密码学
理论与应用基础

王文海 蔡红昌
李新社 任 育 编著

MIMAXUE LILUN YU YINGYONG JICHU

国防工业出版社
National Defense Industry Press

密码学理论与应用基础

王文海　蔡红昌
李新社　任　育　编著

国防工业出版社
·北京·

图书在版编目(CIP)数据

密码学理论与应用基础/王文海等编著. —北京:国防工业出版社,2009.9

ISBN 978-7-118-06424-7

Ⅰ.密… Ⅱ.王… Ⅲ.密码-理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2009)第 099198 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 710×960 1/16 印张 14¼ 字数 247 千字

2009 年 9 月第 1 版第 1 次印刷 印数 1—3000 册 定价 36.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)68428422 发行邮购:(010)68414474

发行传真:(010)68411535 发行业务:(010)68472764

前　言

21 世纪信息时代的大门已经敞开，信息作为一种特殊的资源和财富，正引起人们的高度重视。人们的价值观念也在发生变化：信息就是财富，就是成功的机遇。谁占有了信息优势，谁就掌握了打开“财富宝库”的钥匙，获得成功的先机。在现代战争中，高技术远程精确制导武器的应用更加依赖于信息。先敌制胜，信息是基础。没有信息优势，就不可能夺取战争的主动权。信息战作为一种新的作战样式已经出现，“未战而先胜”的军事思想集中体现了信息优势在军事优势中的特殊地位。

信息在脆弱的公共信道上传输，在不设防的计算机系统中存储，很容易被其他未经授权的人截获、窃用、篡改和破坏。特别是一些重要信息，如个人信用信息、商业情报信息、工业技术情报信息、金融情报信息以及涉及国家重大利益的经济、政治、军事情报信息等，一旦被其他未经授权的人截获、窃用、篡改和破坏，就可能造成难以挽回的巨大损失！

军事情报信息历来是世界各个国家最敏感、最重要的信息。尤其是敌对国家的军事情报信息，双方都在秘而不宣地通过各种手段、渠道极力获取、窃用、篡改或破坏。如何才能确保一些重要信息即使被未经授权的人截获也不会被窃用、篡改和破坏呢？密码学理论和密码技术对这些问题进行了大量的研究并取得了许多重要成果。

密码学和数学一样有着古老的历史。早在数学体系建立之初，密码术就已经应用于传输一些重要的军事情报信息和指挥信息了。然而，现代密码学却是在 20 世纪 70 年代才开始出现的，至今只有短短 30 年左右的时间。因此可以说，现代密码学是一门既古老又年轻的科学。

现代密码学的发展，有两件值得称道的大事：一是 1977 年美国国家标准局正式公布实施数据加密标准（DES）和 DES 加密与解密算法，并批准用于商业保密通信，密码学神秘的面纱从此被揭开。二是 Diffie 和 Hellman 联合

撰写了一篇题为“密码学的新方向”的论文，提出了适用于网络保密通信的公钥密码体制的思想，掀起了公钥密码体制研究的热潮。受 Diffie 和 Hellman 公钥密码体制思想的启迪，各种公钥密码算法纷纷出现，特别是 Rivest、Shamir 和 Adleman 提出的基于幂剩余函数的 RSA 算法，在密码学发展史上竖起了一座划时代的里程碑。可以说，没有 RSA 算法的提出，就没有现代密码学耀眼的光辉。

密码学既属于应用数学，又属于计算机科学。更确切的说，它是应用数学与计算机科学之间的边沿学科。应用数学和计算机科学都是密码学研究的重要工具。在密码学的发展过程中，数学和计算机科学研究领域的学者都做出了卓越的贡献。数学和计算机科学中的许多分支，如数论、近世代数、信息论、椭圆曲线理论、算法复杂性理论、自动机理论、编码理论等，都可以在密码学理论体系中找到各自的位置。另外，密码学与通信科学、情报学也有着紧密的联系，它是通信科学领域解决信息安全传输问题和情报领域解决密码破译问题的主要理论基础。

中国不能没有自己的密码系统，中国也不能没有自己的密码标准。近年来，中国引进了很多新技术设备，唯有密码设备不能靠引进。引进密码设备，就好比将别人的耳目安装在自己的卧室里一样，不仅达不到保密的目的，反而会给别人提供窃密的方便。因此，中国培养密码学人才，开展密码学理论与密码技术研究是当务之急。

本书充分考虑目前国内高校信息安全教学实际，吸纳了一些常用教材的特点和精华内容。可作为大学本科信息安全专业密码学理论与应用基础课程的教材，主要内容分为 10 章，按 60 学时编写。

第 1 章为密码学引论，包括基本概念、算法分类、保密通信系统模型、密码体制的分类。

第 2 章为古典密码学，包括古典密码学中的基本运算、几种典型的古典密码体制、古典密码的统计分析。

第 3 章为密码学的数学基础，包括信息论、复杂性理论、数论、有限域上的离散对数等基本概念。

第 4 章为分组密码，包括分组密码概述、数据加密算法标准(DES)、高级数据加密标准(AES)、典型分组加密算法。

第5章为公钥密码体制，包括公钥密码简介、背包公钥密码算法、RSA算法、椭圆曲线密码、其它公钥密码(简介)。

第6章为序列密码，包括流密码的基本概念、移位寄存器与移位寄存器序列、线性反馈移位寄存器的表示、线性移位寄存器序列的极小多项式、m序列的伪随机性、流密码的破译。

第7章为密钥管理，包括密钥的组织结构、密钥的种类、密钥的产生、密钥分配、密钥协商。

第8章为数字签名，包括数字签名的定义和安全性、对数字签名的攻击、数字签名的分类、基本的数字签名方案、数字签名标准。

第9章为身份认证技术，包括身份认证技术的基本概念、认证协议、身份识别的零知识证明、基本的认证加密方案。

第10章为密码学应用，包括系统的安全性要求和设计目标、系统的基本设计、电子邮件系统设计、电子文件柜系统设计。

其中，第1章、第2章、第7章初稿由蔡红昌编写，第3章、第4章、第5章初稿由李悦编写，第6章、第8章、第9章初稿由任育编写，第10章初稿和第1章～第10章的全部习题由王文海编写。王文海教授还完成了第1章～第9章初稿核心部分内容的编写和全书终稿的统编、审修和校改工作。第二炮兵工程学院信息安全教研室主任李新社副教授对全书进行了终审校阅。

本书在正式公开出版之前，已被第二炮兵工程学院等军队院校遴选为信息安全专业(本科)的主用教材。通过教学实践，听取同行专家和学者的宝贵意见，由王文海教授在萃选和吸收学术研究最新成果的基础上，对各章节内容进行了改写、优化和充实，使本书更具有可读性，内容更加精炼和丰富。在此，谨向对本书提出宝贵意见的各位专家和学者表示衷心感谢。

2008年12月31日

目 录

第1章 密码学引论 …… 1

1.1 密码学概述 …… 1

1.2 基本概念 …… 2

1.2.1 常用术语 …… 2

1.2.2 算法分类 …… 3

1.2.3 保密通信系统模型 …… 5

1.2.4 哈希(Hash)函数 …… 5

1.3 密码体制的分类 …… 7

1.3.1 对称密码体制(Symmetric Encryption) …… 7

1.3.2 非对称密码体制(Asymmetric Encryption) …… 9

习题1 …… 10

第2章 古典密码学 …… 11

2.1 古典密码学中的基本运算 …… 12

2.1.1 单表古典密码中的基本加密运算 …… 12

2.1.2 多表古典密码中的基本加密运算 …… 15

2.2 几种典型的古典密码体制 …… 17

2.2.1 几种典型的单表古典密码体制 …… 17

2.2.2 几种典型的多表古典密码体制 …… 18

2.3 古典密码的统计分析 …… 23

2.3.1 单表古典密码体制的统计分析 …… 23

2.3.2 多表古典密码体制的统计分析 …… 28

习题2 …… 30

第3章 密码学的数学基础 …… 32

3.1 信息论 …… 32

3.1.1 信息 …… 32
3.1.2 信息量和熵 …… 33
3.2 复杂性理论 …… 35
3.2.1 算法 …… 35
3.2.2 算法的复杂性 …… 36
3.2.3 问题与问题的复杂性 …… 38
3.3 数论基础 …… 39
3.3.1 模运算 …… 39
3.3.2 素数 …… 41
3.3.3 最大公因数和最小公倍数 …… 42
3.3.4 求模逆元 …… 43
3.3.5 欧拉定理 …… 44
3.3.6 费马(Fermat)小定理 …… 44
3.3.7 中国剩余定理 …… 44
3.3.8 二次剩余 …… 45
3.4 有限域上的离散对数 …… 45
习题3 …… 46
第4章 分组密码 …… 47
4.1 分组密码概述 …… 47
4.1.1 分组密码的研究背景、意义及现状 …… 47
4.1.2 数学模型与设计思想 …… 50
4.2 数据加密算法标准(DES) …… 51
4.2.1 DES算法描述 …… 52
4.2.2 DES组织模式 …… 58
4.2.3 DES算法的安全性 …… 61
4.3 高级数据加密标准(AES) …… 62
4.3.1 AES的产生背景 …… 62
4.3.2 预备知识 …… 63
4.3.3 AES的算法描述 …… 63
4.4 典型分组加密算法 …… 67
4.4.1 IDEA算法 …… 67

4.4.2 RC5 算法 …… 71
习题4 …… 73
第5章 公钥密码体制 …… 75
5.1 公钥密码简介 …… 75
5.2 背包公钥密码算法 …… 78
5.2.1 背包问题 …… 78
5.2.2 背包公钥密码系统 …… 79
5.3 RSA 算法 …… 80
5.3.1 RSA 算法描述与数字签名 …… 80
5.3.2 对 RSA 算法的攻击 …… 82
* 5.3.3 基于 RSA 的分组随机密码新算法 …… 83
5.4 椭圆曲线密码 …… 90
5.4.1 椭圆曲线基础 …… 90
5.4.2 椭圆曲线密码体制 …… 93
5.5 其他公钥密码简介 …… 97
5.5.1 Diffie-Hellman 密码体制 …… 97
5.5.2 ElGamal 公钥加密算法 …… 99
5.5.3 Goldwasser-Micali 公钥加密算法 …… 100
习题5 …… 100
第6章 序列密码 …… 102
6.1 流密码的基本概念 …… 102
6.1.1 流密码的基本原理 …… 102
6.1.2 同步流密码 …… 104
6.1.3 密钥流产生器 …… 104
6.2 移位寄存器与移位寄存器序列 …… 105
6.3 线性反馈移位寄存器的表示 …… 107
6.3.1 线性反馈移位寄存器的一元多项式表示 …… 107
6.3.2 线性移位寄存器序列的周期性 …… 108
6.3.3 线性移位寄存器的序列空间 …… 109
6.4 线性移位寄存器序列的极小多项式 …… 109
6.5 *m* 序列的伪随机性 …… 112

6.6 流密码的破译 …… 114
6.6.1 流密码中的主要攻击方法 …… 115
6.6.2 m 序列的破译 …… 116
习题6 …… 119
第7章 密钥管理 …… 120
7.1 密钥的组织结构 …… 121
7.2 密钥的种类 …… 123
7.3 密钥生成 …… 124
7.3.1 密钥生成的制约条件 …… 124
7.3.2 如何生成密钥 …… 127
7.3.3 针对不同密钥类型的生成方法 …… 128
7.4 密钥分配 …… 129
7.4.1 单钥密码体制的密钥分配 …… 131
7.4.2 公钥密码体制的密钥分配 …… 134
7.5 密钥协商 …… 139
7.5.1 密钥协商举例 …… 139
7.5.2 Diffie – Hellman 密钥交换协议 …… 140
7.5.3 Shamir 协议 …… 142
7.5.4 身份认证协议 …… 143
7.5.5 其他密钥协商协议 …… 145
习题7 …… 146
第8章 数字签名 …… 147
8.1 数字签名的定义和安全性 …… 147
8.1.1 数字签名的一般定义 …… 148
8.1.2 数字签名的基本要素 …… 150
8.1.3 数字签名的产生方式 …… 151
8.1.4 数字签名安全性所基于的困难问题 …… 152
8.1.5 数字签名的执行方式 …… 154
8.1.6 数字签名安全性的证明方法 …… 155
8.2 数字签名的攻击 …… 156
8.3 数字签名的分类 …… 157

8.3.1 代理签名 …… 157
8.3.2 多方数字签名 …… 158
8.3.3 验证受限的数字签名 …… 158
8.3.4 群签名 …… 159
8.3.5 盲签名 …… 159
8.4 基本的数字签名方案 …… 159
8.4.1 Hash 签名 …… 159
8.4.2 基于素数域上离散对数问题的数字签名方案 …… 165
8.4.3 基于因数分解问题的签名方案 …… 168
8.5 数字签名标准 …… 169
8.5.1 数字签名标准 DSS …… 169
8.5.2 数字签名算法 DSA …… 170
习题 8 …… 171
第 9 章 身份认证技术 …… 172
9.1 身份认证技术的基本概念 …… 172
9.1.1 认证的概念 …… 172
9.1.2 身份识别 …… 173
9.1.3 身份识别的种类 …… 173
9.2 认证协议 …… 175
9.2.1 相互认证 …… 176
9.2.2 单向认证 …… 182
9.3 身份识别的零知识证明 …… 183
9.3.1 交互证明系统 …… 183
9.3.2 Fiat – Shamir 身份识别方案 …… 184
9.3.3 简化的 Fiat – Shamir 身份识别方案 …… 186
9.3.4 零知识证明 …… 188
9.4 基本的认证加密方案 …… 189
9.4.1 Nyberg – Rueppel 认证加密方案 …… 189
9.4.2 Zheng 签密方案 …… 190
9.4.3 Shin – Lee – Shim 签密方案 …… 191
习题 9 …… 192

第 10 章　密码学应用 …… 194
10.1　系统的安全性要求和设计目标 …… 194
10.1.1　现代密码体制的特点 …… 194
10.1.2　系统的安全性要求 …… 195
10.1.3　系统的设计目标 …… 195
10.2　系统的基本设计 …… 197
10.2.1　信文数据格式 …… 197
10.2.2　保密算法选择 …… 197
10.2.3　MIX 算法保密通信概要 …… 198
10.2.4　MIX 算法密钥管理概要 …… 199
10.2.5　MIX 算法密码通信处理 …… 204
10.3　电子邮件系统设计 …… 207
10.3.1　发信信箱与收信信箱数据模型 …… 207
10.3.2　电子邮件数据格式 …… 208
10.3.3　电子邮政管理程序 …… 208
10.4　电子文件柜系统设计 …… 209
习题 10 …… 213
参考文献 …… 214

第1章　密码学引论

1.1　密码学概述

密码学是以研究秘密通信为目的的一门科学，它主要包括两个分支：密码编码学和密码分析学。密码编码学主要研究对信息的加密和解密变换，以保护信息在信道的传输过程中不被通信双方以外的第三者窃用；而收信端则可凭借与发信端事先约定的密钥轻易地对信息进行解密还原。密码分析学则与密码编码学相反，它主要研究如何在不知密钥的前提下，通过唯密文分析来破译密码并获得信息。

密码编码学和密码分析学是同一问题的两个方面，两者的研究目的既是对立的，又是统一的。在对立中互相促进，在统一中共存发展。

密码学的历史极为久远，其起源可以追朔到远古时代，人类有记载的通信密码始于公元前400年。

密码学的发展可以分为三个阶段：古代加密方法、古典密码学和现代密码学。

古希腊墓碑的铭文、密写术以及帮会行话（黑道隐语）都是古代加密方法，这种加密方法已体现了密码学的若干要素，但只能限制在一定范围内使用。

古典密码一般采用手工或机械变换的方式实现，它比古代加密方法更复杂，但其密钥变化量仍然比较小。古典密码时期的密码系统已经初步呈现出现代密码系统的雏形并和数学联姻。古典密码的加密方法一般是文字替换，使用手工或机械变换的方式实现。古典密码的代表密码体制主要有单表代替密码、多表代替密码以及转轮密码。

1949年，Claude E. Shannon发表了“保密系统的通信理论”，1976年，W. Diffie和M. Hellmen发表了“密码学的新方向”，这两篇重要的论文和1977年美国实施的《数据加密标准（DES）》，标志着密码学的理论与技术的划时代的变革，宣告了近代密码学的开始。近代密码学与数学计算机技术、电子通信技术紧密相关。在这一阶段，密码理论蓬勃发展，密码算法设计与分析互相促进，出现了大量的密码算法和各种攻击方法。另外，密码使用范围也在不断扩张，而且出

现了许多通用的加密标准,促进了网络和技术的发展。

目前,计算机网络技术迅速发展,由计算机网络通信而带来的网络安全问题引起了人们的普遍关注,作为网络安全基础理论之一的密码学引起了人们的高度重视,吸引着越来越多的研究人员投入到密码领域的研究当中;同时,由于现实生活当中的实际需要以及计算技术的发展变化,密码学的每一个研究领域都出现了许多新的课题、新的方向。例如,在分组密码领域,由于 DES 已经无法满足高保密性的要求,美国于 1997 年 1 月开始征集新一代数据加密标准 AES(即高级数据加密标准,Advanced Encryption Standard)。2000 年 10 月 2 日,正式宣布选择比利时密码学家所开发的 Rijndael 算法成为 AES 的最终算法。AES 征集活动使国际密码学界又掀起了一次分组密码研究高潮。另外,由于嵌入式系统的发展、智能卡的应用,这些设备上所使用的密码算法由于系统资源本身的限制,要求密码算法可以以较小的资源快速实现,这样,公开密钥密码的快速实现成为了一个新的研究热点。最后,随着其他技术的发展,一些具有潜在密码应用价值的技术也逐渐得到了密码学家的重视,出现了一些新的密码技术。

随着计算机和通信技术的迅猛发展,大量敏感信息要通过公共信息设施或计算机网络进行交换,大量个人信息需要保密,密码学的商业和社会价值日益显著,它与人们的日常生活愈加密切相关。

1.2 基本概念

为了有助于理解密码学中的基本概念,先介绍几个常用术语。

1.2.1 常用术语

密码学的基本思想是将一种形式的信息变换成另外一种形式的信息。因此,从某种意义上讲,密码学也是研究信息变换方法的一门科学。我们把密码学中用到的各种变换称为密码算法。如果一个变换能够将一个意义明确的信息(称为明文)变换成意义不明的乱码(称为密文),从而使非授权者难以解读信息的意义,那么这个变换就称为加密算法。把明文转换成密文的过程称为加密。如果一个变换能够将一个意义不明的乱码变换成意义明确的信息,那么这个变换就称为解密算法(或脱密算法)。把密文恢复(还原)成明文的过程称为解密(或脱密)。如果一个变换能将一个信息变换成一种“证据”,用来验证某个实体对信息内容的认可,那么这个变换就称为一个签名。

在现代密码算法中,加密算法和解密算法是彼此互逆的两个变换,签名算法和和验证算法也是彼此互逆的两个变换。彼此互逆的两个变换通常都是在一组

密钥(Key)的控制下实现的。密钥是一组特定的秘密数据,它不仅能在加密时控制密码算法按照指定的方式将明文变换成相应的密文,并将一组信源标识信息变换成不可伪造的"签名";而且能在解密时控制密码算法按照指定的方式将密文变换成相应的明文,并将"签名"信息变换成不可否认的信源"证据"。加密算法中用到的密钥称为加密钥,解密算法用到的密钥称为解密钥(或脱密钥),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。一般说来,密钥长度越大,相应的密文就越安全。

加密算法和解密算法以及签名算法和验证算法都必须是整数算法。所谓整数算法,即当参与各种计算的所有数据都是整数时,其计算结果也是整数。

1.2.2 算法分类

根据所用加密算法的特点,密码体制(Cryptosystem)可以分为单钥密码体制(又称对称密码体制或私钥密码体制)和双钥密码体制(又称非对称密码体制或公钥密码体制)两种。在单钥密码体制中,加密与解密算法使用的密钥相同,或者由一个可以推出另一个,即知道了加密钥也就知道了解密钥。在双钥密码体制中,加密与解密(或签名与验证)算法使用不同的密钥(发信者使用收信者的公钥进行加密,收信者使用自己的私钥进行解密);收信者以外的任何非授权者都很难从一个公钥得到一个相适配的私钥,因此,收信者以外的任何非授权者都很难对密文进行解密。

注意:单钥密码体制不支持签名与验证。

单钥密码体制的优点是具有很高的保密强度和加密速度,一些常用的单钥加密方法明显地快于任何当前可以使用的双钥加密方法。单钥加密体制的缺点在于它的密钥必须通过安全可靠的途径传输,密钥管理成为影响系统安全性的关键因素,使它难以满足系统的开放性要求。

双钥加密的主要优点是增加了私钥的安全性,密钥管理问题相对简单、方便,可适用开放性的环境。它的主要缺点是在相同密钥长度的前提下,保密强度不如单钥密码体制高,且加密速度也不如单钥加密算法快,尤其是在加密数据量较大时更是如此。

实际工程中常采取的解决办法是将双钥密码体制和单钥密码体制结合起来,充分利用双钥系统密钥管理简单、方便的优点和单钥系统加密速度快的优点,构成混合密钥体制。这种混合密钥体制的工作原理如下:

假设用户 A 与用户 B 要实现保密通信。首先,用户 A 从公钥数据库中找到用户 B 的公钥 Bp_k,然后,用户 A 选择一个本次会话所使用的加密钥(即会话密钥)H_k。会话密钥 H_k 只在本次会话期间有效。用户 A 采用公钥算法 Fp(·)和

用户 B 的公钥 Bp_k 对会话密钥 H_k 进行加密，用户 B 收到后再采用相同的公钥算法 Fp(·)和自己的私钥 Bs_k 进行解密，从而得到会话密钥 H_k。至此，用户 A 和用户 B 之间的会话密钥传输就完成了。然后，用户 A 再采用单密钥算法 Fs(·)和会话密钥 H_k 对信息(明文)进行加密(生成密文)，用户 B 收到后则采用相同的单密钥算法 Fs(·)和会话密钥 H_k 进行解密，从而将密文恢复(还原)成明文。至此，用户 A 和用户 B 之间的一次会话(通信)过程就结束了。

混合密钥体制的工作原理如图 1.1 所示。

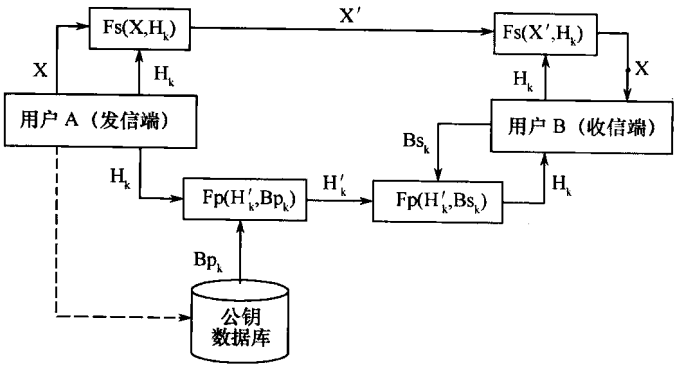

图 1.1　混合密钥体制的工作原理图

由此可见，采用将双密钥算法与单密钥算法相结合的方法，不仅可以简单、方便、安全地实现通过公开信道传输密钥，而且可以实现对信息进行快速加密和快速通信。

根据功能和应用目的不同，密码系统分为保密系统(Privacy System)和认证系统(Authentication System)两种。密码系统用来实现信息的保密性，认证系统用来实现信息的可信性和完整性。认证系统是最近 20 年来随着计算机通信的普遍应用而迅速发展起来的，现在它已成为密码学的一个非常重要的组成部分。

认证系统主要包括以下几个方面的内容：信息认证(Message Authentiction)、身份认证(Identification)、数字签名(Digital Signature)。前两者的目的是解决如何防止第三方篡改、伪造、假冒和欺骗的问题，而后者则是解决当通信双方(比如商业竞争对手)缺乏互信时，如何远距离迅速地用电子签名代替传统的手写签名以防止否认和抵赖的问题。传统的密码系统仅采用单钥密码体制，主要是用于实现信息的保密性，不支持信息认证和身份认证(因而不能实现信息的可信性和完整性)。

1976 年，Diffie 和 Hellman 发表了著名论文“密码学的新方向”，提出了公钥密码体制的概念，对密码学的发展和应用产生了划时代的影响。公钥密码体制

是现代密码学的里程碑,其显著特点是:它不仅可用于实现信息的保密性,而且还支持信息认证和身份认证(所以能实现信息的可信性和完整性)。

1.2.3 保密通信系统模型

一个密码通信系统由以下几部分组成:明文信息空间 M,密文信息空间 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信端传给收信端),加密变换 E_{k_1}(实现 $m\rightarrow c$,由加密器完成,$m\in M, c\in C$,$k_1\in K_1$ 为加密钥),解密变换 D_{k_2}(实现 $c\rightarrow m$,由解密器完成,$m\in M, c\in C, k_2\in K_2$ 为解密钥),称$(M, C, K_1, K_2, E_{k_1}, D_{k_2})$为一保密系统,如图 1.2 所示。

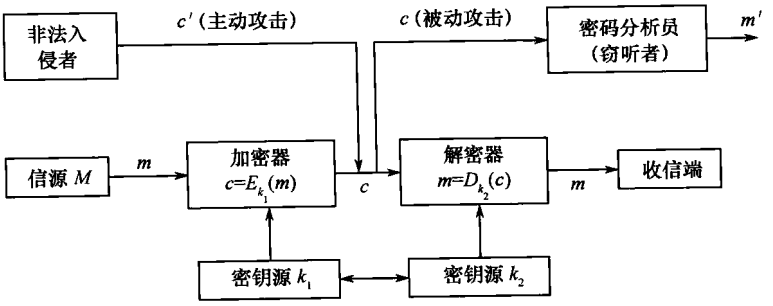

图 1.2 密码系统模型

发信端对于给定明文信息 m 和密钥 k_1,应用加密算法将明文 m 变换为密文 c,即

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

并通过专用秘密信道将解密钥 k_2(单钥密码体制 $k_2=k_1$,双钥密码体制 $k_2\neq k_1$)传送给收信端。

收信端收到密文 c 和解密钥 k_2 后,应用解密算法将密文 c 变换成明文 m,即

$$m=f^{-1}(c,k_2)=D_{k_2}(c), m\in M, k_2\in K_2, c\in C$$

而密码分析者则利用其选定的变换函数 g 和试验密钥 k_t 对截获的密文 c 进行破译,得到的是明文空间 M 中的某个元素 m',即

$$m'=g(c,k_t), m'\in M, k_t\in K_2, c\in C$$

一般来说,$m'\neq m$ 概率非常低。如果 $m'=m$,那么密码分析者便成功地完成了破译任务。

1.2.4 哈希(Hash)函数

如何保证数据的完整性,防止数据被非法篡改是一个非常重要的现实问题。