一、公钥加密

假设一下，我找了两个数字，一个是1，一个是2。我喜欢2这个数字，就保留起来，不告诉你们(私钥），然后我告诉大家，1是我的公钥。

我有一个文件，不能让别人看，我就用1加密了。别人找到了这个文件，但是他不知道2就是解密的私钥啊，所以他解不开，只有我可以用

数字2，就是我的私钥，来解密。这样我就可以保护数据了。

我的好朋友x用我的公钥1加密了字符a，加密后成了b，放在网上。别人偷到了这个文件，但是别人解不开，因为别人不知道2就是我的私钥，

只有我才能解密，解密后就得到a。这样，我们就可以传送加密的数据了。

二、私钥签名

如果我用私钥加密一段数据（当然只有我可以用私钥加密，因为只有我知道2是我的私钥），结果所有的人都看到我的内容了，因为他们都知

道我的公钥是1，那么这种加密有什么用处呢？

但是我的好朋友x说有人冒充我给他发信。怎么办呢？我把我要发的信，内容是c，用我的私钥2，加密，加密后的内容是d，发给x，再告诉他

解密看是不是c。他用我的公钥1解密，发现果然是c。

这个时候，他会想到，能够用我的公钥解密的数据，必然是用我的私钥加的密。只有我知道我得私钥，因此他就可以确认确实是我发的东西。

这样我们就能确认发送方身份了。这个过程叫做数字签名。当然具体的过程要稍微复杂一些。用私钥来加密数据，用途就是数字签名。

总结：公钥和私钥是成对的，它们互相解密。

公钥加密，私钥解密。

私钥数字签名，公钥验证。

举例

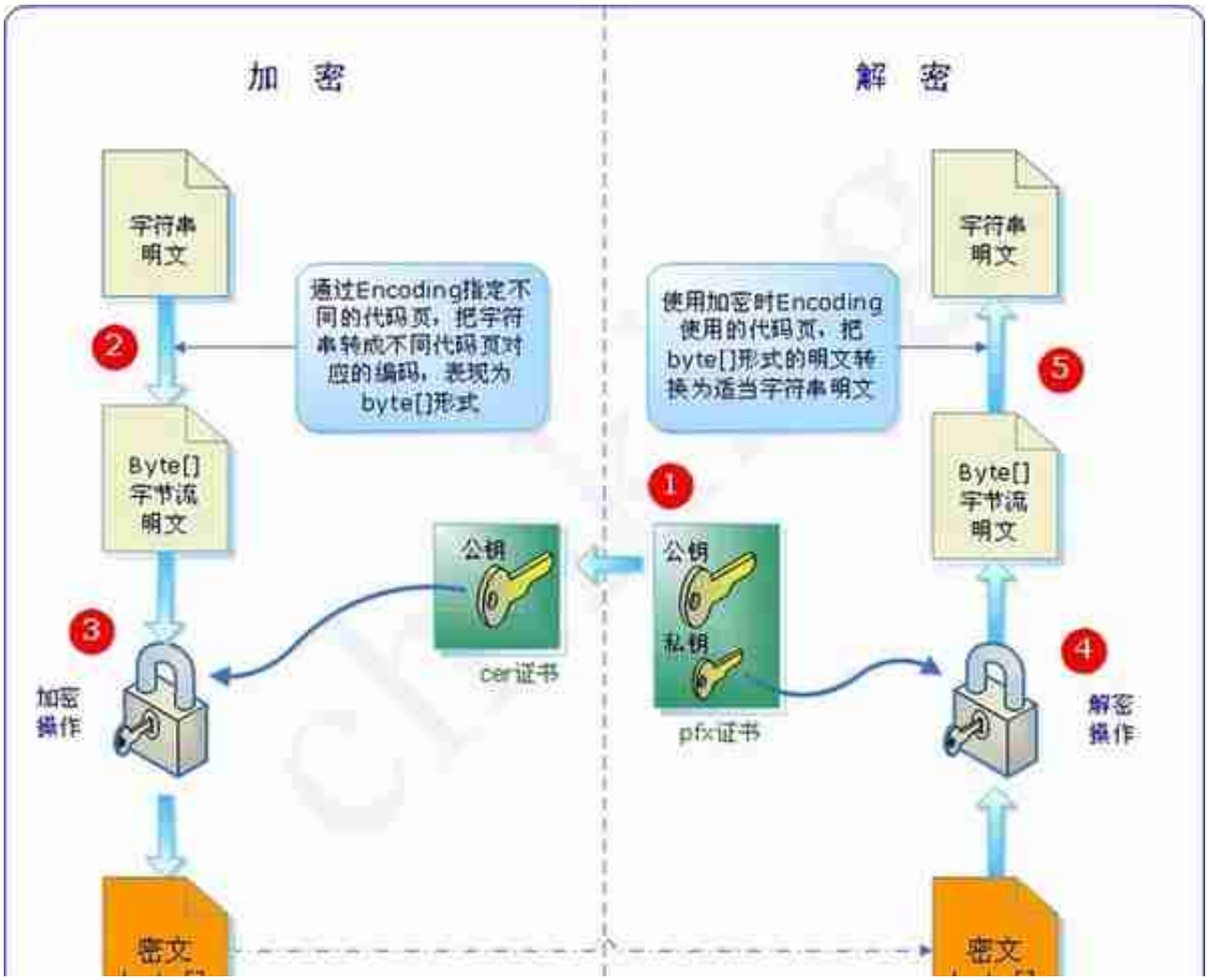
比如有两个用户Alice和Bob，Alice想把一段明文通过双钥加密的技术发送给Bob，Bob有一对公钥和私钥，那么加密解密的过程如下：

Bob将他的公开密钥传送给Alice。

Alice用Bob的公开密钥加密她的消息，然后传送给Bob。

Bob用他的私人密钥解密Alice的消息。

上面的过程可以用下图表示，Alice使用Bob的公钥进行加密，Bob用自己的私钥进行解密。



原文链接：https://blog.csdn.net/21aspnet/article/details/7249401