494733957022585821620069844149760483958862388078140396537461474
a=pow(c,d,n)
b=long_to_bytes(a)
print(b)
```

And execute it you will get the flag

```
from Crypto.Util.number import long_to_bytes

c=8043699268987853202114499051508105582657625054983951327428079205895780608236310777553517277580691117218710620651982155821735525547106433822101183154247917326041338998924343990248788954037863398169783928965373199221080787580086888609656276278481093992028413282773046638755624691580240628613409821560981863622

d=19647620075427694029800638394918447700065873941572496232653223513653212333101

n=9803099968202165514025592578564767398969679981000256249761255978641227957216154789723795513068107338800411911594787725444431141103368802981597833049473395702258582162006984414976048395886238807814039653746147414272134295697754301309981208665241969149637480212186200418653598100546454049432841113225837482781 3

a=pow(c,d,n)

b=long_to_bytes(a)

print(b)
```



root@kali: /home/kali/Desktop/pico reverse/duschund attacks/rsa-wiener-attack

```
================================ 25 passed in 1.53s ================================

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py
Hacked!

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py
d

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 RSAwienerHacker.py
19647620075427694029800638394918447700065873941572496232653223513653212333101

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# python3 mytest.py
b'picoCTF{proving_wiener_6907362}'

┌──(root㉿kali)-[/home/…/Desktop/pico reverse/duschund attacks/rsa-wiener-attack]
└─# 
```