## 17信息化时代的步伐（中文电报码）

题目简介：也许中国可以早早进入信息化时代，但是被清政府拒绝了。附件中是数十年后一位伟人说的话的密文。请翻译出明文(答案为一串中文！) 注意：得到的 flag 请包上 flag{} 提交

打开题目给出一段编码：

606046152623600817831216121621196386

目前看不出是什么编码，直接放到随波逐流里，发现有一种解码为中文：

中文电报码解码:        计算机要从娃娃抓起

加上flag形式提交：

flag{计算机要从娃娃抓起}

## 18.凯撒？替换？呵呵!（变异凯撒密钥替换）

题目：

MTHJ{CUBCGXGUGXWREXIPOYAOEYFIGXWRXCHTKHFCOHCFDUCGTXZOHIXOEOWMEHZO} 注意：得到的 flag 请包上 flag{} 提交, flag{小写字母}

可以看到编码形式与flag及其相似，把编码直接放到随波逐流里，在凯撒解密中没有发现flag，那么根据题目提示编码开头的MTHJ为替换flag的密钥

把编码放入到quipqiup在线密码解算器（https://www.quipqiup.com/）中，在密钥栏中输入MTHJ=flag，在第0项结果中有正确的英文语句：

0   -2.029  flag substitution cipher decryption is always easy just like a piece of cake

变换成flag形式提交：

flag{substitutioncipherdecryptionisalwayseasyjustlikeapieceofcake}

## 19. 萌萌哒的八戒（猪圈密码）

打开题目，给出了一张jpg图片文件，题目提示：

萌萌哒的八戒原来曾经是猪村的村长，从远古时期，猪村就有一种神秘的代码。请从附件中找出代码，看看萌萌哒的猪八戒到底想说啥 注意：得到的 flag 请包上 flag{} 提交

根据提示可以推断出本题使用了猪圈密码，图片上给出了密码的编码形式，找到一个猪圈密码在线解密工具，依次输入编码，最终得到解码：

whenthepigwanttoeat

加上flag形式提交：

flag{whenthepigwanttoeat}

## 20.权限获得第一步（32位MD5哈希解密）

题目：你猜这是什么东西，记得破解后把其中的密码给我。答案为非常规形式。 注意：得到的 flag 请包上 flag{} 提交

打开题目跳转到一个网页，给出一段字符串：

Administrator:500:806EDC27AA52E314AAD3B435B51404EE:F4AD50F57683D4260DFD48AA351A17A8:::

可以看到编码F4AD50F57683D4260DFD48AA351A17A8形式为32位MD5哈希加密，将其放入MD5在线解密工具，得到：

3617656

加上flag提交：

flag{3617656}

## 21.RSA1（已知pqcdpdq求d并解密）

打开题目，给出以下信息：

p = 8637633767257008567099653486541091171320491509433615447539162437911244175885667806398411790524083553445158113502227745206205327690939504032994699902053229

q = 12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469

dp = 6500795702216834621109042351193261530650043841056252930930949663358625016881832840728066026150264693076109354874099841380454881716097778307268116910582929

dq = 783472263673553449019532580386470672380574033551303889137911760438881683674556098098256795673512201963002175438762767516968043599582527539160811120550041

c = 24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073530437657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852

题目还是RSA加密算法，已知p、q、c、dp、dq求d并解密明文。编写代码实现：

```shell

import gmpy2

p = 8637633767257008567099653486541091171320491509433615447539162437911244175885667806398411790524083553445158113502227745206205327690939504032994699902053229

q = 12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469

c = 24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073530437657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852

dp = 6500795702216834621109042351193261530650043841056252930930949663358625016881832840728066026150264693076109354874099841380454881716097778307268116910582929

dq = 783472263673553449019532580386470672380574033551303889137911760438881683674556098098256795673512201963002175438762767516968043599582527539160811120550041

I = gmpy2.invert(p, q)

m\_p = gmpy2.powmod(c, dp, p)

m\_q = gmpy2.powmod(c, dq, q)

m = ((I\*(m\_p-m\_q))%q)\*p+m\_p

print(hex(m))

```

运行代码得到结果：

0x6e6f784354467b57333163306d335f37305f4368316e343730776e7d

结果为一个16进制编码，将其放入到16进制到文本字符串在线工具（https://www.bejson.com/convert/ox2str/）转换一下得到：

noxCTF{W31c0m3\_70\_Ch1n470wn}

变换为flag形式提交：

flag{W31c0m3\_70\_Ch1n470wn}