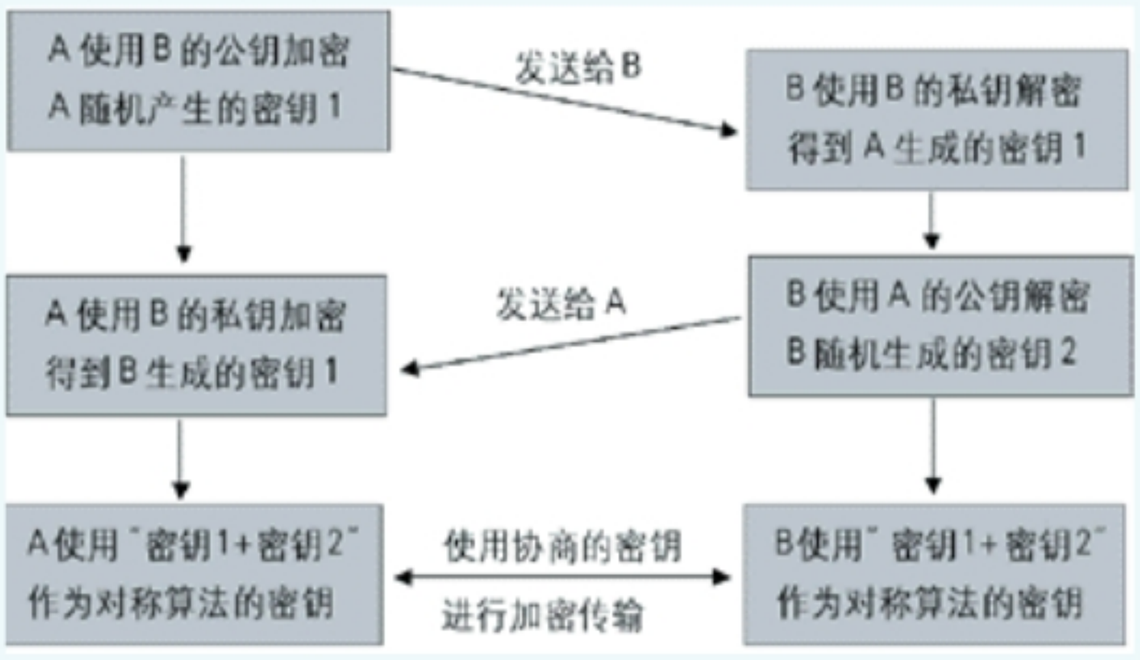
PKI 原理

作者：GONOW 2007-11-02 12:19:59

1976 年，Whitfield Diffie 和 Martin Hellman 提出了公开密钥理论，奠定了 PKI 体系的基础。PKI（Public Key Infrastructure 的缩写）即"公开密钥体系"，是一个利用现代密码学的公钥密码技术、并在开放的 Internet 网络环境中提供数据加密以及数字签名服务的、统一的技术框架。常用的公开密钥算法有 RSA、DSA 和 Diffie Hellman 等。使用公开密钥算法（又叫非对称加密算法）的用户同时拥有公钥和私钥。私钥不能通过公钥计算出来。私钥由用户自己持有，公钥可以明文发送给任何人，公开密钥理论解决了对称加密系统的密钥交换问题。

公钥加密/私钥解密完成对称算法密钥的交换：

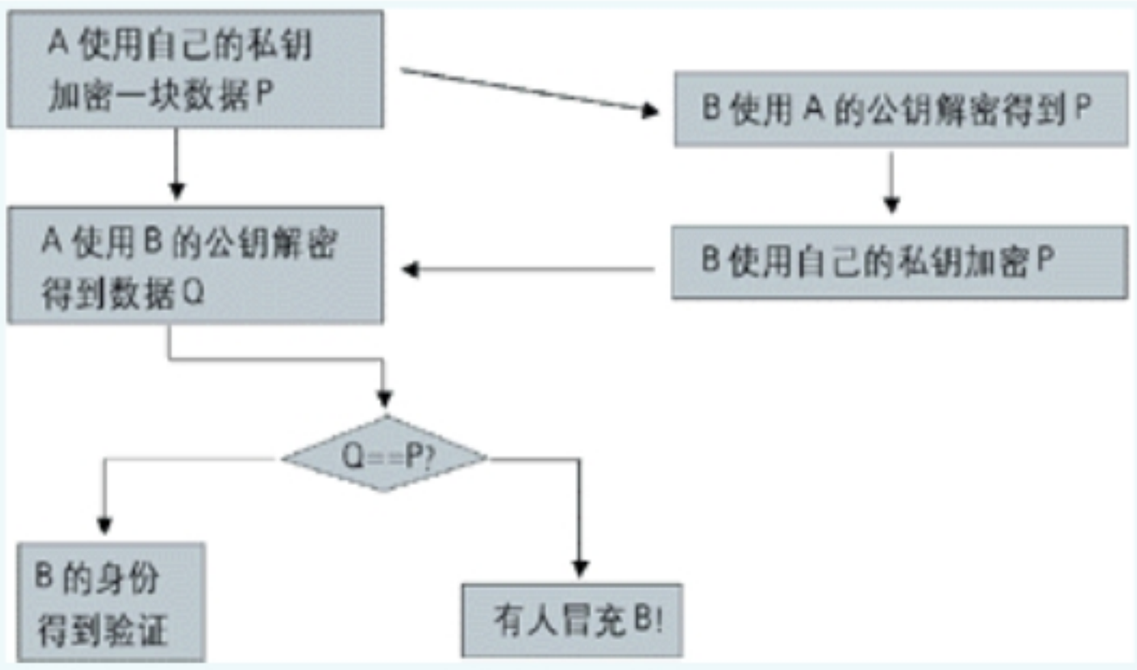
公开密钥算法的速度比对称算法慢得多，并且由于任何人都可以得到公钥，公开密钥算法对选择明文攻击很脆弱，因此公钥加密/私钥解密不适用于数据的加密传输。为了实现数据的加密传输，公开密钥算法提供了安全的对称算法密钥交换机制，数据使用对称算法加密传输。两个用户（A 和 B）使用公开密钥理论进行密钥交换的过程如下：



在对称算法密钥的协商过程中，密钥数据使用公钥加密。在保证私钥安全的前提下，攻击者即使截获传输的信息也不能得到加密算法的密钥，这就保证了对称算法密钥协商的安全性。

私钥加密/公钥解密完成身份验证、提供数字签名：

公开密钥算法可以实现通信双方的身份验证。下面是一个很简单的身份验证的例子（A 验证 B 的身份）：



同样的原理，公开密钥算法可以进行数据的签名和验证。A 需要对一块数据签名，A 只需要使用自己的私钥加密该数据就可以完成签名。A 把数据和数据签名（私钥加密的结果）一起发送给 B，B 使用 A 的公钥解密签名，然后和数据进行比较，如果相同则该签名确实是 A 签署的，并且数据没有被篡改。

同样是因为公开密钥的算法较慢，数据签名一般不直接使用私钥加密数据，而是加密数据的散列值。**数据块的散列值可以通过消息摘要算法计算得到**。消息摘要算法**实际上就是一个单向散列函数**。数据块经过单向散列函数得到一个固定长度的散列值，攻击者不可能通过散列值而编造数据块，使得编造的数据块的散列值和原数据块的散列值相同。**数据块的签名就是先计算数据块的散列值，然后使用私钥加密数据块的散列值得到数据签名**。签名的验证就是计算数据块的散列值，然后使用公钥解密数据签名得到另一个散列值，比较两个散列值就可以判断数据块在签名后有没有被改动。**常用的消息摘要算法有 MD5、SHA 等**。

公钥算法仍然要面对公钥分发、公钥/私钥密钥对与用户真实身份的绑定问题。 PKI 引入证书机制解决了这个问题。证书是由证书中心颁发。

用户在获得自己的身份证书后，就可以使用证书来表明自己的身份，接收方只需要使用签发证书的公钥验证用户证书，如果验证成功，就可以信任该证书描述的用户的身份。证书的签发/验证充分利用了公开密钥算法的数据签名和验证功能，杜绝了冒充身份的可能性。

PKI 的安全性分析

PKI 密钥交换和身份验证的安全性依赖于 PKI 使用的公开密钥算法、对称加密算法和消息摘要算法。

当前使用的公开密钥算法的安全性大都基于大数分解的难度。从一个公钥和密文中恢复出明文的难度等价于分解两个大素数的乘积。当前可以完成的大数分解的位数是 140 位。对于当前市场上广泛使用的 1024 位的 RSA 公开密钥算法来说，它被破解的可能性是微乎其微的。对于 128 位密钥来说，即使全世界的计算机同时进行群举攻击，破译 128 位密钥所需要的时间也是一个天文数字。对于消息摘要算法，单向散列函数的设计已经十分成熟。市场上广泛使用的 MD5、SHA 算法的散列值分别为 128、160 位，足以阻止所有的群举攻击的企图。由此看来，PKI 机制是一个成熟的、安全的技术。

PKI 技术的发展

基于 PKI 技术，人们又开发了很多的安全协议。其中最著名、应用最为广泛的是 SSL 和 SET 协议。

SSL（安全套接字）协议利用 PKI 技术来进行身份认证、完成数据加密算法及其密钥协商，很好地解决了身份验证、加密传输和密钥分发等问题。SSL 被大家广泛接受和使用，是一个通用的安全协议。在 SSL 协议上面可以运行所有基于 TCP/IP 的网络应用。

SET 安全电子交易协议采用公钥密码体制和 X.509 数字证书标准，主要应用于 BtoC 模式中保障支付信息的安全性。SET 协议是 PKI 框架下的一个典型实现，同时也在不断升级和完善。国外的银行和信用卡组织大都采用了 SET 协议。

PKI 原理 1

2007-03-23 09:25

在当今高度信息化、数字化的社会里，随着互联网的发展和信息技术的普及，人们已经开始习惯于通过各种先进的通信手段传递重要的数据、图像和话音等信息进行各种交流，网络给人们的工作和生活带来了前所未有的便利。同时，人们对网络和信息的安全性提出了越来越高的要求。然而，由于互联网所具有的广泛性和开放性，决定了互联网不可避免地存在着信息安全隐患。因此，信息的安全问题成为人们关注的焦点，引起了世界各国政府以及商业机构的高度重视。为了防范信息安全风险，许多新的安全技术和规范不断的出现，公钥基础设施 PKI(Public Key Infrastructure，简称 PKI)即是其中重要一员。

正如电子商务的基础设施之一是网络基础设施，借助于网络基础设施可使不同的网络节点之间互相交换数据，共享网络资源。建立网络基础设施的目的就是使不同的实体只要需要，就可以方便地使用基础设施提供的服务。安全基础设施与网络基础设施遵循同样的原则，安全基础设施为整体应用系统提供安全基本框架，它可以被应用系统中任何需要安全应用的对象使用。因此，其在设计上必须具有一般性和通用性。只有这样，那些需要使用这种基础设施的对象在使用安全服务时，才不会遇到困难。PKI 就是这样一种安全基础设施，利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。用户可利用 PKI 平台提供的服务进行安全通信。

公钥加密技术

PKI 是建立在公钥加密技术之上的，那么要了解 PKI 则首先要看一下公钥加密技术。加密是保护数据的科学方法。加密算法在数学上结合了输入的文本数据和一个加密密钥，产生加密的数据（密文）。通过一个好的加密算法，通过密文进行反向加密过程，产生原文就不是那么容易了，需要一个解密密钥来执行相应的转换。密码技术按照加解密所使用的密钥相同与否，分为对称密码学和非对称密码学，前者加解密所使用的密钥是相同的，而后者加解密所使用的密钥是不相同的，即一个秘密的加密密钥(签字密钥)和一个公开的解密密钥(验证密钥)。在传统密码体制中，用于加密的密钥和用于解密的密钥完全相同，通过这两个密钥来共享信息。这种体制所使用的加密算法比较简单，但高效快速，密钥简短，破译困难。然而密钥的传送和保管是一个问题。例如，通讯双方要用同一个密钥加密与解密，首先，将密钥分发出去是一个难题，在不安全的网络上分发密钥显然是不合适的；另外，任何一方将密钥泄露，那么双方都要重新启用新的密钥。

1976 年，美国的密码学专家 Diffie 和 Hellman 为解决上述密钥管理的难题，提出一种密钥交换协议，允许在不安全的媒体上双方交换信息，安全地获取相同的用于对称加密的密钥。在此新思想的基础上，很快出现了非对称密钥密码体制，即公钥密码体制（PKI）。自 1976 年第一个正式的公共密钥加密算法提出后，又有几个算法被相继提出。如 Ralph Merkle 猜谜法、Diffie-Hellman 指数密钥交换加密算法、RSA 加密算法、Merkle-Hellman 背包算法等。目前，结合使用传统与现代加密算法的具体应用有很多，例如 PGP、RIPEM 等加密软件，是当今应用非常广的加密与解密软件。公共密钥算法的基本特性是加密和解密密钥是不同的，其中一个公共密钥被用来加密数据，而另一个私人密钥被用来解密数据。这两个密钥在数字上相关，但即便使用许多计算机协同运算，要想从公共密钥中逆算出对应的私人密钥也是不可能的。这是因为两个密钥生成的基本原理根据一个数学计算的特性，即两个对位质数相乘可以轻易得到一个巨大的数字，但要是反过来将这个巨大的乘积数分解为组成它的两个质数，即使是超级计算机也要花很长的时间。此外，密钥对中任何一个都可用于加密，其另外一个用于解密，且密钥对中称为私人密钥的那一个只有密钥对的所有者才知道，从而人们可以把私人密钥作为其所有者的身份特征。根据公共密钥算法，已知公共密钥是不能推导出私人密钥的。最后使用公钥时，要安装此类加密程序，设定私人密钥，并由程序生成庞大的公共密钥。使用者向与其联系的人发送公共密钥的拷贝，同时请他们也使用同一个加密程序。之后他人就能向最初的使用者发送用公共密钥加密成密码的信息。仅有使用者才能够解码那些信息，因为解码要求使用者知道公共密钥的口令，那是惟有使用者自己才知道的私人密钥。在这些过程当中，信息接受方获得对方公共密钥有两种方法：一是直接跟对方联系以获得对方的公共密钥；另一种方法是向第三方即可靠的验证机构（如 Certification Authority，CA），可靠地获取对方的公共密钥。

PKI 的定义

现在，我们可以看 PKI 的定义：PKI（Public Key Infrastructure）是一个用非对称密码算法原理和技术来实现并提供安全服务的具有通用性的安全基础设施，是一种遵循标准的利用公钥加密技术为网上电子商务、电子政务的开展，提供一整套安全的基础平台。PKI，公钥基础设施，顾名思义，PKI 技术就是利用公钥理论和技术建立的提供网络信息安全服务的基础设施。PKI 管理平台能够为网络中所有需要采用加密和数字签名等密码服务的用户提供所需的密钥和证书管理，用户可以利用 PKI 平台提供的安全服务进行安全通信。

PKI 公开密钥基础设施能够让应用程序增强自己的数据和资源的安全，以及与其他数据和资源交换中的安全。使用 PKI 安全基础设施像将电器插入墙上的插座一样简单。

1、具有易用的、重所周知的界面。

2、基础设施提供的服务是可预测的并且是一致的、有效的。

3、应用设施无需要了解基础设施是如何提供服务的。

PKI 的内容

一个完整的 PKI 系统必须具备权威认证机构（CA）、数字证书库、密钥备份及恢复系统、证书作废系统

和应用接口（API）等基本组成部分。

1、权威认证机构（Certificate Authority）：权威认证机构简称 CA，是 PKI 的核心组成部分，也称作认证中心。它是数字证书的签发机构。CA 是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构。

2、数字证书库：在使用公钥体制的网络环境中，必须向公钥的使用者证明公钥的真实合法性。因此，在公钥体制环境中，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份以及它与公钥的匹配关系。目前较好的解决方案是引进证书(Certificate)机制。（1）证书。证书是公开密钥体制的一种密钥管理媒介。它是一种权威性的电子文档，形同网络环境中的一种身份证，用于证明某一主体的身份以及其公开密钥的合法性。（2）证书库。证书库是证书的集中存放地，是网上的一种公共信息库，供广大公众进行开放式查询。到证书库访问查询，可以得到想与之通信实体的公钥。证书库是扩展 PKI 系统的一个组成部分，CA 的数字签名保证了证书的合法性和权威性。

3、密钥备份及恢复系统：如果用户丢失了密钥，会造成已经加密的文件无法解密，引起数据丢失，为了避免这种情况，PKI 提供密钥备份及恢复机制。

4、证书作废系统：有时因为用户身份变更或者密钥遗失，需要将证书停止使用，所以提供证书作废机制。

5、PKI 应用接口系统： PKI 应用接口系统是为各种各样的应用提供安全、一致、可信任的方式与 PKI 交互，确保所建立起来的网络环境安全可信，并降低管理成本。没有 PKI 应用接口系统，PKI 就无法有效地提供服务。

整个 PKI 系统中，只有 CA 会和普通用户发生联系，其他所有部分对用户来说都是透明的。