

## 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。

### 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

$p = 8637633767257008567099653486541091171320491509433615447539$   
162437911244175885667806398411790524083553445158113502227745206  
205327690939504032994699902053229

```
q = 12640674973996472769176047937170883420927050821480010581593137
1353724738805956137373376306297525773461470392840300825934907766
30572584959954205336880228469
dp = 65007957022168346211090423511932615306500438410562529
3093094966335862501688183284072806602615026469307610935487
4099841380454881716097778307268116910582929
dq = 78347226367355344901953258038647067238057403355130388913
7911760438881683674556098098256795673512201963002175438762767
516968043599582527539160811120550041
c = 247223054038873820735673164676490806626315529059602293
9907910799560215441817605633580063888752761416407353043765
7085079676157350205351945222989351316076486573599576041978
3398722659250627643185360890073102702785261596789374319038
6289240074791552511898395997060793414297473667578432599344
5942031372107342103852
```

## 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 = 964842302901051567659055174001042653494573763923573
98006439893520398525072984913995610350091634270503701075
70733633350911691280297777160200625281665378483
q = 11874843837980297032092405848653656852760910154543380907
6500401907042833589092085782510630477324439922306479038875100
65547947313543299303261986053486569407
e = 65537
c = 83208298995174604174773590298203639360540024871256126892889
6613457424033149298619391004926666056473166465764865262174570063
7684228086972858172674640158370589994176821413874225968933484073
5633553053887641847651173776251820293087212885670180367406807406
765923638973161375817392737747832762751690104423869019034
```

Use RSA to find the secret message

## 7.6 丢失的 MD5

md5.py 内容为:

```
1 import hashlib
2 for i in range(32,127):
3     for j in range(32,127):
4         for k in range(32,127):
5             m=hashlib.md5()
6             m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJX'+chr(k)+'ZM')
7             des=m.hexdigest()
8             if 'e9032' in des and 'da' in des and '911513' in des:
9                 print des
```

md5.py

