信息安全系列丛书

Public Key Cryptology

Design Principle and Provable Security

公钥密码学

设计原理与可证安全

祝跃飞　张亚娟

高等教育出版社

信息安全系列丛书

Public Key Cryptology

Design Principle and Provable Security

公钥密码学

GONGYAO MIMAXUE

设计原理与可证安全

SHEJI YUANLI YU KEZHENG ANQUAN

祝跃飞　张亚娟

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

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。

图书在版编目(CIP)数据

公钥密码学:设计原理与可证安全／祝跃飞,张亚娟著.
北京：高等教育出版社，2010.1
（信息安全系列丛书）
ISBN 978-7-04-028502-4

Ⅰ.公… Ⅱ.①祝… ②张… Ⅲ.密码术 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字（2009）第 243432 号

策划编辑	陈红英	责任编辑	萧　潇	封面设计	刘晓翔
版式设计	史新薇	责任校对	王效珍	责任印制	韩　刚

出版发行	高等教育出版社	购书热线	010－58581118
社　　址	北京市西城区德外大街 4 号	咨询电话	400－810－0598
邮政编码	100120	网　　址	http://www.hep.edu.cn
总　　机	010－58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京民族印务有限责任公司	畅想教育	http://www.widedu.com

开　　本	787×1092　1/16	版　　次	2010 年 1 月第 1 版
印　　张	11.75	印　　次	2010 年 1 月第 1 次印刷
字　　数	220 000	定　　价	30.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 28502-00

前言

1976 年，Diffie 和 Hellman 在《密码学的新方向》(*New Directions in Cryptography*) 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。计算复杂度方法作为另一种定义密码安全和获得密码安全性证据的较为实用的方法，它所关注的不是密文是否含有相应明文的某些信

息，而是所含有的信息能否有效求得。计算复杂度方法的核心是利用图灵机理论给出安全性的形式化定义，通过安全性证明来建立破坏密码体制安全性的复杂度和某个问题的复杂度之间的联系，而后者已能提供确实可信的难解性证据，从而保证了密码体制的安全性。

在安全性的归约证明中，若对体制构建中的任何组成没有任何假设，便将安全问题约化到难解的问题上，则称该证明是在标准模型下的，也称该体制是标准模型下可证安全的。由于公钥密码体制本身的复杂性以及应用的广泛性，使得在标准模型下证明安全性极其困难。目前最为著名的在标准模型下可证安全的实用的公钥密码体制是 Cramer 和 Shoup 于 1998 年提出的 CS 体制，其安全性是基于判定 Diffie-Hellman 问题的。为了方便证明，密码学家们在安全性的定义模型中引入谕示 (oracle)，以此为基础证明体制的安全性，然后用相应的实例替换谕示。早期的谕示对伪随机函数做了抽象，其显著的缺点是攻击者不能直接访问谕示；随后，引入了公共谕示的思想，即现实存在的各方均可以直接访问谕示；直到 1993 年，Bellare 和 Rogaway 才提出了随机谕示模型的概念，即在安全性定义和证明中将杂凑函数认为是完全随机函数，把它作为公共谕示，此时证明安全的体制称为随机谕示模型下可证安全的。随机谕示模型是应用最广泛的安全性证明模型，有众多的研究成果。其中最受关注的是，在该模型下密码学家们提出了几种由弱安全强度的加密体制构造强安全强度加密体制的途径，如适用于单向陷门置换的 OAEP 和 OAEP+、适用于 (概率) 公钥加密体制的 FO 变换等，并证明了一类具有特定结构签名体制，即一般签名体制的安全性，目前使用的绝大多数签名体制均是一般签名体制。除随机谕示模型外，另一个较受关注的安全性证明模型是一般群模型，它是由 Nechaev 于 1994 年首次提出的，1997 年 Shoup 将该模型应用到密码中。一般群模型假设安全群 (离散对数不可解的群) 中的运算是由一般群谕示实现的，该谕示在保证运算合理的条件下输出是完全随机的。DSA 类签名体制便是一般群模型下可证安全的签名体制。可证安全作为 20 世纪 90 年代提出的以安全性证明为核心的安全性分析方法，虽然其需要较强的技巧性且仅提供相对的安全，但是可证安全特有的严格证明使得其具有相当的可信度，从而使可证安全成为众多国际标准组织甄选密码标准的评判准则之一，如 IEEE P1363、欧洲的 NESSIE 和日本电子政务的 CRYPTREC 等。

公钥密码学内容异常丰富，其涵盖了体制设计、安全性分析、体制实现、体制的使用以及体制的攻击等，而本书是一本 60 学时的专业教材，无法面面俱到。另一方面，国内外已经出版了大量公钥密码学方面的优秀论著，它们几乎均以基本公钥密码体制和数学问题为讨论的重点，很少涉及可证安全知识。鉴于上述原因，本书重点介绍公钥密码的可证安全理论和旁道攻击技术。本书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等三个方面，其中第一部分 (第 1、2 章) 为公钥密码学基础理论，介绍了公钥密码体制的提出、特点，公钥密码与杂凑函数，公钥基础设施以及一些基本体制；第二部分 (第 3 ～ 6 章) 为公钥密码体制

的可证安全理论，重点论述了加密体制的可证安全、签名体制的可证安全以及混合加密体制的可证安全性分析；第三部分 (第 7 章) 概略介绍了公钥密码的旁道攻击技术。本书读者需具备密码学、信息安全数学基础、计算理论以及概率论等预备知识。

本书的编写和出版得到国家 863 项目 (批准号：2007AA01Z471) 的资助，特此感谢!

作者

2009 年 9 月

目录

第 1 章　引论

1.1　信息安全

什么是信息?《牛津词典》的解释是“信息就是谈论的事情、新闻和知识”;《韦氏字典》的解释是“信息就是观察或研究过程中获得的数据、新闻和知识”;苏联学者卢什科夫把信息定义为“物质和能量在空间和时间分布不均的测度”;意大利学者朗格提出“信息是事物间的差异”;我国信息论专家钟义信教授把信息定义为“事物运动的状态和方式”。此外,还有人认为信息是“客观事物可传递的差异性”,更有人认为信息是“事物的运行状态和关于事物动态过程的各种陈述”,或是“对客观事物属性和相互联系特征的表达”。在我国,日常用语中的信息泛指音信、消息。

什么是信息安全? 美国联邦标准定义信息安全是指“保护信息免受意外或故意的非授权泄露、传递、修改或破坏”。

对有价值信息进行保护可以说是一种本能,一种常识。在自然界,动物为了保护自身的生命安全,利用保护色使得自身与环境融为一体,对它们而言,最有价值的信息就是生命。而对于人类而言,有价值的信息不再仅是与生命相关的信息。公元前 1 世纪,朱利叶斯·恺撒担心自己的信件内容被他人知晓,于是他用一种密码技术来给朋友写信,直到今天,这种密码仍以他的名字命名。

同时,对信息进行破坏以达到自己的目的也是普遍存在的行为。杜鹃鸟将自己的蛋下在其他鸟的巢中,诱骗 180 多种鸟帮助自己抚育小鸟。为了避免被发现,它模仿被骗的寄养鸟排列蛋的形状来排列蛋,使得蛋的排列形状不再是可靠的信息。在整个人类历史中,信息破坏的实例不胜枚举。古希腊人将士兵隐藏在木马中,溜进了特洛伊城,该行为破坏了特洛伊人对木马的常规认识。在第二次世界大战中,英军破译了德军的代号为“月光奏鸣曲”的夜间空袭英国工业重镇考文垂的计划,美军破译了日军偷袭中途岛的情报,使得作战信息不再保密。

信息安全是在“攻”、“守”中不断发展变化的。“攻”、“守”双方当前的技术实力对比体现了信息安全的现状,“攻”、“守”双方的发展趋势决定了信息安全今后的走向。“攻”、“守”双方既相互矛盾又相互统一,它们始终相互促进、循环往复、永

无止境。

人类对信息安全的追求过程是一个漫长的深化过程。为了应对非人为因素引起的不安全问题，人们已经研制出了各种各样的纠错编码；为了应对人为因素引起的安全问题，人们广泛采用密码技术。

为防止第三方获得通信双方的机密通信内容，几千年来，以加密和解密技术为基础的通信保密一直是信息安全的重点。但是，随着新的技术革命——信息革命的突飞猛进，社会信息化迅猛深化，多种多样的网络服务在为人们的生活提供便利的同时，也对信息安全提出了更高的要求，信息安全不再是单纯的加密和解密，而是内容丰富的复杂系统。

最简单的通信模型见图 1.1。Alice 和 Bob 通过不安全信道通信，例如，打电话、发送电子邮件、网上购物等，而 Eve 是信道上存在的第三方，他的目的是破坏通信，可能是获得 Alice 和 Bob 传递的秘密消息，也可能冒充 Alice 给 Bob 发送消息，还可能声称 Alice 给他发送了消息。甚至 Eve 可能就是 Alice，他否认曾经给 Bob 发送过消息；Eve 也可能是 Bob，他否认接收过 Alice 的消息；等等。信息的破坏方式和所达成的目的多种多样，从而信息的安全需求也千变万化，但最基本的安全需求是机密性、完整性、可认证性、不可否认性和可用性。

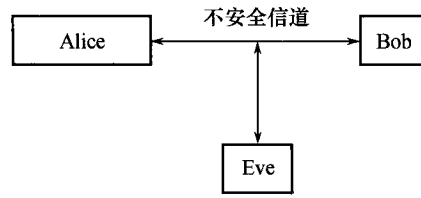

图 1.1 通信模型

1. 信息的机密性 (Confidentiality)：保证信息不被非授权者获取。如 Eve 不能获得 Alice 发给 Bob 的信息。
2. 信息的完整性 (Integrity)：保证信息从真实的信源到达真实的信宿，即信息不能通过非授权方式进行改动。如，若 Eve 改动了 Alice 发送给 Bob 的信息，则 Bob 能检测出该信息被改动过且改动者不是 Alice。
3. 信息的可认证性 (Authentication)：保证信息确实来自预期的发送方 (即数据源认证，Data origin authentication)，或者确认通信方的确是预期的通信方 (即实体认证，Entity authentication)。如，Bob 能够验证接收到的 Alice 的信息的确是 Alice 发送的，Bob 也能够确认与他通信的的确是 Alice。
4. 信息的不可否认性 (Non-repudiation)：每个通信者都有具有法律效力的证据来证明其是否实施过信息交换和获取的行为。如，Alice 不能否认自己发送信息给 Bob 的行为，Bob 也不能否认自己接收了 Alice 所发送信息的行为。

5. 信息的可用性 (Availability)：保证信息可被合法用户访问并按要求的特性使用，即当需要时能否存取所需信息。如，在网络环境下破坏网络和有关系统的正常运行就属于对可用性的攻击。

1.2 密码学

在信息安全的理论体系和应用技术研究中，密码技术占有非常重要的地位，其历史也十分悠久，但直到第二次世界大战为止，密码的设计和破译主要还是凭直觉或猜想而非推理或证明来进行的，密码技术更像是一门艺术而不是一门科学。其主要应用于军事领域，而且涉及的几乎均是加密技术。当时的加密体制是通过通信双方共同约定的密钥来加、解密的，属于对称密码体制，这使得通信双方需要一个安全的通道来传递密钥，而且当通信用户数目增加时，需要的密钥量激增，因此对称密码体制的密钥管理是非常复杂的。

1949 年，Shannon 发表了《保密系统的通信理论》一文，为当时的加密体制建立了理论模型，并利用他刚刚创立的信息论取得了一些极具理论和实践指导意义的结果，从此密码才真正成为一门科学。

1967 年，Kahn 搜集、整理了第一次世界大战和第二次世界大战的大量史料，出版了代表作《破译者》(*The codebreakers*)，该书大致勾画了密码学发展的轮廓。到 20 世纪 70 年代后期，又出现了 Johnson 的《秘密战争》(*The secret war*)、Welchman 的《第六黑屋的故事》(*The hut six story*) 等一些关于密码的文献，使得充满神秘色彩的密码学逐步被人们所了解，但密码的研究仍然是不公开的。

电报发明以后，商业方面对密码学的兴趣主要集中在密本的编制上。到 20 世纪初，则集中于机械和电动机械加密机的设计和制造上。电子计算机的出现，使得密码由机械密码时代进入了电子密码时代。但是直到 20 世纪 70 年代中期，随着集成电路技术的发展，计算机通信的应用越来越广泛，人们越来越担心个人隐私的安全，这些才促使密码学的研究公开化。1973 年，为适应由通信发展带动的公众特别是商业领域对敏感信息保护的现实需求，美国国家标准局 (National Bureau of Standard，NBS) 发布了公开征集密码标准算法的请求。1975 年，NBS 对选定的数据加密标准 DES (Data Encryption Standard) 的算法细节进行了公布，这就揭开了密码学的神秘面纱，吸引了许多学者从事密码学的研究，公开研究从此兴起。

1976 年，W. Diffie 和 M. Hellman 发表了《密码学的新方向》一文，突破了长期使用的对称密码体制，提出了公开密钥密码的思想①，为密码学开拓了广阔的应用前景，从而导致了密码学的一场革命。

Shannon 理论的提出和公钥密码的提出标志着现代密码学的诞生，从此，密码学的研究迅猛发展，密码学者、民间密码学会议、密码学方面的文献都以惊人的速

① 解密文件显示，早在 1970 年，英国的秘密密码研究机构 —— 政府通信总部的 James Ellis 就已经提出了公钥密码的思想和概念。

度增加。

密码学的主题是试图通过各种安全且有效的密码技术解决各种信息安全问题。其可以分为密码编码学 (Cryptography) 和密码分析学 (Cryptanalytics)。密码编码学研究对数据进行变换的原理、手段和方法，以隐藏数据的内容，防止对它进行篡改或非授权使用等。而密码分析学则对密码系统及其输入输出进行分析，以得到秘密信息或敏感数据等。

提供机密性安全服务的密码技术是加密体制 (图 1.2)，其是应用最早且最广的密码技术。发送方用事先协商好的方式，对称为明文 (Plaintext) 的消息进行变换，该操作称为加密 (Encryption)，所得的消息称为密文 (Ciphertext)。实际通信中传送的是密文，接收方用对应的逆变换，由密文恢复出原明文，该操作称为解密 (Decryption)。密码学中称如上述由消息得到密文或由密文得到明文的变换为算法 (Algorithm)。对明文进行加密操作的人员称为加密员 (Cryptographer)。加密员对明文进行加密时所采用的一组规则称为加密算法 (Encryption Algorithm)，传送消息的预定对象称为接收者，他对密文进行解密时所采用的一组规则称为解密算法 (Decryption algorithm)。加密和解密算法的操作通常都是在一组密钥 (Key) 控制下进行的，分别称为加密密钥 (Encryption Key) 和解密密钥 (Decryption Key)。

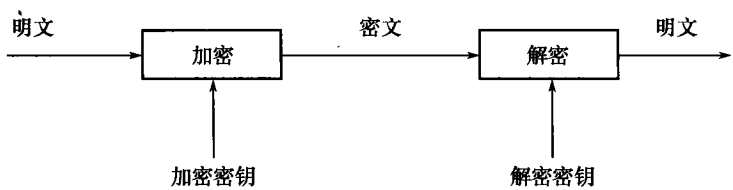

图 1.2 加密体制

根据密钥的特点，Simmons 将密码体制分为对称密码体制 (Symmetric Cryptosystem) 和非对称密码体制 (Asymmetric Cryptosystem) 两种。对称密码体制的加密密钥和解密密钥是相同的或者相互容易导出，故又称为单钥 (One-key) 密码体制或私钥 (Private Key) 密码体制。又因为在 1976 年之前，人们所知道的以及一直采用的都是对称密码体制，所以对称密码体制又称为传统 (Classical) 密码体制。非对称密码体制 (图 1.3) 的加密密钥和解密密钥不同，且由加密密钥难于[①]推出解密密钥，则加密操作和解密操作可以分开，加密操作由任何知道加密密钥的用户公开执行，解密操作只能由解密密钥持有者秘密执行，从而非对称密码体制又称为双钥 (Two-key) 密码体制或者公钥 (Public Key) 密码体制，加密密钥又称为公开密钥或公钥 (Public Key)，解密密钥称为私有密钥或私钥 (Private Key)。依据加密方式密码体制又可以分为流密码 (Stream Cipher) 和分组密码 (Block Cipher)。流密码可以看做是有限符号集上带密钥的伪随机序列，而分组密码则是 n 比特 0、1 序列组

① 此处的“难于”是指不存在多项式时间的算法。

成的集合上带密钥的伪随机置换。

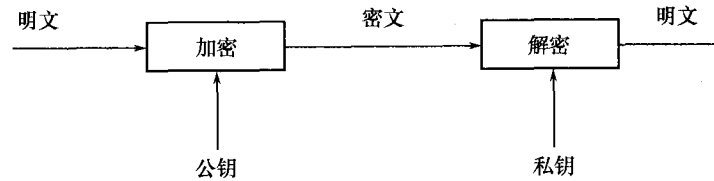

图 1.3 公钥加密体制

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 (Signature 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性等，这个过程称为密码分析 (Cryptanalysis)。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[①] 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。更为重要的是，这一准则是密码公开研究与标准化应

① 荷兰人，1835—1903。

用的前提，所以自然成为公开密码学的基本准则，为各类密码技术所遵循。本书也将其作为分析密码系统安全性的前提条件。

1.3 杂凑函数

杂凑 (Hash) 函数将不定长的数据压缩成该数据的一个定长的指纹 (Fingerprint) 或摘要 (Digest)。计算机科学家利用它加速对大数组或者信息数据库的索引过程，而密码学家则利用它提供消息完整性服务，或者优化系统所提供的安全服务质量。本节将介绍密码学上杂凑函数的分类、设计方法以及其与公钥密码学的关系。

杂凑函数可以分为带密钥的和无密钥的两类。带密钥的杂凑函数的输入是消息和密钥，输出为杂凑值；而无密钥的杂凑函数的输入仅是消息，输出是杂凑值。

杂凑函数还可以依据应用场合或应用目的分为改动检测码 (Modification Detection Codes，MDC) 和消息验证码 (Message Authentication Codes，MAC)。MDC 的目的是确保数据完整性，其实际上属于无密钥杂凑函数，MAC 的目的是确保消息和消息源的完整性，其属于带密钥杂凑函数。一般来说，杂凑函数的计算方法是公开的，也就是说，对于给定输入，任何人可以计算 MDC 的杂凑值；任何拥有密钥的人可以计算 MAC 的杂凑值。图 1.4 描述了杂凑函数的分类情况。

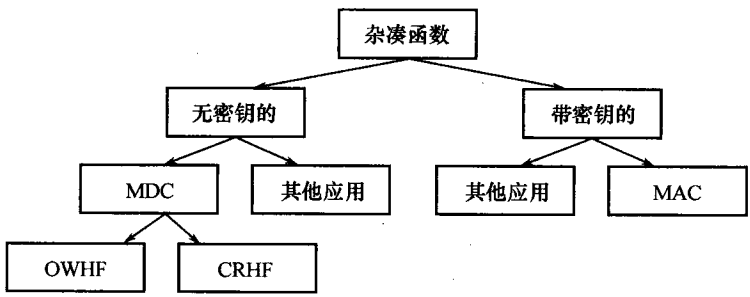

图 1.4 杂凑函数分类

定义 1.1 杂凑函数是具有下述性质的函数 $h(\cdot)$：

1. 压缩：对于任意有限长的输入 x，$h(\cdot)$ 输出固定长度为 n 的 $h(x)$；
2. 易计算：给定 $h(\cdot)$ 和输入 x，$h(x)$ 是容易求取的。

显然，上述定义实际上是无密钥杂凑函数的定义。无密钥杂凑函数可能还具有下述性质：

1. 抗原象攻击：对于任意给定的 y，在不知道其原象的条件下，求取 x，使得 $h(x)=y$ 是困难的；
2. 抗第二原象攻击：对于任意给定的 x，求取 $x' \neq x$ 满足 $h(x)=h(x')$ 是困难的；

3. 无碰撞的：求取 x, x' 满足 $x \neq x'$ 且 $h(x) = h(x')$ 是困难的。

能抗原象攻击的 MDC 称为单向杂凑函数 (One-way Hash Functions，OWHF)。无碰撞的 MDC 称为无碰撞杂凑函数 (Collision Resistant Hash Functions，CRHF)。

抗原象攻击的杂凑函数不一定能抗第二原象攻击。设 $h(\cdot)$ 是单向杂凑函数，对于输入 $x||b$，定义 $h'(x||b) = h(x)$，其中 $||$ 表示比特串的连接，b 是 0 或 1，则 $h'(\cdot)$ 抗原象攻击，但显然 $x||0$ 和 $x||1$ 有相同的杂凑值，所以不能抗第二原象攻击。反之，抗第二原象攻击的杂凑函数不一定能抗原象攻击。设 $h(\cdot)$ 是单向杂凑函数，记比特串 x 的长度为 $|x|$，定义

$$h'(x) = \begin{cases} 0||x, & |x| \leqslant n \\ 1||h(x), & \text{其他} \end{cases}$$

则 $h(\cdot)$ 的抗原象攻击确保了 $h'(\cdot)$ 可以抵抗第二原象攻击，而对于任意杂凑值，其原象均是显然的。

由抗第二原象攻击和无碰撞的定义知，若杂凑函数不能抗第二原象攻击，即对于某个给定的 x，求得 x'，使得 $h(x) = h(x')$，显然，x, x' 也是一对碰撞，故无碰撞的杂凑函数一定抗第二原象攻击。反之，不一定成立。

定义 1.2 消息验证码 MAC 算法是一族被秘密密钥 k 定义的函数 h_k，其满足

1. 易计算：对已知函数 h_k，给定值 k 和消息 x，容易计算求得 $h_k(x)$，该值称为 MAC 值或 MAC；
2. 压缩：h_k 将任意有限比特长度的消息 x 映射为固定长度的输出 $h_k(x)$；
3. 抗计算性：给定多个消息、MAC 对 $(x_i, h_k(x_i))$，对于任意新的消息 $x \neq x_i$，计算出任何消息、MAC 对 $(x, h_k(x))$ 是计算不可行的，需要注意的是此处的密钥 k 可能是变化的。

MAC 的抗计算性实际隐含了密钥的不可恢复性，即给定密钥 k 的多个消息、MAC 对 $(x_i, h_k(x_i))$，求取密钥 k 是计算不可行的。显然，如果 k 可以恢复，则由易计算性知道对于任意消息 x，均可以求得 $h_k(x)$，与抗计算性矛盾。但是，密钥的不可恢复性并不一定意味着抗计算性，因为恢复密钥不一定是求取 MAC 的唯一途径。

1.3.1 设计方法

Preneel[86] 依据安全性假设以及分析方法的不同将杂凑函数的设计方法分为信息论方法、复杂性理论方法和系统论方法。信息论方法以信息论为基础，认为攻击者的计算能力是无限的，提供的是无条件安全性；复杂性理论方法起源于计算的抽象模型，并假定攻击者具有有限的计算能力，提供的是计算安全性；系统论方法的安全性评估是以所知道的攻击该系统的最好的算法和必需的计算能力或实现算法的专用硬件的实际估计为基础的，这是一种很实际的方法。我们认为，上述分类