## 13.Alice与Bob（分解质因数，哈希加密）

题目：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

由题目可知，需要将给出的数进行分解质因数并哈希加密得到答案

首先编写分解质因数的python代码并运行：

```shell

import sympy

def factorize(n):

    factors = sympy.factorint(n)

    return factors

if \_\_name\_\_ == "\_\_main\_\_":

    n = int(input("请输入一个整数："))

    factors = factorize(n)

    print(f"{n} 的质因数分解结果：{factors}")

```

在python编译器上运行代码输出结果为：

请输入一个整数：98554799767

98554799767 的质因数分解结果：{101999: 1, 966233: 1}

得到分解质因数的两个结果101999和966233，按照小的放前面，大的放后面组合得到：101999966233

随后编写哈希加密代码：

```shell

import hashlib

def md5\_encrypt(text):

    md5\_obj = hashlib.md5()

    md5\_obj.update(text.encode('utf-8'))

    md5\_hash = md5\_obj.hexdigest()

    return md5\_hash

if \_\_name\_\_ == "\_\_main\_\_":

    n = input("请输入要加密的字符串：")

    print(md5\_encrypt(n))

```

在python编译器上运行代码输出结果为：

请输入要加密的字符串：101999966233

d450209323a847c8d01c6be47c81811a

在结果加上flag形式即可得到flag：

flag{d450209323a847c8d01c6be47c81811a}

## 14.大帝的密码武器（凯撒密码）

打开题目给出以下信息：

题目

公元前一百年，在罗马出生了一位对世界影响巨大的人物，他生前是罗马三巨头之一。他率先使用了一种简单的加密函，因此这种加密方法以他的名字命名。

以下密文被解开后可以获得一个有意义的单词：FRPHEVGL

你可以用这个相同的加密向量加密附件中的密文，作为答案进行提交。

密文

ComeChina

根据提示一眼盯真为凯撒密码，把FRPHEVGL放到随波逐流里，在凯撒解码偏移量为13时发现有意义的单词：

mode1 #13: SECURITY

那么在凯撒在线加密工具用相同的加密向量13加密密文ComeChina得到：

PbzrPuvan

加上flag形式得到flag：

flag{PbzrPuvan}

## 15.rsarsa（已知pqec逆元解密）

打开题目给出以下信息：

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

p =  9648423029010515676590551740010426534945737639235739800643989352039852507298491399561035009163427050370107570733633350911691280297777160200625281665378483

q =  11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647903887510065547947313543299303261986053486569407

e =  65537

c =  83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576486526217457006376842280869728581726746401583705899941768214138742259689334840735633553053887641847651173776251820293087212885670180367406807406765923638973161375817392737747832762751690104423869019034

Use RSA to find the secret message

已知p、q、e、c的情况下求逆元解密

编写代码：

```shell

import gmpy2

E = 65537

c = 83208298995174604174773590298203639360540024871256126892889661345742403314929861939100492666605647316646576486526217457006376842280869728581726746401583705899941768214138742259689334840735633553053887641847651173776251820293087212885670180367406807406765923638973161375817392737747832762751690104423869019034

p = 9648423029010515676590551740010426534945737639235739800643989352039852507298491399561035009163427050370107570733633350911691280297777160200625281665378483

q = 11874843837980297032092405848653656852760910154543380907650040190704283358909208578251063047732443992230647903887510065547947313543299303261986053486569407

N = p\*q

D = int(gmpy2.invert(E,(p-1)\*(q-1)))

#求逆元

message = gmpy2.powmod(c,D,N)

#使用密钥解密

print(message)

```

将代码在python编译器上运行得到结果：

5577446633554466577768879988

加上flag的形式得到flag：

flag{5577446633554466577768879988}

## 16.Windows系统密码（MD5哈希解密）

打开题目给出几段编码：

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

SUPPORT\_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::

根据编码形式可以推断出是MD5哈希加密，将编码一段一段放入到MD5在线解码工具中，发现a7fcb22a88038f35a8f39d503e7f0062这一段能够成功解密出结果，加上flag形式即可得到flag：

flag{good-luck}