高等学校信息安全系列教材

密码学

金晨辉　郑浩然　张少武　胡斌　史建红　编著

高等教育出版社
Higher Education Press

高等学校信息安全系列教材

密　码　学

金晨辉　郑浩然　张少武　胡　斌　史建红　编著

高等教育出版社
Higher Education Press

内容提要

本书由中国人民解放军信息工程大学密码学课程组在长期教学过程中所使用的内部讲义完善而成，定位于介绍密码学的基本原理和基本方法，通过该书的学习，读者可以系统地掌握密码学的基本原理、基本方法和基本技术。

全书共包括 10 章和 1 个附录。第 1 章介绍了密码学的基本概念和基本编码原理。第 2 章介绍了 Shannon 保密理论和计算复杂性理论。第 3、4 章分别介绍了序列密码和分组密码的基本原理和方法。第 5、6 和 7 章分别介绍了公钥密码、数字签名和杂凑函数的基本理论和方法。第 8 章和第 9 章分别介绍了认证技术、随机数的产生与检验方法。第 10 章介绍了密钥管理和密钥分配协议的理论与方法。附录介绍了相关的数学知识。

为适应不同层次读者的需要，并使他们接触更多的密码学知识，本书有意增加了许多相关内容。在具体的教学实施过程中，可根据需要对有关内容进行选择。本书既可作为本科生的教材，也可作为硕士研究生和密码研究人员的入门教材。

图书在版编目（CIP）数据

密码学／金晨辉等编著．—北京：高等教育出版社，2009.11

ISBN 978-7-04-028045-6

Ⅰ．密… Ⅱ．金… Ⅲ．密码-理论-高等学校-教材 Ⅳ．TN918.1

中国版本图书馆 CIP 数据核字（2009）第 181690 号

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	廊坊市科通印业有限公司	**畅想教育**	http://www.widedu.com
开　　本	787×1092　1/16	**版　　次**	2009 年 11 月第 1 版
印　　张	24.75	**印　　次**	2009 年 11 月第 1 次印刷
字　　数	550 000	**定　　价**	29.10 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。

版权所有　侵权必究

物料号　28045－00

前　言

密码是战争的产物，历史非常悠久。20 世纪 70 年代以前，密码学主要在军队和政府的掌控下秘而不宣地发展，民间对之了解甚少。W. F. Friedman 专题论文《重合指数及其在密码学中的应用》的发表，以及 C. E. Shannon《保密系统的通信理论》的发表，不仅使人们对密码技术有了初步的了解，也使密码研究从技巧性、直觉性和艺术性居多的阶段，迈入科学化、系统化的研究阶段。数据加密标准（DES 算法）的公布，更使密码学在民间的研究水平得到了整体提高。目前，密码技术及其作用已为越来越多的人所熟悉，不仅用于数据加密等传统领域，而且还用于信息认证等领域，成为解决信息安全问题的一个核心技术。目前，为普及密码知识和密码技术，高等院校的很多专业都将密码学作为专业课程或选修课程开设。

本书定位于介绍密码学的基本原理和基本方法。通过本书的学习，读者可以系统地掌握密码学的基本原理、基本方法和基本技术。

全书共包括 10 章和 1 个附录。第 1 章介绍了密码学的基本概念和基本编码原理，使读者对密码学的全貌、基本的编码原理和古典密码有一个基本的了解。第 2 章介绍了 Shannon 保密理论和计算复杂性理论，涵盖了研究密码的信息论方法和计算复杂性两大方法。第 3 章介绍了序列密码的基本原理和方法，包括伪随机序列的基本特性、序列密码的基本模型、基本编码技术和典型算法，以及序列密码的两个基础理论，即线性反馈移存器和 Walsh 谱的基本理论。第 4 章介绍了分组密码的基本原理和方法，包括典型的分组密码算法及其设计思想分析、对分组密码的基本分析方法等。第 5、6 和 7 章分别介绍了公钥密码、数字签名和杂凑函数的基本理论和基本方法。第 8、9 章分别介绍了认证技术、随机数的产生与检验方法。第 10 章介绍了密钥管理和密钥分配协议的理论与方法，附录介绍了相关的数学知识。

本书是由中国人民解放军信息工程大学密码学课程组根据长期教学过程中所使用的内部讲义完善而成的，由于内容的选材和取舍的难度较大，加之作者水平有限、成书仓促，在教材中会有很多不足之处，甚至可能还有疏忽和错误，敬请广大读者批评指正。

编者联系方式：zhangsw37@sina.com

编　者

2009 年 7 月于中国人民解放军信息工程大学

目　录

试读结束：需要全本请在线购买：　www.ertongbook.com

第 1 章　密码学概述

1.1　引　　言

密码学的历史极为悠久，其起源可以追溯到几千年前。大约 4 000 年前，埃及人就开始了密码的使用。可以说，密码是战争的产物，自其诞生之日起，就成为政治、军事和外交斗争的重要工具。在信息的保密和破译上，争斗的双方进行着激烈的、有时甚至是生死存亡的斗争。例如，在第二次世界大战期间，盟军对日本和德国密码的破译对许多战役的胜利发挥了关键性的作用，并加速了战争结束的进程。随着技术的进步，特别是计算机和现代通信的出现，这种斗争更加扩大、更为激烈。

长期以来，密码学主要应用于军事、外交和政府部门。密码学研究也基本上被政府和军事机构垄断，处于秘而不宣的状态，不为人们了解。在 1949 年以前，密码技术基本上可以说是一门技巧性很强的艺术，而不是一门科学。在这个时期，密码专家常常是凭直觉、技巧和信念进行密码设计和密码分析，而不是基于推理和证明。第一次世界大战之前，密码学的重要进展很少出现在公开文献中，密码学在秘而不宣的状态下向前发展。在 1949 年以前，最有影响的密码文献是 1918 年 William F. Friedman 的专题论文《重合指数及其在密码学中的应用》(The Index of Coincidence and Its Applications in Cryptography)，该报告给出了多表代替密码的破译方法，该报告也是战争的产物。

1949 年，C. E. Shannon 发表了《保密系统的通信理论》(Communication Theory of Secrecy Systems) 一文，为密码学奠定了坚实的理论基础，使密码学成为一门科学。1967 年，Kahn 出版了《破译者》(The Codebreakers) 一书。尽管该书没有提出任何新的技术和思想，但却对密码学的历史进行了相当完整的记述，并使成千上万原本不知道密码学的人了解了密码学。自此，密码学研究引起了民间的兴趣，新的密码学文献慢慢地发表出来。

20 世纪 70 年代由美国政府征集、IBM 公司设计和美国国家安全局 (NSA) 参与修改的数据加密标准 (Data Encryption Standard，DES) 的公布，极大地促进了密码学在民间的研究。通过对 DES 算法的研究和分析，民间的密码学水平取得了突飞猛进的提高。

1976 年，Diffie 和 Hellman 发表了《密码学的新方向》(New Directions in Cryptography) 一文，该文引入了公开密钥密码学这个革命性的概念，从而为基于公开信息的密钥交换和互不信任双方的信息认证问题的解决提供了可能。数字签名成为公钥密码对密码学的最重要的贡献之一。

试读结束：需要全本请在线购买：　www.ertongbook.com

密码学最初只用于解决信息的加密保护问题，用以对抗敌手在信道中的窃密行为。20 世纪 60 年代以来由于计算机和通信系统的普及，导致个人和企业对数字信息进行加密保护和信息认证的需求日益广泛。目前，大量的敏感信息需要通过公共通信设施或计算机网络传递，特别是 Internet、局域网和无线通信的广泛应用，以及计算机应用系统（如电子商务、电子政务、电子金融等）的迅速发展，越来越多的个人信息、企业信息、计算机应用系统等需要利用密码技术提供加密保护、真实性认证。例如银行账号、网上交易、产品防伪等就是典型的例子。民间对信息的保密性和真实性的广泛需求，促使密码学的研究和应用走出“黑屋”，步入人们的视野和生活。目前，密码学的研究和应用领域不断拓展，不仅用于对信息的加密保护，而且还用于信息的真实性认证、产品防伪等各种与信息安全相关的领域。

1.2 密码学的基本概念

密码学的基本目标就是解决信息安全中的三个基本安全需求，即信息的机密性、信息的真实性认证和承诺的不可抵赖性。

所谓信息的机密性就是指信息的内容不被非授权者获取。提供机密性的方法有许多种，包括物理保护、信息隐藏和加密保护等。其中加密保护属于密码学的范畴，它是利用加密算法改变信息数据的原形，从而使非授权者无法从变形后的结果中获取原始信息的内容。在信息隐藏技术中，也或多或少地使用到密码技术。

信息认证包括实体身份（如通信双方的身份、一个设备的身份等）的认证；所传送信息的来源、目的地、产生日期、传送时间等的认证；以及信息的完整性认证。信息的完整性认证是指检测信息在传送或存储过程中是否遭到有意或无意的篡改。信息认证的目的不是为了避免不真实信息的出现，而是要保证不真实的信息能以很大的概率被检测出来。

为突出完整性认证的地位，有的书籍也将完整性认证独立地作为信息安全的一个安全需求。

不可抵赖性是指防止否认以前的承诺或行为。例如，一方对自己曾经签署过的命令或商业合同的否认等。在涉及不可抵赖性的密码方案中，必须有一个用于仲裁的可信第三方。

密码学主要包括 3 个分支，即密码编码学、密码分析学和密钥管理学。其中密码编码学和密码分析学是密码学的两个基本分支，密钥管理学是随着密码学研究和应用领域的不断拓展而独立出来的一个分支。

1.2.1 密码编码学

密码编码学的主要任务是研究安全、高效的信息加密算法和信息认证算法的设计理论与技术。

信息加密算法是密码编码学长期以来的基本研究内容。信息加密算法简称加密算法，其基本思想是对信息进行伪装，使得非授权者不能由伪装后的结果还原出被伪装信息。所谓伪装，就是在一个可变参数的控制下，对数据进行可逆的数学变换。变换前的原始数据称为明文，变换后的数据称为密文，变换的过程称为加密，变换时使用的可变参数称为加密密钥，变换时使用的可逆数学变换称为加密算法。加密变换通常用 $c = E_{k_e}(m)$ 表示，其中 m 是明文，c 是密文，k_e 是加密密钥。

当合法的授权者由密文 c 恢复明文 m 时，需要执行加密变换的逆变换。合法用户由密文 c 求出明文 m 的过程称为脱密，脱密时使用的数学变换称为脱密算法，脱密时使用的可变秘密参数称为脱密密钥。脱密算法通常用 $m = D_{k_d}(c)$ 表示，其中 k_d 是脱密密钥。

合法的授权者之所以合法，是因为他合法地拥有秘密的脱密密钥 k_d。在未知脱密密钥的条件下由密文求解明文或脱密密钥的过程就是密码破译。

加密密钥和脱密密钥统称为密钥，它们是一一对应的，因而它们是成对出现的。为保证脱密工作的顺利进行，必须在加密之前将加密密钥 k_e 分配给加密方，并在脱密之前将脱密密钥 k_d 分配给合法的脱密方，这个过程称为密钥分配。为保证密钥的秘密性，密钥分配必须在安全信道上完成，确保密钥在分配过程中不被泄漏。

一个密码体制由明文空间 M、密文空间 C、密钥空间 K、加密算法 $E_{k_e}(m)$ 和脱密算法 $D_{k_d}(c)$ 五个部分组成。如果从函数的定义出发理解密码体制的概念，则密钥空间是密钥的取值集合，明文空间和密文空间分别是加密算法的定义域和值域，也是脱密算法的值域和定义域。其中，对 $\forall m \in M$ 和 $\forall k_e \in K$，都有

$$\begin{cases} c = E_{k_e}(m) \\ m = D_{k_d}(c) = D_{k_d}(E_{k_e}(m)) \end{cases}$$

因此，从函数的定义看，一个密码体制完全由其密码算法决定。因此也常将密码体制与密码算法不加区分。

密码通信系统的基本结构如图 2.1.1 所示。

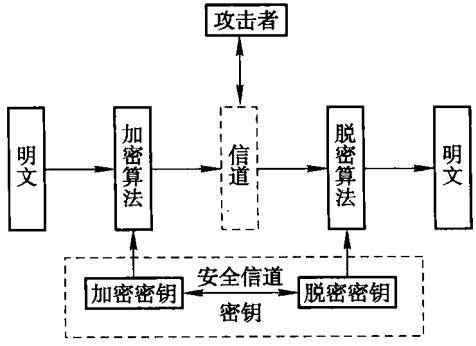

图 2.1.1 密码通信系统的基本结构

为达到保护信息机密性的目的，密码体制应当满足下述要求：

（1）密码体制即使达不到理论上的不可破性，也应当是实际上不可破的。也就是说，密码体制在实际上应当能够抵抗各种可能的攻击方法。

（2）一切秘密蕴涵于密钥之中。换句话说，只要敌手不知道密钥，就不能由已知的信息推出未知的明文信息。

（3）加密算法和脱密算法必须对密钥空间中的所有可能值都有定义，因安全强度不够而

不能使用的密钥应尽可能地少。

（4）密码体制应具有很好的实现性能，能够满足实际工作的需要。

如果一个密码体制的加密密钥与脱密密钥本质上是一个，即由其中一个可以很容易地推出另外一个，则称该密码体制是单密钥密码体制。单密钥密码体制又称为对称密钥密码体制、对称密码体制或单钥密码体制等。

如果一个密码体制的加密密钥可以公开，且由加密密钥在实际上不能推出秘密的脱密密钥，则称该密码体制是公开密钥密码体制。公开密钥密码体制又称为公钥密码体制、非对称密钥密码体制、双钥密码体制等。在公钥密码体制中，任何掌握公开密钥的人都可以加密信息，但只有掌握脱密密钥者才能脱密出明文。

信息认证算法就是对信息数据执行一个数学变换，变换的结果称为认证码。信息认证算法通过信息数据与认证码之间的制约关系，达到对信息数据的真实性进行认证的目的。当利用信息认证算法产生的认证码与信息数据自身携带的认证码不一致时，就可判断该信息数据和认证码至少有一个是不真实的。

因此，信息认证算法就是高效地为信息数据产生人为的冗余，并利用这种冗余检测信息的真实性。

信息认证算法应当保证既不能伪造一个匹配的信息数据-认证码，又不能通过对信息数据及其认证码的修改，产生一对匹配的信息数据-认证码。

信息认证算法由认证码生成算法和认证码检测算法组成，旨在解决不可抵赖性问题的信息认证算法还包括仲裁算法。利用仲裁算法，公正的第三方可对出现的争议进行仲裁。

信息认证算法可分为无密钥认证算法、单密钥认证算法和双密钥认证算法。无密钥认证算法和单密钥认证算法中可以没有仲裁算法。在无密钥认证算法中，由于产生认证码时不需要秘密密钥，因而任何人都可产生每个可能的信息数据的认证码，故无密钥认证算法只能检测出对信息数据无意的修改而不能检测出有意的篡改；在单密钥认证算法中，双方利用同一个秘密密钥生成和检测认证码；双密钥认证算法的密钥由公开密钥和秘密密钥组成，公开密钥与秘密密钥一一对应，但实际上由公开密钥推不出秘密密钥。对于双密钥认证算法，秘密密钥用于认证码的产生，公开密钥用于认证码的检测和仲裁。

1.2.2 密码分析学

密码分析学的主要任务是研究密码破译的理论与技术。密码破译包括信息加密算法的破译和信息认证算法的破译。信息加密算法的破译目的是获取非授权的信息，信息认证算法的破译目的是伪造合理的消息，以达到伪造和欺骗的目的。

密码算法对抗密码破译的能力称为密码算法的保密强度。在很多情况下，密码破译又称为密码分析。

密码破译总是在一定条件下进行的。因此，我们需要对敌手的攻击能力进行假设。最保

险的假设就是所谓的 Kerckhoffs 假设——假设敌手知道除秘密密钥之外的任何信息，其目的是求解未知的密钥或未知的明文。因此，Kerckhoffs 假设的原则就是所有的秘密蕴涵于密钥之中。

换句话说，我们应当假设敌手已掌握以下内容：

① 所使用的密码体制。

② 掌握明文的概率分布规律。

③ 掌握密钥的概率分布规律。

④ 掌握所有的破译方法。

密码体制的保密，无疑会增加密码破译的难度。但是，安全保密措施再好，密码体制也有泄漏的可能。因而，在分析密码体制的抗破译能力时，不应该假设密码体制是保密的。

此外，被加密的明文总具有一定的文意和格式，呈现特有的格式规律和统计规律，这种规律也称为明文的文字规律。明文的具体内容也总与当前发生的事件相关，这种规律也称为明文的情况规律。明文的文字规律和情况规律都是明文自身的内在规律，敌手是能够猜测出来而无法隐瞒的。明文和密钥的信息总是泄漏在密文、明文与密文的对照关系以及相关密钥的明文与密文的对照关系之中，因而总存在一定的信息泄漏。这种信息泄漏的规律又称为密码规律。

密码规律、文字规律和情况规律合称为密码破译中的三大规律。密码破译就是要发掘出密码算法的信息泄漏规律及其利用方法，并借助于文字规律和情况规律，恢复出密钥或明文。在密码破译中，找出可以利用的信息泄漏规律是最困难和最关键的。一个密码的破译总是首先要在这个方面取得突破。

根据敌手所掌握的信息的类别不同，可将对加密算法的攻击分为以下几种类型：

（1）唯密文攻击

敌手除具有上面列举的四项基本知识外，还掌握足够多的使用同一个密钥加密的密文。破译的目的是求出使用的密钥或对应的明文。

由于信道未必是安全信道，因而密文在信道上被截获是很正常的。特别是当密文在无线信道中传输时，更容易从无线信号中截获密文数据。因此，唯密文攻击的条件是很容易满足的。如果能够将密文在信道中隐藏起来，无疑会提高密码的抗攻击能力，但这已不属于密码学的范畴。

（2）已知明文攻击

敌手不仅具有唯密文攻击的条件，而且还掌握足够多的使用同一个密钥加密的密文及其对应的明文。破译的目的是求出使用的密钥或求出其他密文对应的明文。

已知明文攻击在现实中也是容易发生的。因为明文总有一定的文意和格式，敌手总能对某些明文的具体文意进行猜测。在很多情况下，加密的明文也可能会通过其他公开渠道公布出来。因此，密码算法必须能够经得起已知明文攻击的考验。

（3）选择明文攻击

敌手不仅具有已知明文攻击的条件，而且还可以任意选择对密码破译有利的足够多的明

文，并能得到对应的密文。破译的目的是求出使用的密钥或求出其他密文对应的明文。

在选择明文中，被选择的明文可以不再是随机的，所选择的不同的明文之间也可能具有一定的结构规律和制约规律。明文之间的这种相互制约性和不随机性，为密码破译提供了更多的信息，因而能够取得更好的破译效果。

（4）选择密文攻击

敌手不仅具有已知明文攻击的条件，而且还可以任意选择对密码破译有利的足够多的密文，并能得到对应的明文。破译的目的是求出使用的密钥或求出其他密文对应的明文。

在选择密文中，被选择的密文不必是随机的，所选择的不同的密文之间也可能具有一定的结构规律和制约规律。密文之间的这种相互制约性和不随机性，将为密码破译提供更多的信息，因而能够取得更好的破译效果。

选择密文攻击主要用于攻击公钥密码，特别是用于攻击数字签名算法。

（5）相关密钥攻击

敌手不仅具有选择明文攻击和选择密文攻击的条件，而且还能得到由所求密钥的相关密钥对他任意选择的明文加密所得的密文，以及对他任意选择的密文脱密所得的明文。

例如，假设 k 是秘密密钥，$IV_1, IV_2, \cdots, IV_n$ 是 n 个公开的数据，则

$$k \oplus IV_1, k \oplus IV_2, \cdots, k \oplus IV_n$$

就是相关密钥，同时利用由它们加密的明文和密文发起的对密钥 k 的攻击就是一种相关密钥攻击。其中 $\oplus$ 是逐位模 2 加运算。若设 $x_1, x_2, \cdots, x_m, y_1, y_2, \cdots, y_m \in \{0,1\}$，则逐位模 2 加运算 $\oplus$ 定义为

$$(x_1, x_2, \cdots, x_m) \oplus (y_1, y_2, \cdots, y_m) = (x_1 \oplus y_1, x_2 \oplus y_2, \cdots, x_m \oplus y_m)$$

其中对 $1 \leqslant i \leqslant m$，有

$$x_i \oplus y_i = (x_i + y_i) \bmod 2 = \begin{cases} 0, & \text{若} x_i = y_i; \\ 1, & \text{若} x_i \neq y_i. \end{cases}$$

是模 2 加运算（又称为逻辑异或），其运算结果就是 2 除整数 $x_i + y_i$ 所得的余数。

一个密钥的相关密钥是指对密码破译有利的、且与该密钥具有一定内在联系的密钥。

在上述几种攻击类型中，唯密文攻击所需的条件最弱，选择密钥攻击所需的条件最强。尽管一个攻击方法的条件在现实中有时很难满足，但一个攻击方法的成功至少说明密码算法的设计存在安全性缺陷，说明密码算法具有可被利用的信息泄漏，而且不能排除该算法可能存在更大的、未被人发现的安全性缺陷的可能。

从攻击的手段上分，密码分析者攻击密码主要有以下几类方法：

（1）穷举攻击

穷举攻击就是依次利用所有可能的密钥，对密文脱密求出相应的明文，并通过检测得到的明文是否与已掌握的明文信息完全一致的方法判断被测试密钥的真假，从而排除假设错误的密钥，最终达到求出正确密钥的目的。

穷举攻击是攻击密码算法的最基本方法。只要密钥的数量是有限的，在唯密文攻击条件下，总可以使用穷举攻击方法求解密钥。穷举攻击所需的时间代价是制约其性能的重要指标。如果密钥的总个数是 2^n，则平均需要测试 2^{n-1} 个密钥就可找到正确密钥。显然，只要增加可能密钥的个数，就可以对抗穷举攻击方法。

一个密码体制的可能密钥的个数称为密码算法的密钥变化量。在目前的技术条件下，密钥变化量是 2^{64} 的密码算法是不安全的。

例如，假设密钥的变化量是 2^{64}，又假设一台高性能密钥搜索设备每秒钟能够检测 2^{30} 个密钥，则每年能够检测

$$365\times 24\times 3\ 600\times 2^{30}=3.15\times 10^{7}\times 2^{30}\approx 2^{55}$$

个密钥，因而检测完 2^{64} 个密钥至多需要 $2^{64}\div 2^{55}=512$ 年。但是，如果同时使用 2 048 个这样的密钥搜索设备，那么检测完 2^{64} 个密钥只需三个月。如果使用更多的密钥搜索设备，穷举攻击的时间将会更短。

同样可以得出结论，按照目前的计算能力，密钥变化量为 2^{128} 的密码算法仍是安全的。

穷举攻击中所使用的设备，可能仅仅是几个 PC，也可能是大量的超级计算机，也可能是专用的密码破译设备，更可能是利用网络的优势，利用网络中的大量计算机的空闲时间进行破译。此时，穷举攻击的能力将会有成千倍甚至百万倍的提高。

穷举攻击的具体方法和性能指标分析将会在 4.4 节中详细分析。

（2）解析攻击

解析攻击又称为数学分析攻击，它是针对密码算法设计所依赖的数学问题，利用数学求解的方法破译密码。解析攻击是对基于数学难题求解的困难性设计的公钥密码的主要威胁。

（3）统计攻击

统计攻击就是利用明文、密文之间内在的统计规律破译密码的方法。对于设计得不是太简单的对称密码算法，成功的攻击方法基本上都是统计攻击。

（4）代数攻击

代数攻击方法就是将密码的破译问题归结为有限域上的某个低次的多元代数方程组的求解问题，并通过对代数方程组的求解，达到破译密码的目的。

1.2.3 密钥管理学

密钥管理学的主要研究内容有随机数生成理论与技术、密钥分配理论与方法、密钥分散管理技术、密钥分层管理技术、秘密共享技术、密钥托管技术、密钥销毁技术、密钥协议设计与分析技术等。

密钥管理技术总是与密码的具体应用环境和实际的密码系统相联系，总是与密码应用系统的设计相联系。在很多情况下，一个密码应用系统的被攻破往往不是密码算法被破造成的，而是密码系统的密钥管理方案不当造成的。

试读结束：需要全本请在线购买： www.ertongbook.com