WP

midRSA

直接m0左移208位后用long_to_bytes函数得到flag

```
from Crypto.Util.number import long_to_bytes
m0=13292147408567087351580732082961640130543313742210409432471625281702327748963274496942276607
m=m0<<208
flag = long_to_bytes(m)
print("flag: {flag}")
```

backpack

分析代码，可以观察到 `enc` 是通过对 `flag` 进行异或得到， `p` 通过对一组素数 `a` 进行位运算得到。所以想要得到flag，就需要通过p对enc进行逆运算。要做到还原 `p` ，首先是通过对 `bag` 进行逆操作，逐位还原 `p` 的二进制表示。然后就可以使用还原的 `p` 对 `enc` 进行解密，得到 `flag` 。

```
from Crypto.Util.number import long_to_bytes

enc = 871114172567853490297478570113449366988793760172844644007566824913350088148162949968812541218339
a = [3245882327, 3130355629, 2432460301, 3249504299, 3762436129, 3056281051, 3484499099, 2830291609, 3349739489, 2847095593, 3532332619, 2406839203, 4056647633, 3204059951, 3795219419, 3240880339, 2668368499, 4227862747, 2939444527, 3375243559]
bag = 45893025064

p = 0
for i in range(32):
    bit = bag & 1
    p = p | (bit << i)
    bag = bag >> 1

flag = enc ^ p
flag = long_to_bytes(flag)
print(flag)
```