我也刚学有个例子给你看看，很有用：

RSA算法总结如下：

求两个素数P和q

取n=P*q

取t=(p-)。

取任意数e，求满足et和e与t的互质(即最大公因数为1)

取d*e%t==1

从而最终得到三个数：nde

集合音频。

Setc=(M**d)%n获得加密音频c

Setm=(c**e)%n使m==M，从而完成c的解密

注：**代表幂，下面两个公式中的D和E可以互换。

在加密中：

nd两个数组成一个公钥，可以通知别人；

ne的两个数组成一个私钥，e自己保管，不让任何人知道。

发送给他人的音频由e加密。只要别人能用D解锁，就能证明音频是你发的，形成签名机制。

别人给你发音频，用的是D加密，所以你只有有E

才能解密。公共公钥系统有两个主要功能：加密消息和认证。。因为这个方式，我&#039；我会给你链接。请参考一下.众所周知的

公钥和私钥俗称非对称加密，是对之前对称加密(使用用户名和密码)的改进。通过邮件解释原理

使用公钥和私钥的技巧是完成一封安全的电子邮件，必须像进入手腕一样完成：

1。我发给你的方式一定要加密，在邮件传输过程中不能被别人看到。

2。确保我发了邮件。没有其他人在假扮我。

要达到这样的手段，发送邮件的两个人都必须有一个公钥和一个私钥。

公钥自己用。可以通过邮件发布，让别人通过网站下载。公钥实际上用于加密/戳验证。。私钥，是你自己的，一定要非常小心的保管，最好加密码。私钥用于解密/签名。首先，就密钥的所有权而言，私钥只需要归组所有即可。公钥和私钥的作用是：用公钥加密的表单只能用私钥解密，用私钥加密的表单只能用公钥解密。。

比如我想给你发一封加密的邮件。第一，我必须有你的公钥，你也必须有我的公钥。

首先，我用你的公钥加密这封邮件，这样可以保证这封邮件不会被别人看到。并确保此邮件在传输过程中没有被修改。收到邮件后，可以用自己的私钥解密，看内容。

其次，我用我的私钥加密这封邮件，发给你后，你可以用我的公钥解密。因为私钥只需要在我手里这确保了这封邮件是我发的。

A-B数据加密时，A会使用B&#039；s公钥，从而保证只要B就可以解密，否则一般公众都可以解密加密的消息，这就意味着数据的保密性被解除。考证就是利用签验印章的机制。当A把材料发给自己的时候，会用自己的私钥签名，这样所有收到消息的人就可以不用再用A检查印章了&#039；的公钥，然后他们可以确认消息是由.

这是一套保证网络传输安全的加密系统。每个社区都有一组公钥和私钥。公钥可以通过证书下载传输，通知很多人；私钥由用户自己保管。当传输停止时，发送方使用接收方的公钥停止加密数据，以确保传输数据的机密性。同时用自己的私钥停止加密，保证传输数据的真实性——肯定是自己发来的。接收到数据后，接收方用自己的私钥停止解密和校验数据——因为是用自己的公钥加密的，只要自己的私钥能被解密。与此同时，发送者&#039；的公钥对其进行解密，从而确认该资料确实是由私钥持有者恢复的，从而保证了资料的准确性。这样传输的数据也是有法律效力

的！

公钥和私钥成对生成，用于非对称加密算法

主要有两个用途：

1。私钥加密，公钥解密

这种方法用于数字签名，不可接受。因为密钥在你手里，用B密钥和A公钥签名的数据可以&#039；解决不了。相反，它只需要是用a的公钥解密的数据。，这意味着数据是用私钥签名的。

2。公钥加密，私钥解密

公布公钥，每个组都可以把用这个公钥加密的文件发给你，即使数据在途中被截获，也可以&#039；没有我的私人钥匙是无法破解的；

我这么说你应该清楚了吧？

应该给加分。

公钥和私钥是一个算法丢失的密钥对(即公钥和私钥)，其中一个被公开，称为公钥；另一个是自己保管的，叫私钥。。这种算法丢失的密钥对可以保证在世界上是唯一的。使用这个密钥对时，假设一段数据用一个密钥加密，必须用另一个密钥解密。例如，如果数据用公钥加密，就必须用私钥解密，如果用私钥加密，也必须用公钥解密。