

队员信息：(两人均是21级的)

00:21 4G

MayCTF群英萃团队赛...

MayCTF群英萃团队赛报名(whu校内)

所收集信息仅用于颁发奖品和获奖等级评定

*01 队伍名(需与平台开放组队后一致)

GHOST

*02 队长姓名

邵子立

*03 队长学号

2021302181032

*04 队长平台id

GHOST_RUNNER

*05 成员1姓名

00:21 4G

MayCTF群英萃团队赛...

2021302181032

*04 队长平台id

GHOST_RUNNER

*05 成员1姓名

李浩威

*06 成员1学号

2021302181047

*07 成员1平台id

h1Gw

*08 成员2姓名

无

Misc

checkin

已知部分明文求密文，因为 MD5 加密是不可逆的，目前我只知道可以使用Python脚本进行枚举

```
import hashlib

for i_1 in range(0, 10):
    for i_2 in range(0, 10):
        for i_3 in range(0, 10):
            for i_4 in range(0, 10):
                for i_5 in range(0, 10):
                    for i_6 in range(0, 10):
```

```

        m = hashlib.md5() # 获取一个md5加密算法对象
        data = '2021302181171' + str(i_1) + str(i_2) + str(i_3)
+ str(i_4) + str(i_5) + str(i_6)
        # str('flag{HELLO WOR' + chr(i) + chr(j) +
'}`).encode("utf-8")

        m.update(str(data).encode("utf-8")) # 指定需要加密的字符串
        des = m.hexdigest()
        # print(str(i_1) + str(i_2) + str(i_3) + str(i_4) +
str(i_5) + str(i_6))

        if '634f90dc3b212d7949f7657c4a364cb4' == des: # 如果得到
的密文和我们预期的密文相同，输出
            print("data=", data)

```

得出明文后六位应该是

972513

学号+972513进行加密，即可得正确的密文

Crypto

step_in

参考了[2020网鼎杯——you raise me up wp](#)

```

from sympy.ntheory import discrete_log
n = 2**1024
m =
19473863756169470216761513717236231215537697743280372251145129313170008427811446
42944904132739525026774788221127352473409532158124805138997426576869162611724306
28488015507273737520911418908585278744866428986492445201257768328597616260723438
01861069206446551492487339982849621512669210425077834208295662160941
c =
42600578249269264816831356985803772347081052915069067787463640413224330471170684
30483193699930263536116297913101333432636354987592239330410816729392795295912503
37958894961260757000586241027509169480926810654624716224368237688523524710155569
80024242505342426801194296670293552172829288531216875890099304565341
flag_dec = discrete_log(n,c,m) #得到flag的十进制值
print(hex(flag_dec)) #转为十六进制后打印出来

```

结果为：

0x6d61796374667b3534767372302d62747935342d6264746274352d6274726266682d6274747368
74617d74736874617d

然后十六进制转字符串：

```
>>> import base64
>>> hex_str
='6d61796374667b3534767372302d62747935342d6264746274352d6274726266682d6274747368
74617d'
>>> print(base64.b16decode(hex_str.upper()))
b'mayctf{54vsr0-bty54-bdtbt5-btrbfh-bttshta}'
```