#### 腾讯---什么是对称加密，什么是非对称加密，公钥与私钥属于对称加密吗

本专栏专注分享大型Bat面试知识，后续会持续更新，喜欢的话麻烦点击一个star

**面试官: 什么是对称加密，什么是非对称加密，公钥与私钥属于对称加密吗**

**心理分析**：密码学一般是大学计算机专业学的，面试官在靠这个问题的时候 并不会深入密码学底层的内容，知识考到对称与非对称的区别。这个问题一般不会深入问道，但是会问道关于https，https目前使用了非对称加密。但是求职者千万别陷入坑中，说没听过对称与非对称。

**求职者:**应该从 加解密入手

公钥和私钥就是俗称的不对称加密方式，是从以前的对称加密（使用用户名与密码）方式的提高。我用电子邮件的方式说明一下原理。 使用公钥与私钥的目的就是实现安全的电子邮件，必须实现如下目的： 1. 我发送给你的内容必须加密，在邮件的传输过程中不能被别人看到。 2. 必须保证是我发送的邮件，不是别人冒充我的。 要达到这样的目标必须发送邮件的两人都有公钥和私钥。 公钥，就是给大家用的，你可以通过电子邮件发布，可以通过网站让别人下载，公钥其实是用来加密/验章用的。私钥，就是自己的，必须非常小心保存，最好加上密码，私钥是用来解密/签章，首先就Key的所有权来说，私钥只有个人拥有。公钥与私钥的作用是：用公钥加密的内容只能用私钥解密，用私钥加密的内容只能用公钥解密。 比如说，我要给你发送一个加密的邮件。首先，我必须拥有你的公钥，你也必须拥有我的公钥。 首先，我用你的公钥给这个邮件加密，这样就保证这个邮件不被别人看到，而且保证这个邮件在传送过程中没有被修改。你收到邮件后，用你的私钥就可以解密，就能看到内容。 其次我用我的私钥给这个邮件加密，发送到你手里后，你可以用我的公钥解密。因为私钥只有我手里有，这样就保证了这个邮件是我发送的。 当A->B资料时，A会使用B的公钥加密，这样才能确保只有B能解开，否则普罗大众都能解开加密的讯息，就是去了资料的保密性。验证方面则是使用签验章的机制，A传资料给大家时，会以自己的私钥做签章，如此所有收到讯息的人都可以用A的公钥进行验章，便可确认讯息是由 A 发出来的了