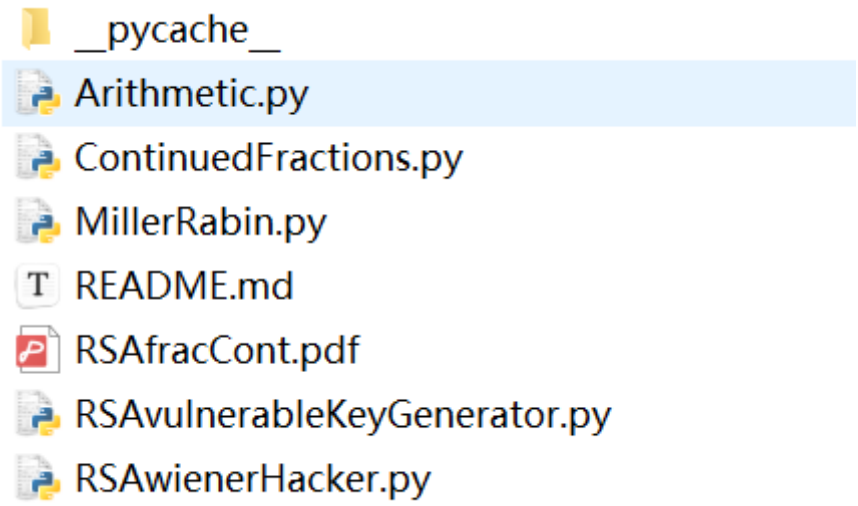
2022 HGAME WEEK3 容世

Crypto

RSA Attack 3

维纳



Hacker改参数

```
if __name__ == "__main__":
    #test_is_perfect_square()
    #print("-------------------------")

 d=hack_RSA(773101998674486777820815721093434727837811356417125976435971225914430112290915335167589252389497554913954894089224374936702525509208266414421896839079739268435054367300148999185874779130322861535452470634938859829411949962517998829841451557330500695644851206607161108281107387846442235197256132801400067836183939951380760306164633982848195506276121020102143152352699452517414078996922749786426636506871577364178312904048711819024639043110954483684984321472929388254189305271887206964975968675758434768102251526592445294814809938431683830165830687477331187030002874233740940518957244941934551751311202430970652708044577870264925789165845368635484458139168194178570640376641016844550001849875312523445828995897462721739700837331301064078106192580772666038985292856344957108468380118582870243295144910587905573050413896146507302677744829546667269498863133868810665939467894600283995232457771713203194446735512683791262038625766275401778882902657144180643347524999405877503745523300081437085620659402456376858333713486033388344472122486488695145850478714420604126221642768947662383838946937593475909779263065810803906853606154077666005735275650169148301320664284547381353801789595906921455774188116776390509297919963131802979248336900 95,507419170088344932990702256911694788408493968749527614421614568612944144764889717229444020813658893362983714454159980719026366361318789415279417172858536381938870379267670180128174798344744371725609827872339512302232610590888649555446972990419313445687852636305518801236132032618350847705234643521557851434711389664130274468354405273873218264222293858509477860634889001898462547712800153111774564939279190835857445378261920532206352364005840238252284065587291779196975457288580812526597185332036342330147250312262816994625317482869849388424397437470502449815132000588425028055964432298176942124697105509057090546600330760364385753313923003549670107599757996810939165300581847068233156887269181096893089415302163770884312255957584660964506028002922164767453287973102961910781312351686488047510932997937700597992705557881172640175117476017503918294534205898046483981707558521558992058512940087192655700351675718815723840568640509355338482631416345193176708501897458649841539192993142790402734898948352382350766125000186026261167277014748183012844440603384989647664190074853086693408529737767147592432979469020671772152652865219092597717869942730499507426269170189547020660681363276871874469322437194397171763927907099922324375991793759)

    print(d)
```

```
\rsa-wiener-attack-master> python RSAwienerHacker.
Hacked!
13094612077654083919
```

得d。

```
import libnum
n =
507419170088344932990702256911694788408493968749527614421614568612944144764889717229444020813658893362983714454159980719026366361318789415279417172858536381938870379267670180128174798344744371725609827872339512302232610590888649555446972990419313445687852636305518801236132032618350847705234643521557851434711389664130274468354405273873218264222293858509477860634889001898462547712800153111774564939279190835857445378261920532206352364005840238252284065587291779196975457288580812526597185332036342330147250312262816994625317482869849388424397437470502449815132000588425028055964432298176942124697105509057090546600330760364385753313923003549670107599757996810939165300581847068233156887269181096893089415302163770884312255957584660964506028002922164767453287973102961910781312351686488047510932997937700597992705557881172640175117476017503918294534205898046483981707558521559992058512940087192655700351675718815723840568640509355338482631416345193176708501897458649841539192993142790402734898948352382350766125000186026261167277014748183012844440603384989647664190074853086693408529737767147592432979469020671772152652865219092597717869942730499507426269170189547020660681363276871874469322437194397171763927907099922324375991793759

c =
165251729917394529793163344300848992394021337429474789711805041655116845722480301677817165053253655027459227404782607373107477419083333844871948673626672704233977397989843349633720167495862807995411682262559392496273163155214888276398332204954185252030616473235814999366132031184631541209554169938146205402400412307638567132128690379079483633171535375278689326189057930259534983374296873110199636558962144635514392282351103900375366360933088605794654279480277782805401749872568584335215630740265944133347038070337891035560658434763924576508969938866566235926587685108811154229747423410476421860059769485356567301897413767088823807510568561254627099309752215808220067495561412081320541540679503218232020279947159175547517811501280846596226165148013762293861131544331444165070186672186027410082671602892508739473724143698396105392623164025712124329254933335350938474840315434232272520318305032814373663133399044553711985586534822121527760837295294270210408894095214285152365163957440907548410685740365145312103657776767243061272802244437087422300177858038763519732504352471939670771338596343291585522715237180052753604855555123772969066354482883062719286757034585391019639785176359154348402313455187659124855798018298196778240905427722 4

d=13094612077654083919
m=pow(c,d,n)
print(libnum.n2s(int(pow(c,d,n))))
```

```
RSA Attack 3> python task.py
b'hgame{dO|YOU:kNOw!tHE*PRINcIplE*bEhInd%WInNEr#aTTacK}'
```

`hgame{dO|YOU:kNOw!tHE*PRINcIplE*bEhInd%WInNEr#aTTacK}`