Easy RSA:

打开文件

```
from math import gcd
from random import randint
from gmpy2 import next_prime
from Crypto.Util.number import getPrime
from secret import flag

def encrypt(c):
    p = getPrime(8)
    q = getPrime(8)
    e = randint(0, p * q)
    while gcd(e, (p - 1) * (q - 1)) != 1:
        e = int(next_prime(e))
        return e, p, q, pow(ord(c), e, p * q)

if __name__ == '__main__':
    print(list(map(encrypt, flag)))
    # [(12433, 149, 197, 104), (8147, 131, 167,
```

显而易见

我看不懂!

学!



在prime.py中可以找到getprime(nbits)函数。这个函数的具体实现是:先随机生成一个数字,然后判断是不是质数。

3.求大整数x模m的逆元v

```
1 import gmpy2
2 #4*6 = 1 mod 23
3 gmpy2.invert(4,23)
4
5 result:mpz(6)
```

GCD算法是用于求解最大公约数^Q的方法。

字面理解 next_prime()可能是下一个素数的意思

原代码总体意思就是将代码 rsa 加密后再打印出 e,q,p 和密文的 ascll 码值

鬼然 这 RSA 不是有手就行?!

上代码

```
import gmpy2
a=[(12433, 149, 197, 104), (8147, 13)
arr=""
for i in a :
    e=i[0]
    p=i[1]
    q=i[2]
    c=i[3]
    s = (p-1)*(q-1)
    d = gmpy2.invert(e,s)
    m=pow (c,d,p*q)
    arr+=chr(m)
print(arr)
```

求得

```
'c:\Users\zzy\Desktop\文件夹\program_py
hgame{L00ks_l1ke_y0u've_mastered_RS4!}
PS_C:\Users\zzy\Deskton\文件夹\program_
```

English Novel:

观察一下附件

- encrypt
- original
- encrypt.py
- flag.enc

分别是

- 1. 加密后的小说
- 2. 原小说
- 3. 加密方式
- 4. 加密后的 flag

鉴于已经有了加密方式,我想到了逆推加密方式的方法求解 key 根据原式子

```
if data[i].isupper():
    result += chr((ord(data[i]) - ord('A') + key[i]) % 26 + ord('A'))
elif data[i].islower():
    result += chr((ord(data[i]) - ord('a') + key[i]) % 26 + ord('a'))
else:
    result += data[i]
```

(式子中有错误的地方已经改正)

写出

```
for i in range(len(data1)):
    if data1[i].isupper() or data1[i].islower():
        key.append((ord(data2[i])-ord(data1[i]))%26)
    else:
       key.append(' ')
```

并用此解密

但是当我观察两个小说文件夹时,发现两个文件夹内的小说的 part 的序号并不是一一对应 的关系

这需要我再去找到对应的小说来求解 key

由于文章内除字母以外的标点符号, 空格或者回车键不会被加密, 我采取了寻找特殊标点的 方式

read:

"'Alfred Simmonds, Horse Slaughterer 比如这一外A cry of horror burst from all the anim

Part0 后面的 3 个标点的位置较为特殊, 所以我们可以利用这个特殊性去加密后的文件夹一

part175.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

wwme:

"'Lmgzwg Vugmtxht, Hbnvd Shzdheysfhu avv Glpl E cmy oj kkxxuz xxqrf blzi xsm oki pfrfaeq. Uu wnq

一寻找、最终找到

Part175 正与其一一对应

但是, 由于有标点符号的存在, 一对文本显然不够。 所以我找到了3对。

```
path1=r"C:\Users\zzy\Desktop\English Novel\encrypt\part175.txt"
path2=r"C:\Users\zzy\Desktop\English Novel\original\part0.txt"
path3=r"C:\Users\zzy\Desktop\English Novel\encrypt\part379.txt"
path4=r"C:\Users\zzy\Desktop\English Novel\original\part3.txt"
path5=r"C:\Users\zzy\Desktop\English Novel\encrypt\part69.txt"
path6=r"C:\Users\zzy\Desktop\English Novel\original\part58.txt"
```

最终得出答案

下面是代码。

1. 根据加密前后的文章求 key

```
def rencrypt(data1, data2):
    key = []
    for i in range(len(data1)):
        if data1[i].isupper() or data1[i].islower():
            key.append((ord(data2[i])-ord(data1[i]))%26)
        else:
            key.append(' ')
        return key
```

2.根据两对文章求得的残缺的 key, 补齐成最终的 key

```
def rkey(key1,key2):
    key=[]
    for i in range(len(key1)):
        if key1[i]!=' ':
            key.append(key1[i])
        elif key2[i]!=' ':
            key.append(key2[i])
        else :
            key.append(' ')
```

3.打开文件读取其中的文本

```
def skey(path1,path2):
    with open(path1) as f1:
        data1 = f1.read()
    with open(path2) as f2:
        data2 = f2.read()
    return rencrypt(data1, data2)
```

4主函数

```
if __name__=="__main__":
    path1=r"C:\Users\zzy\Desktop\English Novel\encrypt\part175.txt"
    path2=r"C:\Users\zzy\Desktop\English Novel\original\part0.txt"
    path3=r"C:\Users\zzy\Desktop\English Novel\encrypt\part379.txt"
    path4=r"C:\Users\zzy\Desktop\English Novel\original\part3.txt"
    path5=r"C:\Users\zzy\Desktop\English Novel\encrypt\part69.txt"
    path6=r"C:\Users\zzy\Desktop\English Novel\original\part58.txt"
    key1=skey(path1,path2)
    key2=skey(path3,path4)
    key3=skey(path5,path6)
    key=rkey(rkey(key1,key2),key3)

print(encrypt(r"klsyf{W0_j0v_ca0z_'Ks0ao-bln1qstxp_juqfqy'?}", key))
```

欢迎欢迎!热烈欢迎!:

嗯。。。

蛛蛛...嘿■我的蛛蛛:

第一步, f12 大法

点击蓝色字体

```
<!DOCTYPE html>
<html>
▶ <head>...</head>
..▼ <body> == $0
        <h1>你现在在第2关</h1>
        <up><a href="?key=x45woG55R7i6zlaYKGd40C9fatgYdw%2FT3ZG0nh%2FNYepw0WENC%2Fc3oKTmUY94u4W6iU0M5%2Ffiu%2FeesctdYI5NDw%3D%3D">点我试试</a>
        <a href> 点我试试</a>
        </body>
</html>
```

继续点。。。

```
<html>
▶ <head> </head>
• ▼ <body> == $0
  <h1>你现在在第22关</h1>
  <红豆泥私密马赛,我忘记我把flag丢在哪一关了,下面有个按钮让你前往下一关,慢慢找叭~XD</p>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
<a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  h2xg%3D%3D">点我试试</a>
  <a href>点我试试</a>
   <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
  <a href>点我试试</a>
   <a href>点我试试</a>
   <a href>点我试试</a>
  <a href>点我试试</a>
```

点到 20 几关的时候我意识到事情的不对劲,这样凭点下去肯定不行。 要么另辟蹊径,要么写一行代码一直点下去看看有没有效果。

好像也没有其他办法、就写了一点代码

```
import requests
import re
url = ' https://hgame-spider.vidar.club/70845b5df1'
s = requests.session()
g = s.get(url)
for i in range(1000):
    s = requests.session()
    g = s.get(url)
    if 'hgame' in g.text:
        print(g.text)
        break
    obj2=re.compile(r'<a href="\?key=(?P<href>.*?)">点我试试</a>',re.S)
    result2=obj2.findall(g.text)
    if len(result2)!=0:
        print(result2[0])
        res = result2[0]
        url='https://hgame-spider.vidar.club/70845b5df1'+"?key="+res
        print(url)
    else:
        print(g.text)
        break
```

如果返回的文本里面有 hgame 就停止

```
waThAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6nzDsCuBVTfb52RGoOVRZuhfg%2F16d2a5ErtWzV3RakjMg%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6nzDsCuBVTfb52RGoOVRZuhfg%2F16d2a5ErtWzV3RakjMg%3D%3D
waThAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6lqFV8TDvVG0H%2F6h6Dck%2FVJIt%2FsgMXKIA75%2F0LPx1Ezbw%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6lqFV8TDvVG0H%2F6h6Dck%2FVJIt%2FsgMXKIA75%2F0LPx1Ezbw%3D%3D
waThAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6kOtkVq3NU96xDA1uD3qjxxy8mwDUE%2BDVOHj3FfFGnw1g%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waThAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6kOtkVq3NU96xDA1uD3qjxxy8mwDUE%2BDYOHj3FfFGnw1g%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waThAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6kOtkVq3NU96xDA1uD3qjxxy8mwDUE%2BDYOHj8FfFGnw1g%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waThAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6khsQrbz0cuJUPrkt6a1dyHr2XJ0oJ4IenX3CRA%2BZ6Rag%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waThAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6khsQrbz0cuJUPrkt6a1dyHr2XJ0oJ4IenX3CRA%2BZ6Rag%3D%3D
```

本想着运行不完就换一个代码

然后

```
</https:
</https://documents.com/
</https://documents.com/
</pre>

</pr>

</pre
```

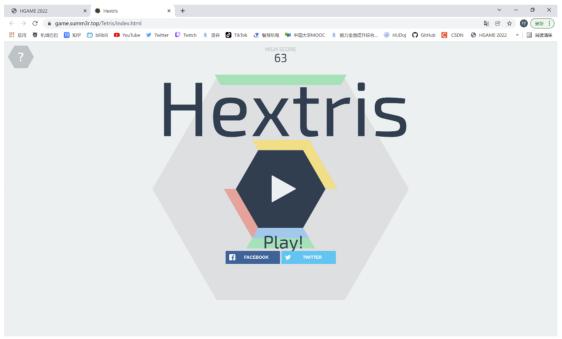
打开网址, f12

date: Fri, 28 Jan 2022 06:32:43 UMI

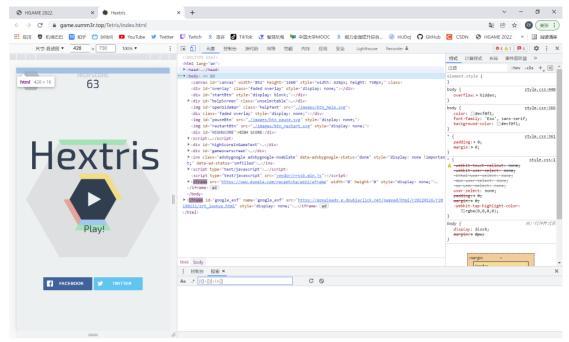
fi4g: hgame{a48cde454289659e2d8aabcd84bbb826275012ac0d0e06b4ad1a266f12ac3109}

welcome-to-haame: See you next week!

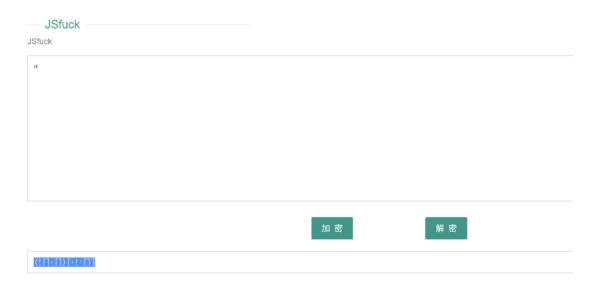
Tetris plus:



稍微玩了一会, 3000 分无望, 用 f12 大法



应该是藏了什么东西 尝试搜索一下'a'的 jsfuck 加密



找到了这个

```
if (score >= 3000 && !window.winned) {
    winned = true
    alert(atob("ZmxhZyDosozkvLzooqvol4/otbfmnaXkuobvvIzlho3mib7mib7lkKch"))
    // [][(![]+[])[+[]]+(![]+[])[!+[]]+(![]+[])[+[]]+(!![]+[])[+[]]][([]]
}
```

解密

Fujiwara Tofu Shop:

先观察题目



想成为车神,你需要先去一趟秋名山 (qiumingshan.net)

可以看见结尾一个很"明显"的提示:

qiumingshan.net

嗯。进不去



无法访问此网站

检查 qiumingshan.net 中是否有拼写错误。

如果拼写无误,请尝试运行 Windows 网络诊断。

DNS_PROBE_FINISHED_NXDOMAIN

重新加载

shop.summ3r.top/giumingshan.net

好吧也进不去

404 page not found

网络上兜兜转转一下午,确实没啥路可以走了,就无脑用 get 尝试一下。 在尝试了无数种可能后,发现 在请求头里面放

```
"referer":"qiumingshan.net",
```

有

接下来就"好办"了(实则经历了无数次的尝试)

```
"User-Agent": "Hachi-Roku",
```

```
<img src="https://game.summ3r.top/assets/raspberry.jpg"
<p>86的副驾上应该放一盒树莓(Raspberry)味的曲奇
ody>
```

```
"Cookie":"flavor=Raspberry",
```

```
/>
<img src="https://game.summ3r.top/assets/petral.jpg
汽油都不加,还想去秋名山?请加满至100
```

"gasoline": "100",

```
/>
<img src="https://game.summ3r.top/assets/win.jpg" alt="win" sty
哪怕成了车神,也得让请求从本地发出来才能拿到 flag ! 
dy>
nl>
```

```
"X-Real-IP": "127.0.0.1"
```

```
hgame{I_b0ught_4_S3xy_sw1mSu1t}
```