xD MAZE

`ida`打开，直接分析，写脚本

```
a=[...]#这里提取一波数据，好多好多行
b=[]
for i in range(len(a)):
  if(a[i]==32):
    b.append(i)
print(len(b))
print(b)

c=''
for i in range(len(b)-1):
  #print(b[i+1]-b[i])
  if(b[i+1]-b[i]==1):
    c+='3'
  if(b[i+1]-b[i]==8):
    c+='2'
  if(b[i+1]-b[i]==64):
    c+='1'
  if(b[i+1]-b[i]==512):
    c+='0'
print(c)
print(len(c))
```

RSA Attack

RSA加密

```
http://www.factordb.com/index.php
```

这个网站可以进行大数分解成两个素数，网上找到脚本修改一下

```
from gmpy2 import *
from libnum import s2n,n2s
from Crypto.Util.number import *

def decrypt():
    flag = ''
    n = 700612512827159827368074182577656505408114629807
    e =65537
    p=715800347513314032483037
    q=978782023871716954857211
    phi_n = (p-1)*(q-1)
```

```
    (g,d,_) = gcdext(e,phi_n)  #利用此函数可以获取私钥d值
    print("Privcate key:",str(g),str(d))
    plaintext =122622425510870177715177368049049966519567512708
    num=int(pow(plaintext,d,n))
    flag=n2s(num)
    print(flag)

if __name__=='__main__':
   decrypt()
```

end