## 一眼就解密（base64编码）

题目给出一串字符，并提示解密后便能获得flag：

ZmxhZ3tUSEVfRkxBR19PRl9USElTX1NUUklOR30=

根据“=”字符结尾的特征大致可以推断出是使用了base64编码，为了方便我们直接将这段字符串放到随波逐流CTF工具或者BP的base64解码工具

得到base64的解码即为flag:

flag{THE\_FLAG\_OF\_THIS\_STRING}

## MD5

题目给出一个压缩包，下载下来后里面有有一个txt文件，其中有一段编码：

e00cf25ad42683b3df678c61f42c6bda

根据题目提示这个字符串为MD5编码，使用随波逐流CTF工具或者线上的MD5解码工具解码即可得到:

admin1

加上flag的样式即为本题的flag：

flag{admin1}

## 3.Url编码

题目给出一个压缩包，下载下来后里面有有一个txt文件，其中有一段编码：

%66%6c%61%67%7b%61%6e%64%20%31%3d%31%7d

根据题目提示这个字符串为URL编码，使用BP的URL解码工具解码即可得到flag:

flag{and 1=1}

## 4.看我回旋踢（Rot回旋编码）

题目给出一个压缩包，下载下来后里面有有一个txt文件，其中有一段编码：

synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

该编码形式与flag极为相似，直接放进随波逐流CTF解码工具，得到两个flag形式：

Rot13解码:        flag{5cd1004d-86a5-46d8-b720-beb5ba0417e1}

Rot18解码:        flag{0cd6559d-31a0-91d3-b275-beb0ba5962e6}

提交发现第一个Rot13（回转13位）解码即为本题的flag

## 5.摩丝（摩斯密码）

题目给出一个压缩包，下载下来后里面有有一个txt文件，其中有一段编码：

.. .-.. --- ...- . -.-- --- ..-

根据题目名称提示可知，这就是著名的，摩斯密码，使用线上摩斯密码解码工具解码可得：

ILOVEYOU

加上flag形式即可得到flag：

flag{ILOVEYOU}

## 6.password

打开下载的压缩文件，有这样几段字符串：

   գ 19900315

key  ʽΪkey{xxxxxxxxxx}

其中有数个特殊字符无法显示

这样看来没有什么头绪，后来查资料发现貌似是显示的问题，显示正确的题目是：

姓名：张三

生日：19900315

key格式为key{xxxxxxxxxx}

这样发现key的大括号内有10位，刚好对应姓名2位和生日8位，根据题目提示可知是典型的将姓名首字母与生日结合设置的密码，这种密码在生活中很常见

加上flag形式等得到flag:

flag{zs19900315}

## 7.变异凯撒

打开题目的txt文件给出以下信息：

加密密文：afZ\_r9VYfScOeO\_UL^RWUc

格式：flag{ }

由题目名称提示可知密文使用了凯撒加密，但是不知道其移位是多少，将密文放进随波逐流CTF工具，在移位为5的凯撒解码发现flag：

flag{Caesar\_variation}

## 8.Quoted-printable（“=”）

打开题目给出一串编码：

=E9=82=A3=E4=BD=A0=E4=B9=9F=E5=BE=88=E6=A3=92=E5=93=A6

根据题目名称提示可知，该编码使用了Quoted-printable编码

通过查阅资料可知，Quoted-Printable编码可译为“可打印字符引用编码”，或者“使用可打印字符的编码”。通常我们接收电子邮件，查看电子邮件原始信息，经常会看到这种类型的编码。

例如：ASCII码换页符（十进制值为12）可以表示为”=0C”。

除了可打印ASCII字符与换行符以外，所有字符必须表示为这种格式。

将编码放入随波逐流CTF工具中，得到：

Quoted解码:       那你也很棒哦

加上flag形式即可得到flag：

flag{那你也很棒哦}