我们来回顾一下RSA的加密算法。我们从公钥加密算法和签名算法的定义出发，用比较规范的语言来描述这一算法。

RSA公钥加密体制包含如下3个算法：KeyGen（密钥生成算法），Encrypt（加密算法）以及Decrypt（解密算法）。

A screenshot of a cell phone

Description automatically generated所以，从算法描述中我们也可以看出：**公钥用于对数据进行加密，私钥用于对数据进行解密**。当然了，这个也可以很直观的理解：公钥就是公开的密钥，其公开了大家才能用它来加密数据。私钥是私有的密钥，谁有这个密钥才能够解密密文。否则大家都能看到私钥，就都能解密，那不就乱套了。

=================分割线=================

我们再来回顾一下RSA签名体制。签名体制同样包含3个算法：KeyGen（密钥生成算法），Sign（签名算法），Verify（验证算法）。

A screenshot of a cell phone

Description automatically generated所以，在签名算法中，**私钥用于对数据进行签名，公钥用于对签名进行验证**。这也可以直观地进行理解：对一个文件签名，当然要用私钥，因为我们希望只有自己才能完成签字。验证过程当然希望所有人都能够执行，大家看到签名都能通过验证证明确实是我自己签的。

=================分割线=================

那么，为什么题主问这么一个问题呢？我们可以看到，RSA的加密/验证，解密/签字过程太像了。同时，RSA体制本身就是对称的：如果我们反过来把e看成私钥，d看成公钥，这个体制也能很好的执行。我想正是由于这个原因，题主在学习RSA体制的时候才会出现这种混乱。那么解决方法是什么呢？建议题主可以学习一下其他的公钥加密体制以及签名体制。其他的体制是没有这种对称性质的。举例来说，公钥加密体制的话可以看一看ElGamal加密，以及更安全的Cramer-Shoup加密。签名体制的话可以进一步看看ElGamal签名，甚至是BLS签名，这些体制可能能够帮助题主更好的弄清加密和签名之间的区别和潜在的联系。

至于题主问的加密和签名是怎么结合的。这种体制叫做签密方案（SignCrypt），RSA中，这种签密方案看起来特别特别像，很容易引起混乱。在此我不太想详细介绍RSA中的加密与签字结合的方案。我想提醒题主的是，加密与签字结合时，两套公私钥是不同的。

A picture containing text, whiteboard, person

Description automatically generated