

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(nbbits)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y

```
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** 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 ascii 码值

果然 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\Desktop\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
    A cry of horror burst from all the anim
```

比如这一处

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:

```
"Lmgzwq Vugmtxht, Hbnvd Shzdheysfhu avv Glpl
E cmy oj kkxxuz xxqrf blzi xsm oki pfrfaeq. Uu wnn
```

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(' ')
    return key
```

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


```
waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6nzDsCuBVTfb52RGoOVRZuhfg%2F16d2a5ErtWzV3RakjMg%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6nzDsCuBVTfb52RGoOVRZuhfg%2F16d2a5ErtWzV3RakjMg%3D%3D
waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo61qFV8TDvVG0Hk%2F6h6Dck%2FVJIit%2FsgMXK1A75%2F0LPx1Ezbw%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo61qFV8TDvVG0Hk%2F6h6Dck%2FVJIit%2FsgMXK1A75%2F0LPx1Ezbw%3D%3D
waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6k0tkVq3NU96xDA1uD3qjxxy8mwDUE%2BDYOHj8fffGnw1g%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6k0tkVq3NU96xDA1uD3qjxxy8mwDUE%2BDYOHj8fffGnw1g%3D%3D
waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6khsQrbz0cuJUPrkt6a1dyHr2XJ0oJ4IenX3CRA%2BZ6Rag%3D%3D
https://hgame-spider.vidar.club/70845b5df1?key=waIhAPv5m%2FNnK8InB0DSntbsBfx00q5vPSQsMdFbo6khsQrbz0cuJUPrkt6a1dyHr2XJ0oJ4IenX3CRA%2BZ6Rag%3D%3D
```

本想着运行不完就换一个代码

然后

```
</style>
</head>
<body>
  <h1>我好像在就是把flag落在这里了欸~ 快帮我找找x</h1>
  <p>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关，慢慢找叭~XD</p>
  <a href="">点我试试</a>
</body>
</html>
```

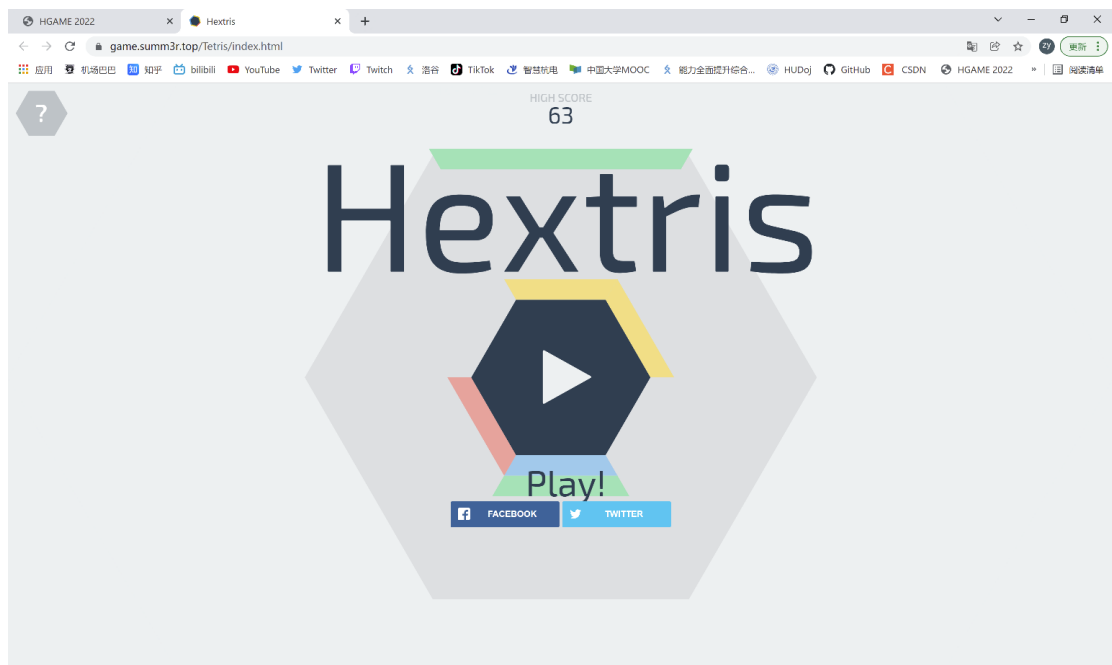
打开网址，f12

date: Fri, 28 Jan 2022 06:52:45 GMT

fi4g: hgame{a48cde454289659e2d8aabcd84bbb826275012ac0d0e06b4ad1a266f12ac3109}

welcome-to-hgame: See you next week!

Tetris plus:



稍微玩了一会，3000分无望，用f12大法


```
'alert("hgame{jsfuck_1s_s0_f0u1n}")'
```

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

或者？

shop.summ3r.top/qiumingshan.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

```

<p>只有借助AE86才能拿到车神通行证（Hachi-Roku）</p>
</body>
```

接下来就“好办”了（实则经历了无数次的尝试）

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

```
</body>

<p>86的副驾上应该放一盒树莓（Raspberry）味的曲奇</p>
</body>
```

```
"Cookie": "flavor=Raspberry",
"referer": "qiumingshan.net"
```

```
</body>

<p>汽油都不加，还想去秋名山？请加满至100</p>
</body>
```

```
"gasoline": "100",
```

```
</body>

<p>哪怕成了车神，也得让请求从本地发出来才能拿到 flag ! </p>
</body>
</html>
```

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

```
c:\Users\zzy\Desktop\文件夹\prog...
hgame{I_b0ught_4_S3xy_sw1mSu1t}
D6-G\Hgame\src\Desktop\文件夹\pro...
```