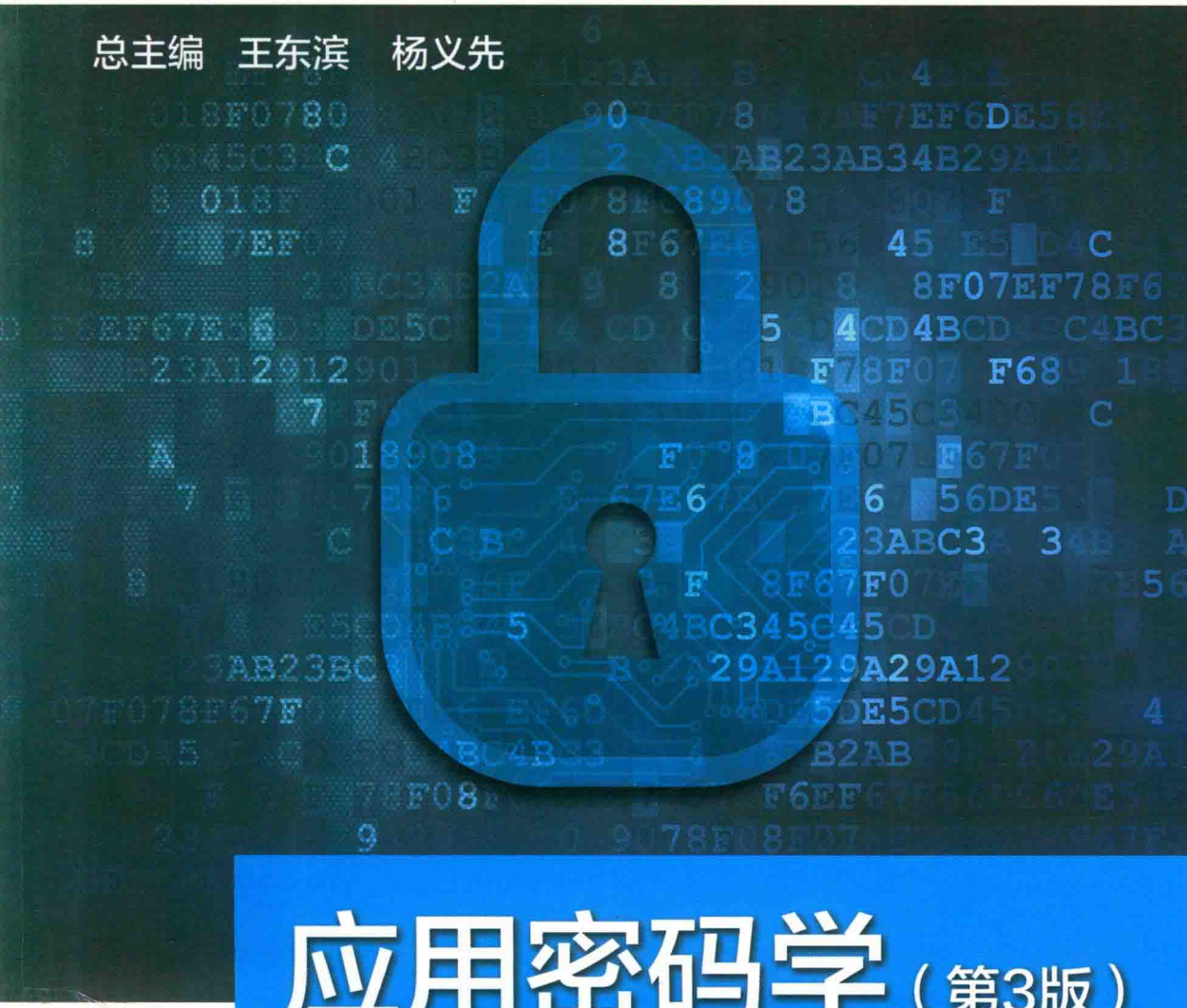
网络空间安全专业规划教材

总主编　王东滨　杨义先



应用密码学（第3版）

APPLIED CRYPTOGRAPHY

主编　雷　敏　杨义先

北京邮电大学出版社
www.buptpress.com

网络空间安全专业规划教材

总主编　王东滨　杨义先

应用密码学

（第3版）

主编　雷　敏　杨义先

北京邮电大学出版社
www. buptpress. com

内 容 简 介

信息安全的核心是密码，而应用密码学则是信息安全应用领域需要掌握的基础知识之一。本书对分组密码、公钥密码、密码杂凑函数、数字签名、认证与访问控制、云计算安全等进行了深入而系统的讲解。

本书内容全面，既有密码学的基本理论，又有应用密码学的关键技术；图文并茂，文字流畅，表述严谨。

本书可作为信息安全、密码学、网络空间安全等相关专业本科生和研究生的教材，也可作为信息处理、通信保密、网络空间安全、信息安全等领域科研人员和工程技术人员的参考书。

图书在版编目(CIP)数据

应用密码学 / 雷敏，杨义先主编. -- 3 版. -- 北京：北京邮电大学出版社，2022.4
ISBN 978-7-5635-6612-9

Ⅰ. ①应… Ⅱ. ①雷… ②杨… Ⅲ. ①密码术—高等学校—教材 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2022)第 043636 号

策划编辑：马晓仟　**责任编辑**：刘春棠　**封面设计**：七星博纳

出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号
邮政编码：100876
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：保定市中画美凯印刷有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：11
字　　数：270 千字
版　　次：2005 年 6 月第 1 版　2013 年 6 月第 2 版　2022 年 4 月第 3 版
印　　次：2022 年 4 月第 1 次印刷

ISBN 978-7-5635-6612-9　　定价：32.00 元

Prologue 序

Prologue

作为最新的国家一级学科，由于其罕见的特殊性，网络空间安全真可谓是典型的“在游泳中学游泳”。一方面，蜂拥而至的现实人才需求和紧迫的技术挑战促使我们必须以超常规手段来启动并建设好该一级学科；另一方面，由于缺乏国内外可资借鉴的经验，也没有足够的时间纠结于众多细节，所以，作为当初“教育部网络空间安全一级学科研究论证工作组”的八位专家之一，我有义务借此机会，向大家介绍一下2014年规划该学科的相关情况，并结合现状，坦陈一些不足，以及改进和完善计划，以使大家有一个宏观了解。

我们所指的网络空间，也就是媒体常说的赛博空间，意指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。它已成为继陆、海、空、太空之后的第五空间。网络空间里不仅包括通过网络互联而成的各种计算系统(各种智能终端)、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他四个空间不同，网络空间没有明确的、固定的边界，也没有集中的控制权威。

网络空间安全研究网络空间中的安全威胁和防护问题，即在有敌手对抗的环境下，研究信息在产生、传输、存储、处理的各个环节所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所涉及的信息保密性、完整性和可用性，还包括构成网络空间基础设施的安全和可信。

网络空间安全一级学科下设五个研究方向：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。

方向1，网络空间安全基础，为其他方向的研究提供理论、架构和方法学指导；它主要研究网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与

评测等内容。

方向2,密码学及其应用,为后三个方向(系统安全、网络安全和应用安全)提供密码机制;它主要研究对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等内容。

方向3,系统安全,保证网络空间中单元计算系统的安全;它主要研究芯片安全、系统软件安全、可信计算、虚拟化计算平台安全、恶意代码分析与防护、系统硬件和物理环境安全等内容。

方向4,网络安全,保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全;它主要研究通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御(攻防与对抗)、端到端的安全通信等内容。

方向5,应用安全,保证网络空间中大型应用系统的安全,也是安全机制在互联网应用或服务领域中的综合应用;它主要研究关键应用系统安全、社会网络安全(包括内容安全)、隐私保护、工控系统与物联网安全、先进计算安全等内容。

从基础知识体系角度看,网络空间安全一级学科主要由五个模块组成:网络空间安全基础、密码学基础、系统安全技术、网络安全技术和应用安全技术。

模块1,网络空间安全基础知识模块,包括数论、信息论、计算复杂性、操作系统、数据库、计算机组成、计算机网络、程序设计语言、网络空间安全导论、网络空间安全法律法规、网络空间安全管理基础。

模块2,密码学基础理论知识模块,包括对称密码、公钥密码、量子密码、密码分析技术、安全协议。

模块3,系统安全理论与技术知识模块,包括芯片安全、物理安全、可靠性技术、访问控制技术、操作系统安全、数据库安全、代码安全与软件漏洞挖掘、恶意代码分析与防御。

模块4,网络安全理论与技术知识模块,包括通信网络安全、无线通信安全、IPv6安全、防火墙技术、入侵检测与防御、VPN、网络安全协议、网络漏洞检测与防护、网络攻击与防护。

模块5,应用安全理论与技术知识模块,包括Web安全、数据存储与恢复、垃圾信息识别与过滤、舆情分析及预警、计算机数字取证、信息隐藏、电子政务安全、电子商务安全、云计算安全、物联网安全、大数据安全、隐私保护技术、数

字版权保护技术。

其实，从纯学术角度看，网络空间安全一级学科的支撑专业至少应该平等地包含信息安全专业、信息对抗专业、保密管理专业、网络空间安全专业、网络安全与执法专业等本科专业。但是，由于管理渠道等诸多原因，我们当初只重点考虑了信息安全专业，因此就留下了一些遗憾，甚至空白，比如，信息安全心理学、安全控制论、安全系统论等。不过值得庆幸的是，学界现在已经开始着手，填补这些空白。

北京邮电大学在网络空间安全相关学科和专业等方面，在全国高校中一直处于领先水平，从20世纪80年代初至今，已有30余年的全方位积累，而且一直就特别重视教学规范、课程建设、教材出版、实验培训等基本功。网络空间安全专业规划教材主要是由北京邮电大学的骨干教师们，结合自身特长和教学科研方面的成果，撰写而成。本系列教材暂由《信息安全数学基础》《网络安全》《汇编语言与逆向工程》《软件安全》《网络空间安全导论》《可信计算理论与技术》《网络空间安全治理》《大数据安全与隐私保护》《数字内容安全》《量子计算与后量子密码》《移动终端安全》《漏洞分析技术实验教程》《网络安全实验》《网络空间安全基础》《信息安全管理(第3版)》《网络安全法学》《信息隐藏与数字水印》等20余本本科生教材组成。这些教材主要涵盖信息安全专业和网络空间安全专业，今后，一旦时机成熟，我们将组织国内外更多的专家，针对信息对抗专业、保密管理专业、网络安全与执法专业等，出版更多、更好的教材，为网络空间安全一级学科提供更有力的支撑。

杨义先

教授、长江学者

国家杰出青年科学基金获得者

北京邮电大学信息安全中心主任

灾备技术国家工程实验室主任

公共大数据国家重点实验室主任

2017年4月，于花溪

前言

Foreword

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

为了更多、更快、更好地培养网络安全人才，国务院学位委员会、教育部于2015年6月决定在“工学”门类下增设“网络空间安全”一级学科。如今，许多高校都在努力培养网络安全人才，都在下大功夫、下大本钱聘请优秀老师，招收优秀学生，建设一流的网络空间安全学院。优秀的教材是网络空间安全专业人才培养的关键之一。而撰写教材是一项十分艰巨的任务。原因有二：其一，网络空间安全的涉及面非常广，知识体系庞杂、难以梳理；其二，网络空间安全的相关技术发展很快，因此教材内容也需要不断地更新。

当前许多院校都有“网络空间安全”和“信息安全”本科专业、硕士点或博士点。“应用密码学”课程已经成为信息安全专业或网络空间安全专业的重要课程，许多高校的相关专业（如计算机科学与技术、信息与计算科学、通信工程、电子信息工程、电子科学与技术、电子信息科学与技术、信息工程、数学与应用数学、电子商务等）也开设密码学相关的课程。

2020年1月1日，《中华人民共和国密码法》正式施行。国家鼓励和支持对密码科学技术的研究和应用，促进密码科学技术的进步和创新，加强密码人才培养和队伍建设，采取多种形式加强密码安全教育。2021年2月，教育部正式发布《教育部关于公布2020年度普通高等学校本科专业备案和审批结果的通知》及《列入普通高等学校本科专业目录的新专业名单（2021年）》，我国普通高等学校开设新专业“密码科学与技术”。近年来，密码学有了很大的发展，国产商用密码得到了大范围推广与应用。因此，作者对《应用密码学》第2版进行了修订。

《应用密码学》第3版对第2版的内容进行了调整，删除了第2版中的部分章节，使内容更加紧凑；在第2章公钥密码中增加了ElGamal公钥密码和国产商用密码算法SM2的相关内容；在第3章密码杂凑函数中增加了国产商用密码算法SM3的相关内容；将第4章数字签名修改为数字签名及其扩展，同时更新了该章的部分内容；将第5章访问控制修改为认证与访问控制，同时更新了该章的部分内容，增加了云计算安全的相关内容。另外，在每一章后面增加了思考题，在本书的最后增加了书中所有英文的缩略语。

本书可作为信息安全、密码学、网络空间安全等相关专业本科生和研究生的教材，也可

作为信息处理、通信保密、网络空间安全、信息安全等领域科研人员和工程技术人员的参考书。

本书在撰写过程中参考了国内外大量的文献,在此对这些文献的作者一并表示感谢。

由于作者水平有限,书中难免存在不妥之处,欢迎大家批评指正。

目录

Contents

绪　论

1. 基本概念

密码学是一门综合性学科，所需知识涵盖数学、物理、计算机、信息论、编码学和通信技术等多门学科。密码学研究信息与信息系统的安全，在保护信息的机密性和完整性等方面发挥着重要作用，而且还可以防止信息在生成、传递、处理和保存等过程中被未授权者非法提取、篡改、删除、重放和伪造等。

密码学(Cryptology)包含密码编码学(Cryptography)和密码分析学(Cryptanalysis)两个分支。密码编码学是对信息进行编码从而实现隐蔽信息的科学，其主要目的是寻求信息保密性(Privacy)和认证性(Authentication)的方法。密码分析学是研究密码破译的科学，其主要研究加密消息的破译或消息的伪造。密码编码学和密码分析学研究既相互对立又互相促进地向前发展。

密码学的基本思想是为保障通信双方信息的安全，将一种形式的消息变换为另外一种无授权难以读懂的消息。因此，从某种意义上讲，密码学也是研究消息“变换”方法的一门学科，将密码学中所用的各种变换方法称为密码算法。一次变换能够将有意义的明文(Plaintext)信息按照一组编码规则变换成密文(Ciphertext)信息，那么这个过程就称为加密(Encryption)，这组变换规则称为加密算法。如果合法用户使用一组变换规则能够将非授权者读不懂的密文信息变换成能看得懂的明文信息，那么这个过程称为解密(Decryption)，这组变换规则称为解密算法。多数密码算法都有一个“逆”算法，一般是成对出现和存在的。例如，一个加密算法的“逆”算法称为解密算法，一个签名算法的“逆”算法称为验证算法等。

加解密运算通常都是在一组密钥(Key)控制下进行的，加密算法用到的密钥称为加密密钥，解密算法用到的密钥称为解密密钥，签名算法用到的密钥称为签名密钥，验证算法用到的密钥称为验证密钥等。例如，加密密钥是一串特定的字符串，加密过程是指对明文按照指定的算法并使用加密密钥运行而产生相应的密文。一般说来，密钥越长，生成的密文破解难度就越大。

2. 密码体制概述

密码体制也称为密码系统，能完整地解决信息安全中的机密性、完整性、认证、身份识别、可控性及不可抵赖性等问题中的一个或多个问题。一个密码体制可以用图 0.1 表示。它由以下几部分组成：明文消息空间 M；密文消息空间 C；密钥空间 K_1 和 K_2，单钥体制下 $K_1=K_2=K$，此时密钥 k 需经过安全的密钥信道由发送方传给接收方；加密变换 E_{k1}，

$M\to C$，其中 $k_1\in K_1$，由加密器完成；解密变换 D_{k2}，$C\to M$，其中 $k_2\in K_2$，由解密器实现。称 $(M,C,K_1,K_2,E_{k1},D_{k2})$ 为一个密码体制，对于给定明文消息 $m\in M$、密钥 k(单钥体制下)或加密密钥 $k_1\in K$(双钥体制下)，加密变换将明文 m 变换为密文 c：

$$c=f(m,k_1)=E_{k1}(m),\qquad m\in M,k_1\in K_1$$

信息接收者利用安全信道传来的密钥 k(单钥体制下)或利用本地密钥发生器产生的解密密钥 $k_2\in K_2$(双钥体制下)控制解密操作 D，对收到的密文 m 进行变换得到恢复的明文消息：

$$m=D_{k2}(c),\qquad m\in M,k_2\in K_2$$

密码分析者是非授权的用户或机构，通过各种非法手段窃取信道中的密文信息，利用选定的变换函数 h，对截获的密文 c 进行变换，得到的明文是明文空间的某个元素：

$$m'=h(c),\qquad m\in M,k_2\in K_2$$

若 $m'=m$，那么密码分析者便成功地破译了密文信息。

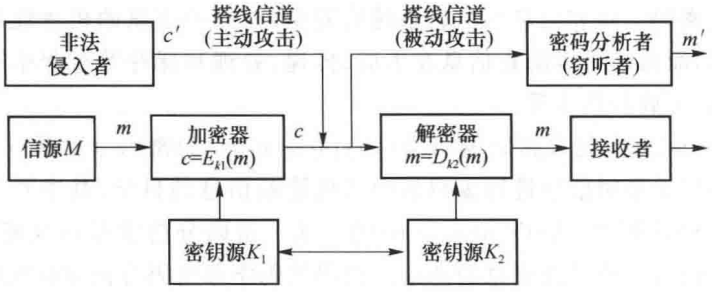


图 0.1　密码系统模型

3. 密码体制的分类

密码体制根据所使用加密算法的特点可分为单钥密码体制和双钥密码体制。

单钥密码体制又称为对称密码体制或私钥密码体制，加密和解密算法使用的密钥相同或实质上等同，即从一个密钥可以很容易推导出另一个密钥；双钥体制又称为公钥密码体制或非对称密码体制，加密和解密(签名和验证)算法使用的密钥不同，对于非授权者来说，很难从一个密钥推导出另一个密钥。

单钥密码体制的优点是保密强度高，而且计算的速度也比较快，缺点在于密钥必须通过安全可靠的途径传输，因此密钥管理成为影响系统安全性的关键因素，难以满足系统的开放性要求。

双钥加密的每个用户拥有一对密钥，称为公钥和私钥。公钥可以像电话号码一样公开，私钥仅对该用户可见，通信双方通过公钥传递信息，不需要交换私钥。双钥加密增加了私钥的安全性，密钥管理问题相对简单，适用于开放性的环境。它的主要缺点是加密效率不如单钥加密算法，尤其是在加密数据量较大的时候。

为充分利用双钥系统密钥分配的优点和单钥系统加密效率高的优点，在实际使用过程中常将双钥和单钥密码体制结合起来使用，工作原理是利用单钥密码算法对需要传输的明文信息进行加密，然后利用双钥密码算法对单钥密码的密钥进行加密，具体过程如下。

假设用户 A 与用户 B 要实现保密通信。首先用户 A 通过用户接口模块从双钥数据库中找到用户 B 的公钥，然后用户 A 选择一个随机数作为此次会话的加密密钥，即会话密钥，

会话密钥只在此次会话期间有效。用户 A 以会话密钥作为秘密密钥，采用对称密钥算法作为加密算法，对会话信息加密得到会话密文。紧接着，用户 A 以用户 B 的公钥对会话密钥进行加密，利用公钥密码算法为加密算法，得到会话密钥的密文。最后，用户 A 将会话密钥的密文及会话密文发送给用户 B。

用户 B 在收到用户 A 发来的包含会话密钥及会话内容的密文后，首先输入自己的私钥，利用解密算法恢复出会话密钥，再用会话密钥恢复出会话内容，至此，会话密钥的分配及一次会话过程就完成了。

由此可见，将非对称密钥算法与对称密钥加密算法相结合的方法可以安全地实现经由公开信道的密钥分配以及快速有效的保密通道的目的。

密码系统根据功能不同还可分为保密系统（Privacy System）和认证系统（Authentication System），前者用来实现消息的保密性，后者用来完成消息认证。传统的加密只使用单钥密码体制，其主要作用是实现消息的保密性，一般不提供消息的认证。公钥密码体制的诞生使得密码学不仅能够实现信息的保密性，还能完成信息认证。

认证系统随着计算机通信的普遍应用而迅速发展，已经成为密码学一个非常重要的组成部分，主要有以下几个方面的内容：消息认证（Message Authentication）、身份认证（Identification）和数字签名（Digital Signature）。前两者的目的是解决在相互信任的通信双方中，如何防止第三方伪装和破坏的问题。而数字签名则解决互不信任的通信双方，如何远距离迅速地利用电子签名代替传统的手写签名和印签的问题。

密码还可分为分组密码和序列密码。其中分组密码是应用最为广泛、影响最大的一种密码体制，其主要任务是提供数据保密性。

4. 密码杂凑函数

如何保证数据的完整性，防止数据被非法篡改是信息安全中非常重要的一个问题。保证数据完整性的方法很多，包括加密和数字签名等。如果只需保证数据的完整性而不需提供机密性和消息认证的话，则可通过对受保护的数据使用基于密码杂凑函数（也称为 Hash 函数）的消息认证码（MAC）来实现。

密码杂凑函数能将任意长度的输入映射为固定长度的输出，该输出称为消息摘要或散列和。SHA-1 是一个很有代表性的密码杂凑函数，它可将最大长度为 2^{64} 比特的输入映射成 160 比特的输出。密码杂凑函数为每个消息产生独一无二的散列值，且这个过程不可逆。计算消息摘要的过程如图 0.2 所示。

具体地说，理想的密码杂凑函数 $y=h(x)$ 应满足以下条件：

- 对于任意给定的 y，求出 x 使得 $h(x)=y$ 是困难的；
- 对于任意给定的 x，求出 z 使得 $h(x)=h(z)$ 是困难的；
- 求出 (x,z) 使得 $h(x)=h(z)$ 是困难的。

密码杂凑函数通过 MAC 来实现数据认证。数据认证是认证和数据完整性的结合。所谓的 MAC 计算如下：

$$\mathrm{MAC}(\mathrm{message})=f(\mathrm{Secret\ Key},\ \mathrm{message})$$

其中，函数 f(Secret Key, message)基于特定的密码杂凑函数组合。如果发信方和收信方都已经知道密钥，则收信方就可以将已知的密码杂凑函数、密钥以及消息结合得到 MAC，来检查发信方身份的真实性以及消息的完整性。但目前已经发现将密码杂凑函数用于密钥

及消息的连接,即计算 f(Secret Key, message)是不安全的,因此常使用嵌套的密码杂凑函数计算 MAC,如 f[Secret Key, f(Secret Key, message)]。

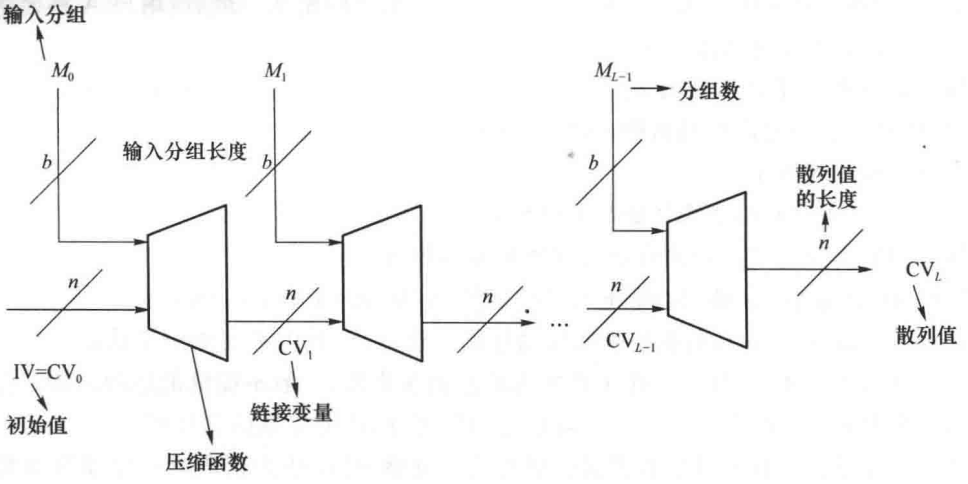


图 0.2　计算消息摘要的过程

密码杂凑函数的另一个重要应用是数字签名,它使消息的接收者能够验证发送者并且能验证消息自发送后未经改动。实现数字签名的过程如图 0.3 所示。

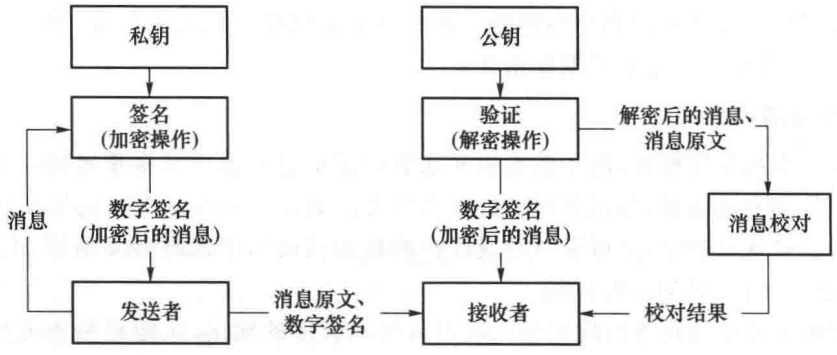


图 0.3　签名及验证过程

接收者将由签名解密得到的消息摘要与由明文经过密码杂凑函数得到的摘要进行对比,若两个摘要相同,则可以验证签名。

第1章 分组密码

1.1 分组密码

1.1.1 基本概念

分组密码是一种常用的密码体系，通俗地说就是利用密钥将一组一组明文消息等长地加密为密文消息，且一般情况下明文和密文等长。分组密码的优点是能够快速处理，而且节约存储空间，从而避免浪费带宽。分组密码的最大特点是容易标准化，由于其高强度、高速率、便于软硬件实现等特点成为标准化进程的首选体制。数据加密标准（Data Encryption Standard，DES）属于密码体制中的对称密码体制。作为数据加密标准，DES算法完全公开，任何个人和团体均可以使用，其信息的安全性取决于密钥的安全，这也正是现代分组密码的特征。

分组密码是将明文消息序列 $m_1, m_2, \cdots, m_k, \cdots$ 分成等长的消息组 $(m_1, m_2, \cdots, m_n)$，$(m_{n+1}, m_{n+2}, \cdots, m_{2n})$，$\cdots$。各组在密钥控制下，按固定的算法 E_k 一组一组地进行加密，加密后输出等长密文组 $(y_1, \cdots, y_m)$，$(y_{m+1}, \cdots, y_{2m})$，$\cdots$。分组密码的加密过程如图 1.1 所示。一个分组长为 n 比特、密钥长为 t 比特的分组密码，在数学上可以看作在 2^t 个密钥控制下的 $GF(2)^n \to GF(2)^m$ 的置换，用来加密的置换只是全体置换所构成集合的一个子集。

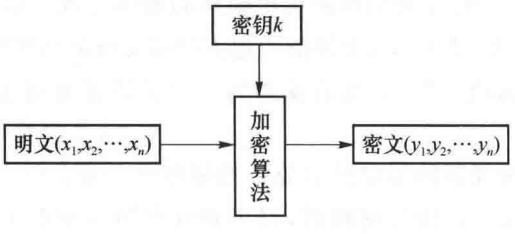


图 1.1 分组密码的加密过程

一般地，分组密码可以定义为如下一种映射：

$$F_2^n \times F_2^t \to F_2^m$$