南開大學
Nankai University

网络空间安全学院

网络安全技术实验报告

数字签名工作原理分析

姓名：魏伯繁

学号：2011395

专业：信息安全

2023 年 5 月 7 日

目录

1 数字签名原理分析 **2**

1.1 数字签名基本原理 2

1.2 数字签名的作用 3

1.3 数字签名的缺点 3

1 数字签名原理分析

1.1 数字签名基本原理

加密通信和数字签名之间存在一定的相似性。在加密通信中，使用公钥将信息加密为密文，而私钥用于解密。另一方面，在数字签名中，则采用私钥加密来生成数字签名，而公钥则用于验证数字签名。这表明，在加密通信和数字签名中，各自包含了加密算法、解密算法、签名算法、以及验证算法，具有相似的对称性。

事实上，在加密通信中，利用加密算法将信息转换为密文，通过私钥解密算法进行解密。反之，在数字签名中，秘钥方案被用来生成数字签名，而公钥则被用来验证数字签名的有效性。由此可见，对称性存在于加密算法、解密算法、签名算法和验证算法之间。

数字签名主要的功能在于确认签名者的身份，这意味着让所有的参与者都明确确认数字签名是否是由私钥持有人创建的。数字签名是通过签名算法生成，签名算法需要两个输入，一个是私钥，另一个是要签署的信息，随后输出一个字符串作为数字签名。然而，要确认数字签名是否是由私钥持有人签署的，需要使用验证算法。验证算法会使用三个输入，一个是信息本身，另外一个是数字签名，第三个是公钥，输出的结果是确认是否验证成功或失败。因此，在数字签名的过程中，私钥作为“签名 key”，而公钥则是“验证 key”。

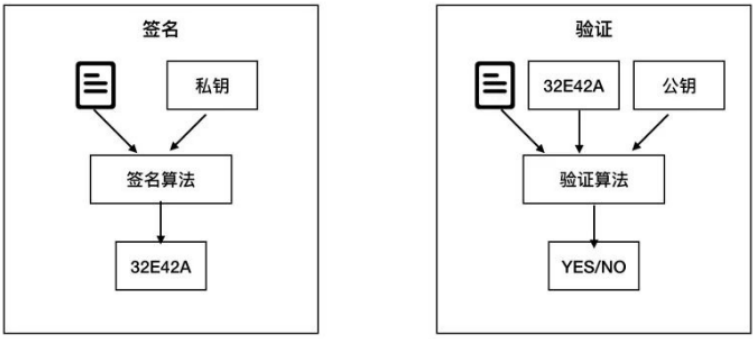

图 1.1

上面这张图片就已经把数字签名解释的非常清楚了，他的原理是由公钥密码体制引申而来的，也就是说：我要是签名，那么我加密的东西就可以是我的名字，这个东西就对应了需要验证的信息本身，然后我用私钥加密他，因为某一个小心是随着我的签名发出的，所以接收者只需要用公钥解密密文内容，看密文内容是不是我的名字就可以判断数字签名是否来源于我。下面这张图片就很好的解释了这个过程，假设 Alice 的签名是 A，那么其他人只需要用 Alice 的公钥去解秘密信息 32E42A 密然后比较解密结果和 A 是否相等就可以判定签名是否有效。

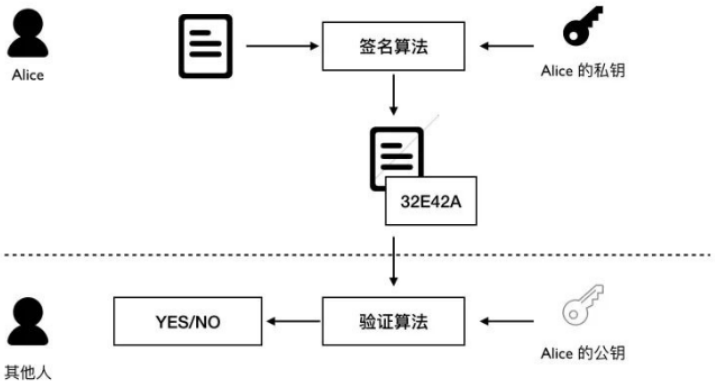

图 1.2

由此我们就可以很清楚的解释数字签名的工作原理，我为什么要相信这个东西是你发出来的呢?很简单，因为我用你的公钥解密一个秘密信息发现是你的专属认证，那么只有一种可能就是这个秘密信息是用和这个公钥对应的私钥加密而成的，但是私钥按理说只有对应的人才拥有，这就是数字签名的可信性来源也就是工作原理。

1.2 数字签名的作用

数字签名具有三大作用。首先，数字签名用于身份认证，即确认签署人的真实身份。这一功能与传统的纸笔签名相似。其次，数字签名可以防止抵赖，这也是纸笔签名的作用之一。一旦签署双方签署了合同，就必须承担相应的责任，因为签名本身是无法否认的。最后，数字签名保证了文件的完整性，防止篡改，而这是纸笔签名所无法实现的。在应用数字签名时，其验证过程与签名过程相似，需要两个输入，一个是私钥，另一个则是文件本身。当文件被篡改后，在验证过程中就会失败，从而保证了文件的完整性。类似于纸笔签名领域中的相关技术，例如在签订合同时覆盖被签署区域和加盖蜡封等，这些措施是为了避免篡改，从而保证了签名和文件的可信性。

1.3 数字签名的缺点

数字签名同样存在很多缺点，比如可能遭到中间人攻击，也就是我把秘密信息和其他的恶意文件一起发送，让别人误以为我的签名是针对恶意文件的而非针对源文件的，这个攻击是致命的，所以才会有后来的数字证书的出现来保证数字签名的正确性和唯一性。同样的，数字签名还必须处理时间戳的失效问题以及不能长期保存的问题，数字签名验证的准确性需要依赖时间，而时间戳可能会受到时钟漂移、伪造攻击等问题的影响，从而导致数字签名验证失败。