Chapter 7

密码学 CTF 练习

此部分题目来源于`https://buuoj.cn`。此练习的评价不使用编程类练习的评价标准，按照你提交的 writeup 进行评分。

此部分练习最终以课程群里发布的练习压缩包为准。

7.1 Alice 与 Bob

密码学历史中，有两位知名的杰出人物，Alice 和 Bob。他们的爱情经过置换和轮加密也难以混淆，即使是没有身份认证也可以知根知底。就像在数学王国中的素数一样，孤傲又热情。下面是一个大整数:98554799767, 请分解为两个素数，分解后，小的放前面，大的放后面，合成一个新的数字，进行 md5 的 32 位小写哈希，提交答案。

注意：得到的 *flag* 请包上 *flag* 提交。

7.2 MD5

e00cf25ad42683b3df678c61f42c6bda

7.3 RSA

在一次 RSA 密钥对生成中，假设 p=473398607161，q=4511491，e=17

求解出 d 作为 flga 提交

7.4 RSA1

p = 86376337672570085670996534865410911713204915094336154475391624379112441758856678063984117905240835534451581135022277452062053276909395040329946999020532 29

q = 12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469

dp = 6500795702216834621109042351193261530650043841056252930930949663358625016881832840728066026150264693076109354874099841380454881716097778307268116910582929

dq = 783472263673553449019532580386470672380574033551303889137911760438881683674556098098256795673512201963002175438762767516968043599582527539160811120550041

c = 24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073530437657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852

7.5 rsarsa

Math is cool! Use the RSA algorithm to decode the secret message, c, p, q, and e are parameters for the RSA algorithm.

p = 964842302901051567659055174001042653494573763923573980064398935203985250729849139956103500916342705037010757073363335091169128029777160200625281665378483

q = 11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647903887510065547947313543299303261986053486569407

e = 65537

c = 83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576486526217457006376842280869728581726746401583705899941768214138742259689334840735633553053887641847651173776251820293087212885670180367406807406765923638973161375817392737747832762751690104423869019034

Use RSA to find the secret message

7.6 丢失的 MD5

md5.py 内容为：

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM')
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print des
```

md5.py