什么是证书？

如果你获取到的公钥是伪造的，那么不管你的签名算法多完美，也是会得到错误的结果。

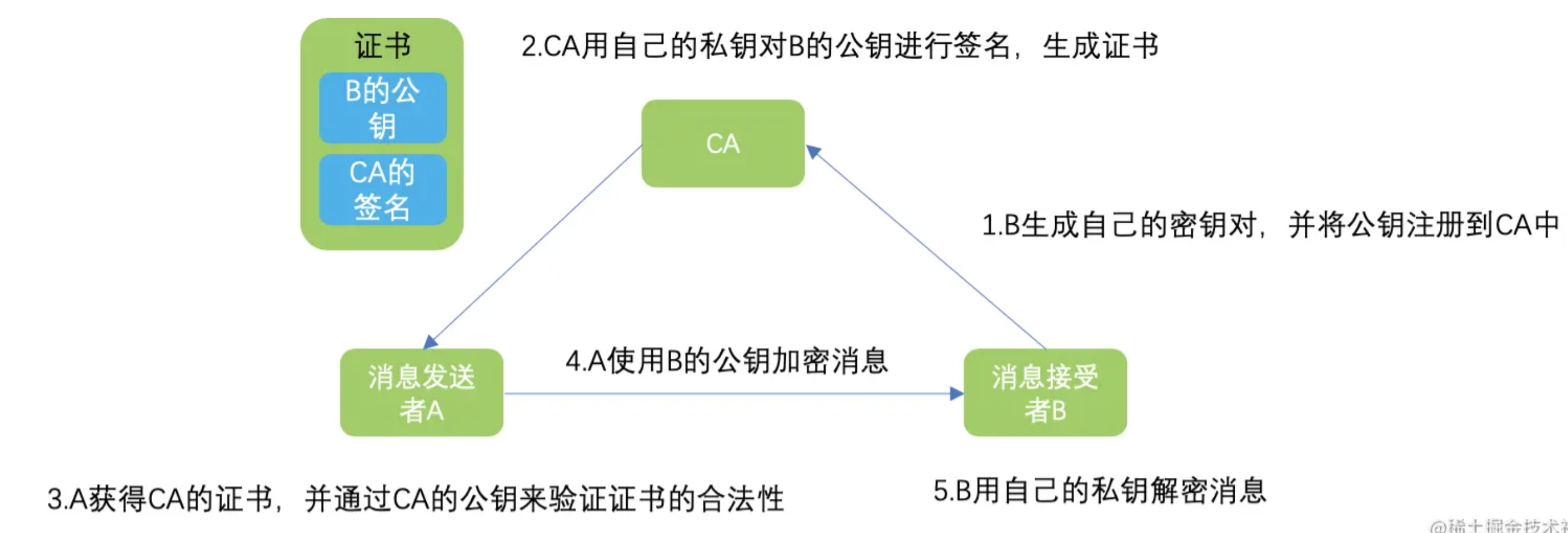
那么我们怎么才能安全的获得发送者的公钥呢？这里就需要使用到证书了。所谓证书就是通过第三方的可信机构对发送者的公钥进行签名而得到的。

这里有两个概念：公钥证书（Public-Key Certificate, PKC）和认证机构(Certification Authority, CA)。

证书的例子

我们看一个实际中可能会遇到的例子：

假如A要向B发送一条消息，这条消息希望使用B的公钥来加密，但是A事先无法知道B的公钥到底是什么，那么可以使用下面的证书架构：



在第一步，B需要生成自己的密钥对，然后将公钥注册到CA中。这里CA就是一个第三方的可信赖的机构。

CA获得到了B的公钥之后，使用自己的私钥对B的公钥进行签名，得到证书。

A从CA获得到证书和CA的公钥（CA是个可信赖机构，可以从公共站点中获取），并使用CA的公钥来验证证书签名的合法性。

A获得了B的公钥，使用B的公钥加密消息。

B用自己的私钥解密消息，得到明文。

证书的标准和生成

因为证书是由认证机构颁发的，使用者需要对其进行验证，那么就需要一个标准的证书格式来方便使用者使用。最广泛的一个证书标准格式是由ITU（International Telecommunication Union）和ISO(International Organization for Standardization)制定的X.509规范。

x.509有很多扩展格式包括：DER、CRT、CER、PEM等。他们在不同的环境中有不同的用处。

那么怎么生成证书呢？可以借助第三方工具，也可以使用命令行命令比如：openssl来生成。

PKI

有了证书的格式，是不是就可以实际使用证书了呢？

其实这还是不够的，我们还需要定义证书该由谁来颁发，如何颁发，如果作废证书等。而PKI(Public-Key Infrastructure)公钥基础设施就是为了有效的使用证书而制定的一系列规范和协议。

PKI的组成主要有三部分：

用户

用户是使用PKI的人，也就是需要借助CA来发布自己的公钥和获取别人公钥的人。

认证机构

认证机构就是CA了，它是对证书进行管理的人。CA除了生成证书之外，还有一个非常重要的工作就是作废证书。

因为用户有可能会丢失密钥，或者出于特殊的原因，废弃掉某些证书。那么就可以向CA发起一个作废请求。而作废的证书会被保存在CRL中。CRL就是对外的证书废弃列表。用户在使用证书的时候必须首先查看该证书是否在CRL列表中。如果在则该证书不能够被使用。

仓库

仓库是一个保存证书的数据库，用户注册之后生成的证书都存在仓库中，以供其他的用户获取使用。

CA的层级结构

我们从上面的介绍可以知道，其实CA不仅仅可以由机构来担任，任何人只要会对公钥进行签名都可以构建CA。

如果是一个很大的机构要构建CA，比如一个总公司要构建CA，那么它可以先构建一个root CA，然后再在root CA之下构建子CA，这些子CA来负责底层具体用户的证书颁发。

对证书的攻击

因为证书是基于数字签名技术，所以所有基于数字签名技术的攻击都适用于证书。

这里主要针对于PKI体系的攻击做个介绍：

在公钥注册之前替换公钥。

用户B如果想生成证书的话，需要在CA注册，并且将自己的公钥提交到CA。那么在公钥提交之前，可能会被恶意替换。

窃取认证机构的私钥

所有的用户公钥都是由CA的私钥做签名的，如果CA的私钥被盗的话，那么所有的证书都是不安全的。

CA其实是一个中心化的机构，中心化的机构往往都会出现这样的问题。攻破一个就攻破了所有。

伪装成认证机构

攻击者可以伪装成认证机构让用户上当。所以用户在注册的时候一定要小心。

CRL时间差攻击

如果B的密钥丢了，那么他会向CA提交一个废弃申请，但是在提交申请到申请生效，到CRL生成直接有一个时间差，这段时间内废弃的密钥仍然可以合法使用。