应用密码学

杨义先　钮心忻　编著

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所有人员必须了解的基础知识。作为相关专业的研究生教材，本书对密码学基础、数据加密标准(DES)、高级数据加密标准(AES)、典型分组加密算法、RSA密码的软硬件实现、高速加密卡、椭圆曲线密码、序列密码基础、序列密码乱源、序列密码设计、序列密码强度评估等加密知识和数字签名基础、代理签名、多重签名、盲签名、PKI、WPKI、PMI、AAA系统、口令认证、身份认证、访问控制、密钥管理等认证知识以及VPN、IPSec协议等应用知识进行了深入而系统地描述，并通过多个实用系统全面剖析了相关的密码应用。

本研究生教材内容全面，既有密码学的基本理论，又有应用密码的关键技术，还有当前热门的实用案例介绍。全书图文并茂，文字流畅，表述严谨，包含了应用密码方面的许多国际最新进展和发展趋势。本书的初衷虽然是通信、计算机、信息安全、密码学等相关专业的研究生教材，但是，本书也可以广泛适用于从事信息处理、通信保密、计算机等领域的科研人员和工程技术人员等。

图书在版编目(CIP)数据

应用密码学/杨义先，钮心忻编著 .—北京：北京邮电大学出版社，2005

ISBN 7-5635-1065-6

Ⅰ.应… Ⅱ.①杨…②钮… Ⅲ.密码—理论 Ⅳ.TN·918.1

中国版本图书馆CIP数据核字(2005)第031481号

书　　名：应用密码学
编　　著：杨义先　钮心忻
责任编辑：李欣一
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(100876)
电话传真：010-62282185(发行部)　010-62283578(FAX)
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×1 092 mm　1/16
印　　张：18.75
字　　数：461千字
印　　数：1—3 000册
版　　次：2005年6月第1版　2005年6月第1次印刷

ISBN 7-5635-1065-6/TN·378　　定　价：29.00元

前　言

到目前为止，国内正式开设信息安全本科专业的高等院校已经超过50所，拥有“信息安全”或“密码学”硕士点或博士点的高校就更多了。“应用密码学”课程已经成为信息安全专业或密码学专业的必修课，同时还是许多高校相关专业（比如，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、计算机科学与技术、信息工程、信息与计算科学、数学与应用数学、电子商务等专业）的主要选修课。此外，社会上从事信息处理、通信保密、计算机等领域的科研人员和工程技术人员等也需要从应用角度全面了解密码学。与应用密码学的巨大社会需求形成鲜明对比的是：到目前为止，国内出版的应用密码学研究生教材不多，理想教材就更少了，有些外行翻译教材不但文字不通，甚至差错连篇，不可用！介于此种情况，北京邮电大学信息安全中心的全体二百余位研学人员决定在过去20年密码学研究积累的基础上，借助于相关老师近十年的应用密码学和现代密码学讲义精华，协力编著此本教材，希望能够缓解国内信息安全与密码学相关人才培养的瓶颈问题。

本书共分为3篇：加密、认证和应用。

加密篇分为3章（分组密码、公钥密码、序列密码）涉及密码学基础（分组密码的数学模型、设计原则、安全性分析和密钥管理）、数据加密标准（设计思想、算法描述、工作模式、安全性分析）、高级数据加密标准（背景、数学基础、算法描述、安全性分析）、典型分组加密算法（Camellia密码加密算法、IDEA加密算法、RC4加密算法、Feistel网络的优化）、RSA密码的软硬件实现（算法描述、参数选择、软件实现、加速算法、硬件实现等）、高速加密卡（整体架构、智能卡技术、PCI设备驱动、板上操作系统）、椭圆曲线密码（椭圆曲线基础、加密、密钥协商、签密）、序列密码基础（原则、实现、移位寄存器、应用）、序列密码乱源（移位寄存器的串联和并联、它控采样序列、背包序列、基于LFSP的序列）、序列密码设计（总体编制、密钥设计、算法设计、设计模式）、序列密码强度评估（序列密码的分析要点、编制的强度评估和密钥流的强度评估）等加密基础知识。

认证篇分为3章（数字签名、公钥基础设施、接入控制）涉及数字签名基础（基本概念、基于因子分解的数字签名、基于离散对数的数字签名、同时基于多个数学难题的数字签名）、代理签名（基于离散对数的代理签名、基于因子分解的代理签名、多级代理签名）、多重签名与多重代理签名、盲签名与盲代表签名（基于DSA变形的盲签名、基于Nyberg-Rueppel签名方案的盲签名、基于DSA变形的盲代理签名、基于Nyberg-Rueppel签名方案的盲代理签名）、PKI（概论、模块、结构、互通）、WPKI（组成、证书、优化、管理）、PMI（权限管理技术、PMI技

术、权限管理系统设计、基于PMI的安全应用)、AAA系统(AAA平台功能概述、单点登录模型、基于PKI的单点登录方案、AAA服务器的关键协议)、口令认证(简单口令、一次口令机制、强口令的组合攻击、Peyravian-Zunic口令系统)、身份认证(挑战握手认证协议、双因子身份认证协议、S/KEY认证协议、Kerberos认证协议)、访问控制(访问控制模型、简单访问控制、基于角色的访问控制、实例介绍)、密钥管理(密钥协商、密钥认证、密钥共享、密钥托管)等认证方面的理论和技术。

应用篇(虚拟专用网)涉及VPN关键技术(VPN的原理与构成、特点与实现、隧道技术、类型)、IPSec协议(协议架构、AH协议、ESP协议、IKE协议)、IPSec VPN的体系结构(基于主机BITS方案的IPSec VPN、IPv4/IPv6混合网络下的IPSec VPN、基于群集技术的高速VPN、嵌入式VPN模型)、基于IPSec协议的完整VPN系统(安全网关的实现、客户端IPSec协议的实现、精简内核系统、设备管理)等典型的应用技术与系统。

本教材的特点可以归纳为

1. 突出应用性。全书不但对密码学的基本理论和关键技术有系统而深入的介绍,而且还介绍了许多非常实用的热门案例,因此,更适合于当前的国内现状。

2. 内容新颖成熟。追求成熟稳定是教材的立足点,但是,本书不但对成熟的密码应用有深入的介绍,而且,还对许多国际前沿的应用进行了详细剖析,读者从中可学到不少实用价值很大的知识。

3. 图文并茂的描述方式使得读者可以很容易对相关内容产生深刻的印象。

4. 全书的逻辑体系结构也十分有助于读者在把握全局的同时,深入了解局部知识。

5. 读者对象广泛。作为国内应用密码学方面不多的一本研究生教材,本书的主要读者当然是通信、计算机、信息安全、密码学等相关专业的研究生,但是,本书也可以广泛适用于从事信息处理、通信保密、计算机等领域的科研人员和工程技术人员等。为了使本书既能够面向初学者又能够面向专家,本书每章都给出了不少参考文献供有兴趣的读者查阅。

6. 本书尽量避免出现大量的数学公式和推理证明,各个章节尽量保持独立完整,因此,本教材的讲授可有多种形式的组合。对理论要求较高的专业可重点讲授第1、3、4章;对技术要求较高的专业可重点讲授第1、2、5、6章;对应用要求较高的专业可重点讲授第1、5、6章;对系统集成要求较高的专业可重点讲授第2、5、6、7章;对产品感兴趣的工程师可重点阅读第2、5、7章。建议读者根据自己的需要,先浏览本书目录,然后选定自己的阅读顺序。

讲授进度方面的考虑:本书编著之时就充分考虑了不同专业讲授此课程的课时安排差异。本书可同时适应于60学时和40学时的课程安排,进度控制主要依靠理论推导和具体应用系统细节的简与繁。对60学时的课程建议讲授进度为:第1、2、3章各10学时;第4、5两章各7学时;第6、7章各5学时。对40学时的课程建议讲授进度为:第1、2、3章各6学时;第5、6、7章各5学时;第4章5学时。

本书是北京邮电大学信息安全中心全体师生集体智慧的结晶,许多博士和硕士都在不同程度上参与了本书的素材提供和选择,我们在每章的参考文献之前列出了相关章节的主

要贡献者。特别感谢胡正名教授、李中献副教授、徐国爱副教授、卓新建副教授、罗群教授、张茹博士、崔宝江博士、周亚建博士后、罗守山教授、牛少彰教授、温巧燕教授、李新博士、张振涛博士、夏光升博士等。他们同心协力，率领北京邮电大学信息安全中心两百余位研究人员在网络信息安全研究的丰富成果是本书的营养源泉。

感谢北京邮电大学数字内容研究中心的大力协助。

本书也是国家自然科学基金(60372094，90204017，60473016)、国家“973”项目(编号：G1999035804)、北京市自然科学基金(4042022)、教育部优秀青年教师资助计划项目、国家863项目(2005AA143040)的成果总结，特此致谢。

由于作者水平有限，书中难免出现各种失误和不当之处，欢迎大家批评指正。

作　者

2004年12月于北京

目　　录

第一篇　加　　密

第1章　分组密码

第2章　公钥密码

第二篇　认　　证

第4章　数字签名

第5章　公钥基础设施

第一篇

加密

第1章 分组密码

1.1 密码学基础

1.1.1 基本概念

1. 常用名词术语

密码学的主要任务是解决信息的保密性和可认证性问题，即保证信息在生成、传递、处理、保存等过程中不能被未授权者非法地提取、窜改、删除、重放和伪造等。密码学本身也是一门正在迅速发展的综合性新学科。密码学所需要的知识横跨数学、物理、计算机、信息论、编码学、通信技术等多种学科。密码学是信息安全的核心，它为解决信息安全问题提供了许多有效的核心技术，在保护信息的机密性、认证性等方面发挥着关键性的作用。

简单地说，密码学(Cryptology)是研究信息系统安全的一门科学。它主要包括两个分支，即密码编码学(Cryptography)和密码分析学(Cryptanalysis)。密码编码学是对信息进行编码实现隐蔽信息的一门学问，其主要目的是寻求保护信息保密性(Privacy)和认证性(Authentication)的方法。密码分析学是研究分析破译密码的学问，其主要目的是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相互对立，而又互相促进地向前发展。

密码学的基本思想是将一种形式的消息变换成另外一种形式的消息。因此，从某种意义上讲，密码学也是研究消息“变换”方法的一门科学。我们称密码学中用到的各种变换为密码算法。例如，如果一个变换能够将一个有意义的消息(称为明文)变换成无意义的消息(称为密文)，从而使非授权者难以读取明文的内容，那么称这个变换为加密算法。把可读的“明文”信息转换成不可读的“密文”信息的过程叫做加密。如果合法用户用一个变换能够将一个非授权者读不懂的信息变换成有意义的信息，那么称这个变换为解密算法(或脱密算法)。由合法用户把已加密的信息(密文)恢复成明文的过程叫做解密。如果一个变换能将一个消息变换成一种“证据”，用来证明某个实体对消息内容的认可，那么称这个变换为一个签名算法。

多数密码算法一般都有一个“逆”算法，他们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。这些算法的运算通常都是在一组密钥(Key)的控制下进行的。密钥是一种特定的值，它能够使密码算法按照指定的方式运行并产生相应的密文。一般说来，密钥长度越大，相应的密文就越安全，如，加密算法中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。

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(又称为对称密码体制，或私钥密码体制)和双钥体制(又称为公钥密码体制，或非对称密码体制)两种。在单钥密码体制中，一对加密和解密(或签名和验证)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地得出另一个密钥；在双钥体制中，加密和解密(或签名和验证)算法使用的密钥不同，而且对于非授权者来说，他很难从一个密钥得到另一个密钥。

单钥密码体制的优点是具有很高的保密强度，可以达到经受国家级破译力量的分析和攻击。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，可适用开放性的环境。它的主要缺点是保密强度的人为控制力度不如对称密码体制的水平，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。

实际工程中常采取的解决办法是将双钥和单钥密码体制结合起来，充分利用双钥系统密钥分配方面的优点和单钥系统速度方面的优点。这种系统的工作原理是：

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，通过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。

根据功能不同，密码系统可分为：保密系统(Privacy System)和认证系统(Authentication System)两种。前者用来保护消息的保密性，后者用来保护消息的认证性。虽然认证系统是最近 20 年来随着计算机通信的普遍应用而迅速发展起来的，但是它已成为密码学的一个非常重要的组成部分。认证系统主要有以下几个方面的内容：消息认证(Message Authentication)、身份认证(Identification)、数字签名(Digital Signature)。前两者的目的是解决在通信双方利害一致的条件下，如何防止第三方伪装和破坏的问题。而数字签名则解决了当通信双方并不互相信任(比如，他们是竞争对手)时，如何远距离迅速地用电子签名代替传统的手写签名和印签的问题。传统的加密只使用单钥密码体制，而且其主要作用是保护消息的保密性，一般不提供消息的认证性。1976 年，Diffie 和 Hellman 发表了他们的著名论文《密码学的新方向》，提出了公钥密码体制的概念，给密码学的发展和应用带来了革命性的变革。公钥密码体制的显著特点是可以提供信息的认证性。公钥密码体制的诞生，使得密码学不仅能够保护信息的保密性，而且还能够提供信息的认证性。

3. 保密通信系统模型

一个密码通信系统可以用图 1.1 表示。它由以下几部分组成：明文消息空间 M；密文消息空间 E；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}，$M\to E$，其中 $k_1\in K_1$，由加密器完成；解密变换 D_{k2}，$E\to M$，其中 $k_2\in K_2$，由解密器实现。称总体$(M,E,K_1,K_2,E_{k1},D_{k2})$为一保密系统。对于给定明文消息 $m\in M$，密钥 $k_1\in K$，加密变换将明文 m 变换为密文 c：

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

接收端利用通过安全信道送来的密钥 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，对收到的密文进行变换得到恢复的明文消息：

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

而密码分析者则利用其选定的变换函数 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：

$$m'=h(c),\quad m\in M,k_2\in K_2。$$

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

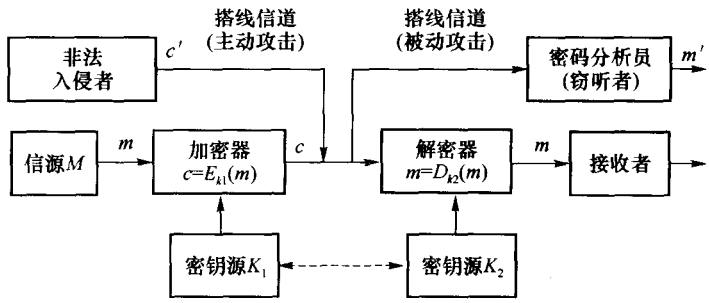

图 1.1　密码系统模型

4. 哈希函数

如何保证数据的完整性，防止数据被非法窜改是一个非常重要的现实问题。实现数据完整性的手段很多，包括加密、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，则可通过对受保护的数据使用基于哈希(Hash)函数的消息认证码(MAC)来实现。

哈希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哈希和。哈希函数对每个消息给出一个不同的值，也就是说，为每个消息产生独一无二的哈希值，并且这个过程是不可逆的。计算消息哈希值(或称为消息摘要)的过程如图 1.2 所示。

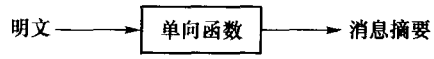

图 1.2　计算消息摘要的过程

SHA-1 是一个很有代表性的哈希函数，它可将最大长度为 2^{64} bit 的输入映射成 160 bit 的输出。因为所有输入组成的集合远大于所有输出组成的集合，所以必然有多个输入映射到同一个输出。

具体地说，理想的哈希函数 $y=h(x)$ 应满足以下条件：如果要做到

(1) 对于任意给定的 y,求出 x 使得 $h(x)=y$;

(2) 对于任意给定的 x,求出 z 使得 $h(x)=h(z)$;

(3) 求出 (x,z) 使得 $h(x)=h(z)$。

要找到映射到同一个输出的多个输入在计算上是很困难的。

目前流行的哈希函数是以 MD4 和 MD5 为代表的 MD 系列,它们是由 R. Rivest 研制的。更好的哈希函数选择是 SHA-1。

哈希函数还可通过 MAC 码来实现数据认证。数据认证是认证和数据完整性的结合。所谓的 MAC 计算如下:

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

其中函数 $f(\ )$ 基于特定哈希函数的组合。如果发信方和收信方都已经知道密钥,则收信方就可以通过 MAC 码来检查发信方身份的真实性以及消息的完整性,具体方法是:将已知的哈希函数与密钥及消息相结合。关于 MAC 的第一个方案是仅仅将哈希函数用于密钥及消息的连接,即计算 h(Secret Key, message)。不幸的是已经证明这种方法是不安全的。目前最好的方法是使用嵌套的哈希函数(如,h[Secret Key, h(Secret Key, message)]),并使用填充手段。

哈希函数的另一个重要应用是数字签名,它使得消息的接收者能够证实消息的发送者并且能验证消息自发送后未经改动。签名及验证过程如图 1.3 所示。

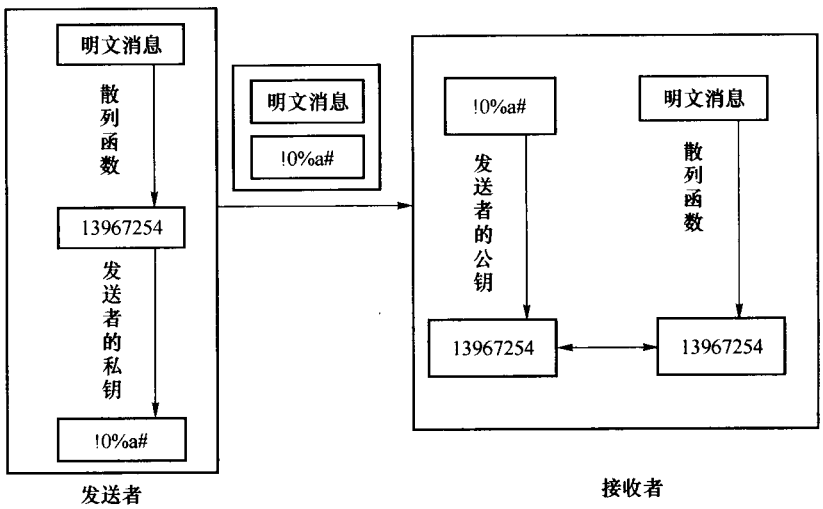

图 1.3 签名及验证过程

如图 1.3 所示,接收者将由签名解密得到的消息摘要与由明文经过哈希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。

1.1.2 分组密码的数学模型

1. 加密过程

分组密码是对称密码的典型代表。通俗地说就是数据在密钥的作用下,一组一组、等长地被处理,且通常情况是明、密文等长。这样做的好处是处理速度快,节约了存储,避免了浪

费带宽。分组密码也是许多密码组件的基础，比如，很容易转化为流密码、哈希函数。分组密码的另一特点是容易标准化，分组密码由于其固有的特点（高强度、高速率、便于软硬实现）而成为标准化进程的首选体制。DES 就是首先成为数据加密标准的分组密码典型代表。作为数据加密标准，DES 算法完全公开，任何个人和团体都可以使用，其信息的安全性取决于各自密钥的安全性，这正是现代分组密码的特征。

分组密码又分为 3 类：代替密码（Substitution）、移位密码（Transposition）和乘积密码。早期的代替和移位密码已无安全可言。显然，增加密码强度的方法是合并代替和移位密码。这样的密码称为乘积密码。如果密文是由明文运用轮函数作用多次而得，这样的乘积密码又称为迭代分组密码。

分组密码就是将明文消息序列 $m_1, m_2, \cdots, m_k, \cdots$ 分成等长的消息组 $(m_1, m_2, \cdots, m_n)$，$(m_{n+1}, m_{n+2}, \cdots, m_{2n}), \cdots$。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 1.4 所示。一个分组长为 n bit，密钥长为 t bit 的分组密码，数学上可以看作是在 2^t 个密钥控制下的 $GF(2)^n \to GF(2)^n$ 的置换。由于 $GF(2)^n \to GF(2)^n$ 的置换有 $2^n!$ 个不同的方式，故一个极好的 n bit 分组密码可以接受的密钥长度可达 $\lfloor \log_2(2^n)! \rfloor$ bit。用来加密的置换只是全体置换所构成集合的一个子集。设计分组密码的问题，关键在于找到一种算法，它能在密钥的控制下从一个足够大且“好”的置换子集中简单而迅速地选出一个置换。

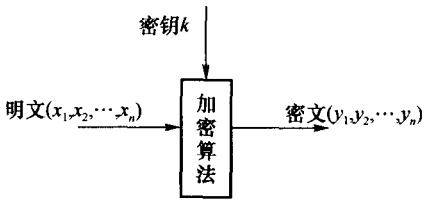

图 1.4　分组密码的加密过程

一般地，分组密码可以定义为如下一种映射：

$$F_2^n \times F_2^r \to F_2^m,$$

记为 $E(X,K)$ 或 $E_K(X)$，$X \in F_2^n$，$K \in F_2^r$，F_2^n 称为明文空间，F_2^m 称为密文空间，F_2^r 为密钥空间。n 为明文分组长度，当 $n > m$ 时，称为有数据压缩的分组密码；当 $n < m$ 时，称为有数据扩展的分组密码，当 $n = m$ 且为一一映射时，$E_K(x)$ 就是 $GF(2)^n$ 到 $GF(2)^n$ 的置换。通常的情况是 $n = m$。

2. 分组密码的结构

一个安全的分组密码既要难于分析（复杂），又要易于实现（简单）。迭代密码就是为了克服这一对矛盾而产生的一种分组密码。其加密变换（置换）一般采取如下结构：由一个简单的函数 F（易于实现）迭代若干次而形成，如图 1.5 所示。

在图 1.5 中，$Y(i-1)$ 是第 i 轮置换的输入，$Y(i)$ 是第 i 轮的输出，$z^{(i)}$ 是第 i 轮的子密钥，k 是种子密钥。每次迭代称为一轮，每轮的输出是输入和该轮子密钥的函数，每轮子密钥由 k 导出，这种密码就是迭代密码，如 DES 就是 16 轮迭代密码。函数 F 称为圈函数或轮函数。一个适当选择的轮函数通过多次迭代可实现必要的混淆和扩散。

如果把一个 $GF(2)^n$ 到 $GF(2)^m$ 的变换看作一个网络，那么常用的轮函数 F 都是基于代换-置换的网络，即以多次变换的乘积构成，称为置换的变换提供扩散，而称为代换的变换提供混淆，其中代换网络是精心设计且起关键作用的，人们常称其为黑盒子。为了增强安全性，n 一般都比较大。在代换的实现中，其难度将随 n 指数增长，难于处理，不易实现。因