<<公钥密码学>>

图书基本信息

书名：<<公钥密码学>>

13位ISBN编号：9787040285024

10位ISBN编号：7040285029

出版时间：2010-1

出版时间：高等教育出版社

作者：祝跃飞，张亚娟 著

页数：175

前言

1976年，Diffie和Hellman在《密码学的新方向》（Neu，Directions in Crypto-graphy）一文中首次提出了公钥密码体制的思想，开创了密码学的新纪元。
公钥密码体制中，每个用户拥有公开的公钥和私有的私钥，且由公钥无法导出私钥。
这不仅避免了对称密码体制固有的密钥分发问题，也催生了数字签名体制，而公钥密码体制所提供的可认证性、机密性、不可否认性和数据完整性等安全服务使得其成为当前网络环境下保障信息安全的核心技术。

密码体制的安全性分析是密码体制设计中不可或缺的重要环节，而对直观上的“安全”给予严格的定义是安全性分析的基础。
到目前为止，学术界有两种定义方法：信息论方法和复杂度方法。
信息论方法所关注的是密文是否具有相应明文的信息。
粗略地说，如果密文含有相应明文的某些信息，则认为该加密体制是不安全的。
已经证明，只有当密钥长度超过所加密的明文时，才能实现高级别的安全性（无条件的安全）。
在实际应用中，这是极其不方便的。
只使用中等长度的密钥就可以进行不限量安全通信的密码是更可取的。
但是暴力破解的存在使得在原则上不可能有这样的密码，然而如果该密码没有其他破译方法，且暴力破解对于当前的计算能力而言是不可行的，那么在实际中人们仍然可以使用该密码。
但问题在于如何确信密码不能被快速破译。
当然，在数学上对上述问题给予证明是最佳方案，但是NP是否不等于P是世界难题，这说明无法数学证明密码是不可破译的，所以人们似乎只能依靠实际证据来说明密码体制是安全的。
过去，密码的质量靠请专家破译密码来评价，如果他们不能破译，就会增强对密码安全的信心。
这种方法有明显的不足，如果别人有更好的专家，或者我们对自己的专家缺乏信任，那么密码的完善性可能受到损害。
尽管如此，直到最近这个方法仍是唯一可供使用的方法，并且靠它支持像美国国家标准局正式批准的数字加密标准（DES、AES）这样一些广泛使用的密码的可靠性。

随着对密码基础研究的深入，密码学家认为将密码的不可破译性与公认的数学难题相挂钩，则在现有的计算能力下，可以说明密码的安全性，这便是计算复杂度方法的安全性证明思想。

<<公钥密码学>>

内容概要

本书重点介绍公钥密码的可证安全理论和旁道攻击技术，内容涵盖公钥密码基础理论、公钥密码的可证安全理论和旁道攻击三个部分。
第一部分为公钥密码学基础理论，介绍公钥密码体制思想的提出和特点，公钥密码与杂凑函数，公钥基础设施以及基本体制；第二部分为公钥密码体制的可证安全理论，重点论述可证安全的加密体制、可证安全的签名体制以及混合加密体制的可证安全性分析；第三部分概略介绍公钥密码的旁道攻击技术。
本书适合高等学校计算机、信息安全、电子信息与通信、信息与计算科学等专业的研究生以及相关专业的研究人员使用。

作者简介

祝跃飞，解放军信息工程大学教授、博士生导师。
长期从事信息安全领域的教学与研究工作。
曾参与编著《算法数论》、《椭圆曲线密码导引》和《密码学与通信安全基础》。

<<公钥密码学>>

书籍目录

章节摘录

由于公钥密码体制中加密操作和解密操作的可分离性，产生了一种新的密码体制——数字签名，它以电子方式实现传统手写签名的功能，为消息提供不可否认性的安全服务。
签名者（signer）利用自己的私钥，对消息进行变换，该操作称为签名算法（Signa‘ ture Algorithm），所得的结果称为签名（signature）。
实际通信中传送的是消息及其签名，验证者（Verifier）利用签名方的公钥和对应的变换，验证签名的合法性，该操作称为验证算法（Verification.Algorithm）。
由于签名仅能由拥有对应私钥的签名者产生，所以签名者不能否认曾发送带有签名的消息，即提供了不可否认的安全服务。
当然，上述结论是以签名算法安全为前提的，即不知道签名者的私钥则难于伪造利用签名者公钥可通过验证的签名。
加密体制和签名体制是公钥密码的主要内容，但是随着网络的日益普及和电子商务、电子政务的蓬勃发展，又产生了形形色色的密码应用环境，提出了多种新的密码需求，随之涌现出众多实现其他密码功能的公钥密码体制。
今天的公钥密码不再仅仅包含加密体制和签名体制，可以认为具有多个密钥、密钥间不能完全相互导出、至少一个密钥是公开的密码系统均是公钥密码。
其中密钥间不能完全相互导出是指至少存在一个密钥，利用系统的其他密钥无法（或者不存在多项式时间的算法）求得该密钥。
消息传送过程中，非授权者可以通过各种方法，如搭线窃听、电磁窃听、声音窃听等来窃取消息，本书称这些非授权者为截收者（Eavesdropper）或攻击者。
截收者通过分析窃取获得的消息，采取可行方法破坏密码系统所提供的安全服务，如获得密文对应的明文以破坏机密性，伪造签名以破坏不可否认l生等，这个过程称为密码分析（Cryp tanalysis）。
早期密码的安全性大都基于对算法的保密，但是算法一旦泄露，此前保护的消息将失去机密性。
后来，在算法中引入了特殊变量——密钥，密钥的随机性增加了算法泄露后获得保密信息的困难程度。
从提高密码安全性和增强密码实用性的角度出发，Kerckhoff提出了Kerckhoff准则：算法细节必须是公开的，密码安全性应仅基于使用密钥的保密。
因为如果在知道算法的条件下仍不能破坏算法所提供的安全服务，则在不知道算法的条件下更难，所以上述准则实际上增强了对密码的安全要求。

版权说明