文章编号：2096-1472(2017)-04-50-04

安全通信中的密钥分配教与学

贺文华[1]，刘 浩[1]，贺劲松[1]，彭智朝[1,2]
（1.湖南人文科技学院信息学院，湖南 娄底 417000；
2.天津大学计算机科学与技术学院，天津 300192）

摘 要：保密信息的安全传输在商业贸易、网络通信、国防军事等领域有着广泛的应用需求，然而信息安全的核心无疑是密码技术，密钥分配与管理又是密码技术的关键。本文阐述了传统密码算法的密钥分配、身份密码体制的密钥分配、基于生物特征的密钥分配、量子密钥分配的常用技术，我们对它们进行了必要的分析和比较教学，达到了教学的目的，并提高了教学效果。

关键词：传统密钥；身份密钥；生物特征密钥；量子密钥；密钥分配
中图分类号：TP393 **文献标识码**：A

The Teaching and Learning of Key Distribution in Secure Communication

HE Wenhua[1],LIU Hao[1],HE Jingsong[1],PENG Zhichao[2]
(1.*School of Information,Hunan University of Humanities,Science & Technology,Loudin* 417000,*China*;
2.*School of Science and Technology,Tianjin University,Tianjin* 300192,*China*)

Abstract: Secure transmission of confidential information has broad application requirements in the fields of commercial trade,network communication,national defense and military,etc.Beyond all doubt,cryptography technology is the core of information security,while key distribution and management is the critical point ofcryptography technology.This paper expounds the common distribution techniques of the traditional key,the identity key,the biometric key and the quantum key.Through necessary analysis and comparison of the techniques,the teaching goal is achieved and the teaching effect is effectively improved.

Keywords:traditional key;identity key;biometric key;quantum key;key distribution

1 引言(Introduction)

密码学分为密码编码学和密码分析学两大部分。密码编码学是保持明文的秘密以防止入侵者知晓；密码分析学是不知密钥的情况下，恢复明文的科学。正是因为密码编码学和密码分析学的此消彼长，促进了密码学的迅速发展。目前密码体制分成两大类，一类是基于数学的密码理论，主要包括对称密码、非对称密码、身份认证、密钥管理等，另外一类是基于非数学的密码理论，主要包括量子密码、生物特征密码、密钥管理等。

随着社会的信息化进程的推进，信息安全在生产和生活中的重要性越来越突出，加密技术被广泛地应用于国防军事、企业、商业和个人隐私等的保护工作中。现代密码中，加解密算法是完全公开的，当有了确定的加解密算法，密钥的保密性成为了密码系统的核心。因此，密钥管理是数据加解密技术中的重要一环，其在整个保密系统中占有重要地位[1]。可见信息的安全性是由对密钥的保护性来决定的，而不是由对算法或硬件本身的保护来决定的，而密钥安全又是网络环境中密钥管理要遵守的宗旨。事实上，不仅安全密码算法和协议设计十分困难，而且密钥管理则更加艰难[2]。因此，若密钥得不到合理的保护和管理，无论算法设计得多么精巧和复杂，保密系统也是脆弱的，而密钥管理中的一个关键环节又是密钥分配。

2 密钥分配(Key distribution)

密钥分配是密钥产生后到使用者获得密钥的全过程。密钥分配技术一方面为减轻负担，提高效率，引入自动密钥分配机制；另一方面为提高安全性，尽可能减少系统中驻留的密钥量。故密钥必须通过安全的信道进行分配，通常，不同密码系统采用不同的分配方法。密钥分配需要完成两个功能，也就是将密钥分发给双方和双方互相认证。

2.1 密钥分配方法

假设通信双方是Alice和Bob，常用的密钥分配方法如下：

①由Alice选定密钥后用物理手段安全地传送给Bob。

②由可信的第三方选定密钥后并用物理手段安全地发送

www.rjgcz.com

给Alice和Bob。

③假设Alice和Bob已拥有一个密钥，则任意一方选定新密钥后并用已拥有的密钥加密新密钥发送给对方。

④假设Alice和Bob能通过保密信道与可信的第三方通信，则可信的第三方选定密钥后就可安全地发送给Alice和Bob。

⑤假设由可信的第三方发布Alice和Bob的公开密钥，则Alice和Bob可用对方的公开密钥进行保密通信。

前两种人工配送方法不可取。对于第三种方法，攻击者一旦获得一个密钥就可获取以后所有的密钥；而且用这种方法对所有用户分配初始密钥时，代价仍然很大[3]。第4、5种方法是目前常用的方法。

2.2　传统密码算法的密钥分配

传统密码体制目前分为单钥密码和双钥密码体制，单钥密码体制也就是对称密码体制，它的加密密钥和解密密钥是同一把密码钥匙；双钥密码体制也就是非对称密码体制，它的加密密钥与解密密钥不是同一把密码钥匙，而是各不相同，也被称为公钥体制。

(1) 对称密码技术的密钥分配

a.集中式密钥分配

密钥分配中心KDC(Key Distribution Center)是集中式密钥分配的第三方，负责分配密钥。假定发起者A和响应者B的身份分别是IDA和IDB，它们与密钥分配中心KDC有一个共享密钥(也称为主密钥)Ka和Kb，通过共享密钥分配给发起者A和响应者B的密钥被称为会话密钥，发起者A要与响应者B建立一个连接，且用会话密钥保护连接传输的数据，通信传输完成后，会话密钥即被销毁。如图1所示。

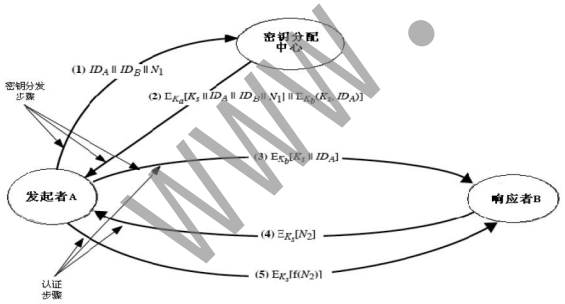

图1 集中式密钥分配

Fig.1 Centralized key distribution

具体过程如下：

①发起者A向密钥分配中心KDC发送会话密钥请求的信息IDA ‖ IDB ‖ N1，其中唯一标识符N1，通常是时间戳、计数器或随机数。

②密钥分配中心KDC向发起者A返回应答信息EKa[Ks ‖ IDA ‖ IDB ‖ N1 ‖ EKb[Ks ‖ IDA]]。应答信息用Ka加密，又含有会话密钥Ks。应答信息只有发起者A才能解密，同时将会话密钥Ks存储起来，并且发起者A也据此确信应答信息是由密钥分配中心KDC发送。

③发起者A向响应者B发送含有会话密钥Ks的请求信息EKb[Ks ‖ IDA]。此请求信息用Kb加密，响应者B收到后解密，获到会话密钥Ks，同时将会话密钥Ks存储起来，且根据EKb确信Ks来自KDC，根据IDA判断对方是发起者A。因为由发起者A转发的是由密钥分配中心KDC用Kb加密后的密文，所以转发过程不存被窃听、窃取。至此，会话密钥Ks的密钥分配已经完成。

④响应者B向发起者A返回应答信息EKs[N2]。响应者 B用会话密钥Ks加密随机数N2后发送给发起者A，也就是通知告诉发起者A，响应者B当前是可以通信的。

⑤发起者A向响应者B再返回应答信息EKs[f(N2)]。发起者A应答响应者B发送的信息N2，并对N2作函数变换，且用会话密钥Ks加密后发送给响应者B。

事实上第④、⑤两步结合第③步完成发起者A和响应者B的相互认证，且响应者B能确信所收到的信息没有产生重放。

随着网络用户数的增加，一个密钥分配中心KDC成为整个系统的瓶颈，承担不了密钥分配的重任，于是采用多个KDC的分层结构方法来解决[1]。

b.分布式密钥分配

如果网络中通信各方拥有相同的地位，且协商解决相互之间的密钥分配，不受任何限制，这就是分布式密钥分配。如果网络中有n个用户，则需有n(n−1)/2个主密钥。当n很大时，整个网络中的主密钥很多，但每个节点最多只保存个n−1主密钥。本方案是适用的是小型网络或局域网。在大型网络中，由于用户数太多，本方案是不适用[1]。

假设发起者A和响应者B的身份分别是IDA和IDB，每个用户事先和其他用户之间存在一个主密钥MKm，用主密钥来产生会话密钥，则发起者A和响应者B之间产生会话密钥的过程如图2所示。

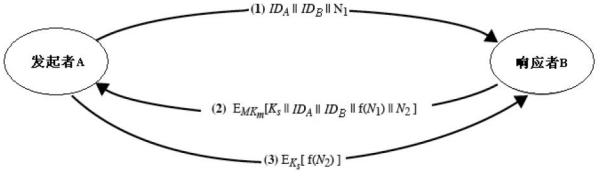

图2 分布式密钥分配

Fig.2 Distributed key distribution

具体过程如下：

①发起者A向响应者B发送会话密钥请求的信息IDA ‖ IDB ‖ N1。其中唯一标识符N1，通常是时间戳、计数器或随机数，告知发起者A希望与响应者B通信。

②响应者B向发起者A返回应答信息

www.rjgcz.com

EMKm[Ks ‖ IDA ‖ IDB ‖ f(N1) ‖ N2]。应答信息用共享的主密钥MKm加密，并含有响应者B产生的会话密钥Ks和发起者A向响应者B身份标识符与函数变换f(N1)及随机数N2。发起者A用共享的主密钥MKm解密应答信息获取会话密钥Ks，用于双方通信。

③发起者A向响应者B返回应答信息EKs[f(N2)]。发起者A用会话密钥Ks对函数变换f(N2)加密发送给响应者B，使响应者B能确信信息没有产生重放。

此外，我们常利用非对称密码技术的密钥分配来进行对称密码技术的密钥分配。

(2) 非对称密码技术的密钥分配

在公钥体制中，公钥分配的方法通常有公开发布、公用目录、公钥机构和公钥证书等多种。

a.公开发布

公开发布就是网络用户把自己的公开密码钥匙发送给或广播给其他网络用户，这种方法的不足是可能会产生伪造、冒充。

b.公用目录

公用目录中含有每个网络用户的一个目录项，即进行安全认证的网络用户身份标识符和公开密码钥匙等，通常是由可信任的机构或组织来建立和维护这个动态目录。网络用户可以从这个动态目录获取所需的公开密码钥匙。公用目录比公开发布的安全性较好，但严重不足是攻击者获得目录管理机构私有密码钥匙后可伪造公开密码钥匙，产生欺骗行为。

c.公钥机构

为克服公用目录的弱点，引入公钥管理机构，来进一步提高安全性。假设发起者A和响应者B的身份分别是IDA和IDB，发起者A和响应者B都可靠地知道公钥管理机构的公开密码钥匙，且公钥管理机构自己的私钥为KRauth，公钥分配过程如图3所示[3]。

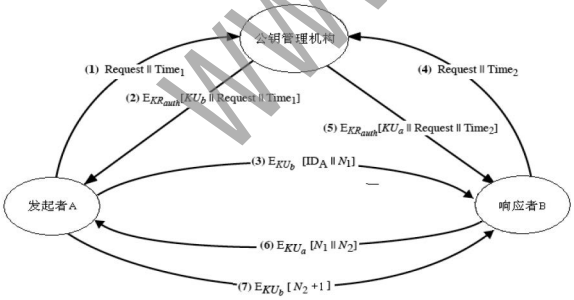

图3 公钥管理机构分配公钥

Fig.3 Public key managers distribute public keys

具体过程如下：

①发起者A向公钥管理机构发送获取响应者B公开密码钥匙的请求信息。其中唯一标识符Time1是时间戳。

②公钥管理机构向发起者A返回应答信息。应答信息中含有响应者B的公开密码钥匙KUB和发起者A的请求及时间戳Time1，并用公钥管理机构的私钥KRauth加密。返回发起者A的请求以验证请求信息没有被篡改，返回时间戳Time1以告之发起者A不是一个旧信息。

③发起者A向响应者B发送用响应者B的公开密码钥匙KUB加密的信息。信息中含有发起者A的身份IDA和唯一标识符N1。

④响应者B用类似①②步骤的方法从公钥管理机构获取发起者A的公开密码钥匙KUA。至此，公开密码钥匙KUA和KUB分配完毕，双方可进行保密通信。

⑤响应者B向发起者A发送用发起者A的公开密码钥匙KUA加密的信息。信息中含有唯一标识符N1和N2。因只有响应者B才能解密③的信息，所以发起者A据此(收到的信息中的唯一标识符N1)确信通信的另一方确实是响应者B，实现发起者A对响应者B的身份认证。

⑥发起者A向响应者B发送用响应者B的公开密码钥匙KUB加密的信息，响应者B解密后确信通信的另一方确实是发起者A，实现响应者B对发起者A的身份认证。在这个过程中，如果发起者A用响应者B的公开密码钥匙只对N2加密，则响应者B不能确信通信的另一方是发起者A，原因是可能产生重放。

获得对方公开密钥后可保存起来供以后使用。然而还必须定期地通过公钥管理机构获取通信对方的公钥，以保证对方公钥更新后仍能进行保密通信。

当网络用户数增加时，公钥管理机构可能会成为系统的瓶颈，承担不了密钥分配的重任，于是采用多个KDC的分层结构方法来解决[1]。

d.公钥证书

公钥管理机构分配公钥存在公钥管理机构可能会成为系统的瓶颈，为解决此问题引入公钥证书。用户通过交换公钥证书来互相交换自己的公钥。

证书一般由第三方发行，这个第三方称为证书权威中心(Certificate Authority，CA)，证书由CA签名表明证书的拥有者所具有的公钥等信息。假设IDA是用户A的身份标识，PKA是用户A的公钥，T是当前时间戳，PKCA是CA的公钥，SKCA是CA的私钥。证书由CA用它的私钥签名，其他用户可以用CA的公钥验证证书的真假。公钥证书的分配过程如图4所示 。

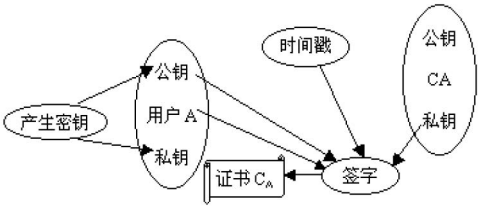

图4 公钥证书分配公钥

Fig.4 Public key certificate distribute public key

www.rjgcz.com

用户利用公钥证书也可将自己的公钥发给其他用户，对方接收后用PKCA验证证书，即DPKCA[ESKCA[T，IDA，PKA]]=[T，IDA，PKA]。

此外，由于公钥算法速度很慢，在通信中一般不使用公钥加密消息，而是使用会话密钥(对称密码密钥)加密消息。因此一般的做法是用会话密钥加密消息，用公钥来实现会话密钥的分配。

2.3 身份密码体制的密钥分配

通过前面的阐述，我们知晓公钥密码体制中重点是保证公钥的真实性，于是引入证书机制来实现。然而由于证书的产生、发布与分配、存储与管理、撤销与验证等所占用资源太多，密钥管理开销越来越大，实时性能明显降低，于是引入基于身份密码体制。

以用户的身份标识直接作为用户公钥或者可计算出用户公钥的密码体制称为身份密码体制IBC(Identity-Based Cryptography)。身份标识是任意唯一的字符串标识符，用户公钥(也称身份公钥)是身份标识的函数，身份标识是用户公钥的担保[4]。通过可信第三方私钥产生中心PKG(Private Key Generator)利用用户公钥和系统主密钥来产生用户私钥(也称身份私钥)，并安全发放。由于用户公钥是直接计算出来的，从而避免了证书的存储与管理等开销，优化了密钥管理，实时性明显提高。

目前有一种称为可分离匿名的私钥分发方案(简称SAKI)。2009年，Chow提出了将加密方案中的接收者身份匿名，采用匿名分发私钥的方式，PKG无法将密钥和用户身份联系起来，也就无法进行对应的解密行为[5]。

2.4 基于生物特征的密钥分配

生理特征和行为特征统称为生物特征，利用计算机或终端设备来进行人体的生理特征或行为特征来实现身份鉴别称为生物特征识别，从而实现了用户数字身份和物理身份的统一。在生物特征加密技术中，我们用密钥绑定来获取与自身特征相对应的密码钥匙。利用生物特征的唯一性、不可替代性来解决传统密码学中密钥容易遗忘和被窃取等问题。文献[6]提出了模糊匹配协议和基于拉格朗日插值法的Fuzzy vault协议两种方法用于安全传输用户的生物特征密钥。

传统的密码技术，基于数学的密码理论，主要包括对称密码、非对称密码、身份认证、密钥管理等，都存在一定的安全缺陷。主要原因是安全性限于当前的计算能力，密钥管理难度大，同时，网络传输密钥，存在窃取与篡改，安全性问题难以解决。

2.5 量子密钥分配

现代密码学认为，加密和解密算法都可以公开，其安全性在于密钥的保密性。由于窃听的存在，通信双方绝对安全密钥是难以保证的。然而，今天的量子密码已成这现实，过去的DES、RSA算法不再安全了。

量子信息论包括量子计算和绝对安全保密通信的量子密钥分配。量子计算对公钥体制有着颠覆性的打击，特别是安全特性；而量子保密通信又是连量子计算也无法破解的绝对安全通信。量子密钥分配原理来源于光子偏振，基于量子态的概率特性，是用量子态来编码密钥，在多用户间传输单个或纠缠量子进行密钥分配的，其安全性是由量子力学的三条基本物理定律(测量塌缩理论、海森堡不确定原理和量子不可克隆定律)来保证的，而不是由计算复杂度保证的。

量子密钥分配协议是发送和接收方利用量子态时所共同遵循的信息加载、探测、比对方式和后处理过程。主要的量子密钥分配协议有采用单光子的BB84、B92、SARG、六态协议和采用纠缠光源的E91协议等[2]。

3 结论(Conclusion)

传统密码、身份密码、生物特征密码的理论已成熟，已被广泛应用在电子商务、电子政务、身份认证、数字签名等领域中，而量子密码离实际应用尚有一定的距离。信息安全的核心是密码技术，密钥分配又是密码技术的关键。在2016年“信息安全理论与技术”课程教学中，我们对传统密码算法的密钥分配、身份密码体制的密钥分配、基于生物特征的密钥分配、量子密钥分配的常用技术进行了讲授，并进行了必要的分析和比较教学，达到了教学的目的，期末笔试考试密钥管理答题同上届比较，优秀率从21%提高到了36.6%，不及格率从23%下降到了8.8%，提高了教学效果。

参考文献(References)

[1] 李飞,吴春旺,王敏.信息安全理论与技术[M].陕西:西安电子科技大学出版社,2016.

[2] 闫鸿滨,密钥管理技术研究综述[J].南通职业大学学报,2011(01):79-83.

[3] 郭亚军,宋建华,李莉.信息安全原理与技术[M].北京:清华大学出版社,2012.

[4] 李楠.基于身份密码体制的密钥管理技术研究[D].解放军信息工程大学,2010.

[5] 张波.基于身份密码方案的研究[D].山东大学,2010.

[6] 蒋磊.基于 Biometrics 的无线 BASN 安全机制的研究[D].电子科技大学,2010.

作者简介：

贺文华(1964-)，男，硕士，教授.研究领域：计算机网络与信息安全.

刘　浩(1976-)，男，博士，副教授.研究领域：计算机网络与信息安全.

贺劲松(1989-)，男，研究生．研究领域：计算机网络与安全.

彭智朝(1975-)，男，博士，副教授.研究领域：计算机网络与大数据.

www.rjszz.com