[GKCTF 2021]Random（MT19973随机数破解)

原创

是真的白 于 2022-04-19 17:18:27 发布 669 收藏
文章标签： 密码学

本文链接：https://blog.csdn.net/m0_62506844/article/details/124278580

对于MT19973有randcrack一把梭

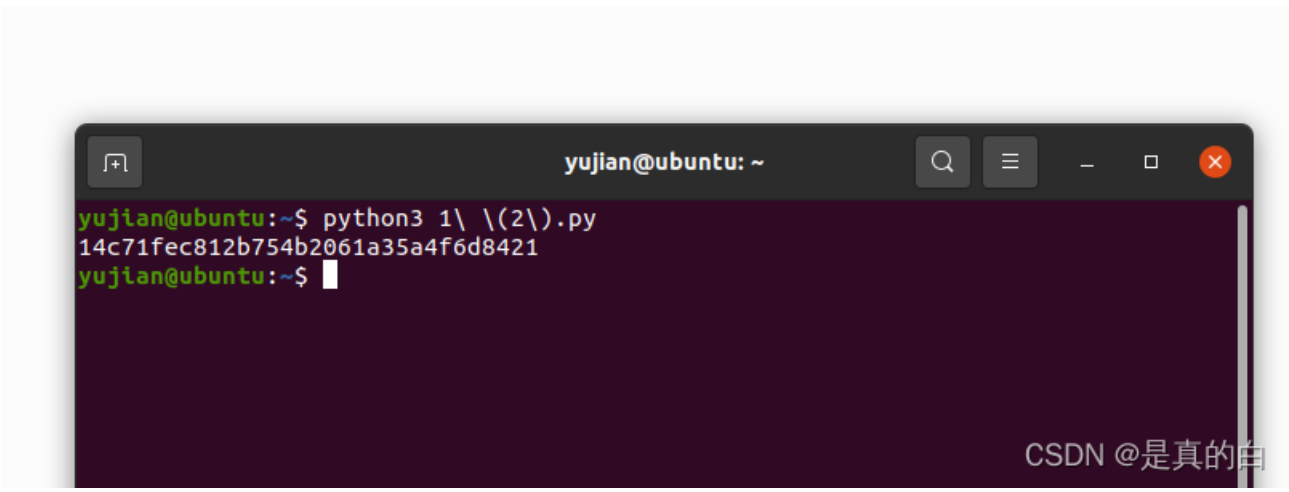
我这本地有点小问题，虚拟机才能安上randcrack库

这道题的难度在于MT19973是如何生成32，64，96位随机数的

实际上MT19973一次只能生成32位随机数，生成64位就要从低位到高位生成两组32位随机数，借鉴一下大佬们的wp吧，具体原理我也不是很清楚

```
from hashlib import md5
from randcrack import RandCrack

with open(r'random.txt', 'r') as f:
    l = f.readlines()
l = [int(i.strip()) for i in l]
t = []
for i in range(len(l)):
    if i % 3 == 0:
        t.append(l[i])
    elif i % 3 == 1:
        t.append(l[i] & (2 ** 32 - 1))
        t.append(l[i] >> 32)
    else:
        t.append(l[i] & (2 ** 32 - 1))
        t.append(l[i] & (2 ** 64 - 1) >> 32)
        t.append(l[i] >> 64)
rc = RandCrack()
for i in t:
    rc.submit(i)
flag = rc.predict_getrandbits(32)
print(md5(str(flag).encode()).hexdigest())
```



flag: GKCTF{14c71fec812b754b2061a35a4f6d8421}