基于FPGA密码技术的设计与应用

杨 军 余 江 赵征鹏〇著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络通信及智能计算实验室专项经费（X3110012）
云南大学校级第三批精品课程建设项目（WX070141）

基于FPGA密码技术的设计与应用

杨 军 余 江 赵征鹏 著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

全书共 7 章，包含基础知识到应用实例的讲解、分析，并总结了开发技巧，可以帮助读者快速提高硬件加/解密系统的开发能力和实战经验。第 1～2 章为基础知识部分，介绍密码基础知识和项目开发环境；第 3～6 章为应用实例部分，共安排了 4 个经典的设计实例，详细介绍了硬件加/解密系统开发的技术和技巧，深入讲解了开发方案与设计思路，并对设计过程中的重点和难点进行了详细分析和注释；第 7 章为经验总结部分，总结了书中 4 个应用开发实例和编者多年来的开发经验，以及遇到的难点和问题，让读者在吸取经验和掌握技巧的同时，迅速提升开发的实践能力。

本书适合高等学校电子、电气及计算机类等相关专业高年级本科生和研究生以及相关领域的研究人员，也可供从事 FPGA 设计与开发的技术人员参考。

图书在版编目（CIP）数据

基于 FPGA 密码技术的设计与应用 / 杨军，余江，赵征鹏著. —北京：电子工业出版社，2012.5
ISBN 978-7-121-16883-3

Ⅰ. ①基… Ⅱ. ①杨… ②余… ③赵… Ⅲ. ①密码术 Ⅳ. ①TN918.3

中国版本图书馆 CIP 数据核字（2012）第 080838 号

责任编辑：赵　娜　　特约编辑：王　纲
印　　刷：北京天宇星印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：14　字数：320 千字
印　　次：2012 年 5 月第 1 次印刷
定　　价：39.80 元（含 CD 光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

FPGA 技术综合了灵活性、低成本和快速上市周期的优势，同时还具备高性能、系统集成和最先进的开发工具，是电子系统设计领域的发展趋势，将在未来电子设计领域发挥越来越重要的作用。作者结合近几年 FPGA 的实践和教学经验，针对读者可能遇到的实际问题，参考了大量设计书籍和技术文献，组织编写了本书。书中研究的是近些年来倍受重视的信息安全技术，尤其是基于 FPGA 的硬件加/解密技术，作者根据自己近几年在 FPGA 和密码学领域方面的研究和实践，综合了两者的应用，针对面临的实际开发问题和当前网络对信息安全的需求，尤其是基于 FPGA 技术下的密码技术应用，使本书满足广大读者学习和工作的需要。本书以实用为原则，通过讲练结合的方式，对实例项目进行开发技术和经验的介绍与总结，重视开发方案与设计技巧的讲解，注重读者动手能力的培养，能迅速帮助读者在经验和实践能力两方面得到提升，培养和提高读者基于 FPGA 的硬件密码技术的开发和设计能力。

系统设计的基本软件工具如下：

Quartus Ⅱ：用于完成 Nios Ⅱ 系统的综合、硬件优化、适配、编程下载及硬件系统调试等。

SOPC Builder：Altera Nios Ⅱ 嵌入式处理器开发软件包，用于实现 Nios Ⅱ 系统的配置和生成。

ModelSim：用于对 SOPC 生成的 Nios Ⅱ 系统的 HDL 描述进行系统功能仿真。

Nios Ⅱ IDE：用于进行软件开发、调试以及向目标开发板进行 Flash 下载。

全书简要叙述了密码学和硬件密码学知识，简单介绍了 Quartus Ⅱ，ModelSim，Nios Ⅱ IDE 等基本软件工具的操作应用（包括嵌入式系统的硬件配置、硬件设计、硬件仿真、软件设计及软件调试等）；分析和讲解了基于 FPGA 技术的硬件加/解密技术的设计和实现，在实例的讲解中总结了作者实践项目的开发经验、技巧及开发过程中遇到的问题；提供了基于 FPGA 的 SOPC 设计技术的系统集成实例，实例代表性和实践性强，来自于作者近几年来主持的基金项目和指导的比赛获奖作品，且全部调试通过。

本书语言简洁，结构清晰，内容系统全面，基础知识和实际工程结合，紧紧围绕实用原则，总结了作者实践项目的开发经验、技巧及开发过程中遇到的问题。在实例的讲解上，既介绍了设计原理、结构框图、基本步骤和流程，提供了开发方案和设计思路，也穿插了一些经验技巧和注意事项，在潜移默化的过程中提高读者的理论知识和实践能力。同时重视开发方案与设计技巧的讲解，注重读者动手能力的培养。

本书由杨军、余江主笔，赵征鹏共同编写完成。其中第 2、5、6 章由杨军教授编写，第 3、4 章由余江教授编写，第 1、7 章由赵征鹏副教授编写。另外为本书的顺利完成做出贡献的人员还有舒平平、张伟平、陈成、董寅、王小军、杜琛、李剑和赵嘎等，他们在资料的收集、整理，源代码的设计、分析、仿真，硬件平台的验证，书稿的录入、排版和绘图等方面做了大量的工作，在此一并向他们表示最诚挚的谢意！

基于FPGA硬件加/解密系统的设计技术涉及的知识范围广，本书中硬件设计和软件设计中分别采用了硬件描述语言和C语言，随书将提供丰富的实例工程文件和程序源代码，读者稍加修改便可应用于自己的工作中或完成自己的课题。由于作者水平有限，加之编写时间仓促，书中难免有错误和不足之处，恳请读者批评指正。

编　者

2012年3月

目　录

第1章

密码学简介

1.1 引言

在当今计算机和电子通信技术迅速发展的时代，信息是推动社会前进的巨大资源，人们可以随时随地享用各种信息服务。随着 Internet 的广泛应用，个人通信、办公自动化、电子邮件、电子自动转账支付系统、自动零售业务等的相继建立与实现，各种计算和通信系统已经成为人类生活环境的重要组成部分，它们以多媒体形式收集、分析、存储、展示和传播信息，并作为独立产品或与其他物理产品相结合为人类的政治、经济、军事和文化服务。在这种背景下，如何安全有效地使用各种信息已成为保证人类社会发展的重要基石；与此同时，各种窃密的黑客技术也得到了前所未有的发展，用户对信息的安全存储、安全处理和安全传输的需求越来越迫切，也越来越高，如何确保信息在公开网络上的传输与处理过程中，不被非法窃取、窃听、伪造和篡改，即信息的认证与保密的问题，成为了人们关注的问题，因此密码学理论与其实现技术，就成为信息科学与技术中的一个重要研究领域，并日益受到重视。

信息安全（即密码安全技术）是一个综合的、多学科交叉的领域，它结合数学、计算机科学、电子与通信等诸多学科于一身，通过综合利用数学、物理、通信、计算机等诸多学科的长期知识积累和最新发展成果，进行自主创新研究，提出系统、完整、协同的解决方案。与其他学科相比，信息安全的研究更强调自主性和创新性，自主性可以杜绝后门，保护国家主权；而创新性可以抵抗各种攻击，适应技术发展的需求。信息安全的目的就在于保证数据信息在确定的时间、确定的地点条件下只能被拥有使用权限的用户所使用或识别。一般来说，信息安全至少应具有以下五个方面的特性。

① 机密性：防止未经授权的信息被获取，如未经授权，则无法理解信息本身的真正含义（加密信息）等。

② 完整性：防止未经授权的信息被更改（修改、删除、增加），如未经授权则无法对信息进行任何形式的更改。一般用于防止对信息的主动、恶意的篡改。

③ 可获取性：防止未经授权的信息被截流（在信息传输过程中的非法截取）。

④ 真实性：真实性就是通过一系列的技术手段验证信息的真实性。

⑤ 持久性：指长时间信息保存的可靠性、准确性等。

加密是实现信息安全的一种重要手段，加密技术可使一些重要数据存储在不安全的计算机

上，或在不安全的信道上传送，只有持有合法密钥的那方才可获得明文。然而仅仅考虑加密算法是不足以确保数据安全的，还必须考虑在数据加密和存储过程中所可能发生的攻击行为，再好的加密算法也需要系统的支撑，由此就提出了信息安全对系统的要求。采用软件实现的加密系统虽然系统成本较低，但是具有占用主机系统资源较多、核心模块容易被跟踪和替换、密钥管理难度较大的特点。同时传统的软件加/解密技术已经越来越不能满足信息安全对运算速度和系统安全性的要求了。因此，现代密码学提出了使用硬件加密系统，这样不仅可以减轻主机系统内存和 CPU 的负担，从整体上提高服务器的性能，还能进一步提高系统的安全性，从而推动各种安全应用的快速发展。

1.2 密码学和现代密码学

密码学（Cryptography，源于希腊语 kryptós“隐藏的”和 gráphein“书写”）是研究如何隐密地传递信息的学科。在现代特别指对信息及其传输的数学性研究，常被认为是数学和计算机科学的分支，它与信息论也密切相关。著名的密码学者 Ron Rivest 解释道：“密码学是如何在敌人存在的环境中通信”，这是从工程学的角度来看的，在此也可以看出密码学与纯数学的异同。在密码学中，研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学。密码学是信息安全等相关领域（如认证、访问控制）的核心，在这些领域中密码学的首要目的是隐藏信息的含义，而不是隐藏信息的存在。因此也可以说密码学是研究编制密码和破译密码的技术。

1.2.1 传统密码体制

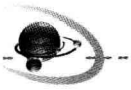
传统密码体制主要通过字符间的简单置换和代换来实现对信息的加/解密。现在来看，传统密码体制的技术、思想以及破译方法相对简单，但它们反映了密码设计和破译的基本思想，可以作为学习现代密码学的入门资料，对于理解、设计和分析现代密码学具有很好的借鉴价值。下面介绍两种主要的传统密码体制：置换密码和代换密码。

1. 置换密码（Permutation Cipher）

置换密码又称换位密码，是指根据一定的规则重新排列明文，以便打破明文的结构特征。置换密码的特点是保持明文的所有字符不变，只是利用置换打乱明文的位置和次序。最常见的置换密码有两种：一种是列置换密码，另一种是周期置换密码。

定义 1.1 有限集 X 上运算 σ：$X \to X$ 被称为一个置换，则 σ 是一双射函数，即 σ 既是单射又是满射，并且 σ 的定义域和值域相同。也就是说，任意 $x \in X$，存在唯一的 $x' \in X$ 使得 $\sigma(x)=x'$。同理可以定义置换 σ 的逆置换 σ^{-1}：$X \to X$，这是因为 σ^{-1} 也是双射函数，并且 σ^{-1} 的定义域和值域相同。也就是说，任意 $x' \in X$，存在唯一的 $x \in X$ 使得 $\sigma^{-1}(x')=x$。

定义 1.2 设 n 为一固定整数，P、C 和 K 分别为明文空间、密文空间和密钥空间。明/密文是长度为 n 的字符序列，分别记为 $X=(x_1,x_2,\cdots,x_n) \in P$ 和 $Y=(y_1,y_2,\cdots,y_n) \in C$，$K$ 是定义在 $\{1,2,\cdots,n\}$ 的所有置换组合集合。对于任何一个密钥 $\sigma \in K$（即一个置换），定义置换密码



如下：

$$e_\sigma(x_1,x_2,\cdots,x_n)=(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})$$
$$d_\sigma^{-1}(y_1,y_2,\cdots,y_n)=(y_{\sigma^{-1}(1)},y_{\sigma^{-1}(2)},\cdots,y_{\sigma^{-1}(n)})$$

上式中，σ^{-1}是σ的逆置换，密钥空间 K 的大小为 $n!$。

（1）列置换密码

列置换密码是一种常见的置换密码方式，列置换密码的加密方法如下：

① 把明文字符以固定的宽度 m（分组长度）水平地（按行）写出，即每行有 m 个字符；若明文长度不是 m 的整数倍，不足的地方用双方约定的方式填充。

② 按 1,2，…，m 的某一置换σ交换列的位置次序得到字符矩阵。

③ 把矩阵按 1,2，…，m 列的顺序读出得密文序列 c。

相应的解密过程就是上述加密过程的逆过程，故密文 c 的解密过程如下：

① 将密文 c 以分组宽度 n 按列写出得到字符矩阵。

② 按加密过程用的置换σ的逆置换σ^{-1}交换列的位置次序得到字符矩阵。

③ 把矩阵按 1,2，…，m 列的顺序读出得明文序列 p。

（2）周期置换密码

周期性置换密码是将明文 p 串按固定长度 m 分组，然后对每组中的子串按 1,2，…，m 的某个置换重新排列位置从而得到密文，其中密钥包含分组长度信息。解密时同样对密文 c 按长度 m 分组，并按σ的逆置换σ^{-1}把每组子串重新排列位置得到明文 p。

2. 代换密码（Substitution Cipher）

代换密码是将明文中的字符替换为其他字符的密码体制。基本方法是：建立一个代换表，加密时将待加密的明文字符通过查表代换为相应的密文字符，这个代换就是密钥。代换是传统密码体制中最基本的技巧，它在现代密码学中也有广泛的应用。按照一个明文是否总是被一个固定的字母代替进行划分，代换密码主要分为单表代换密码和多表代换密码。

1）单表代换密码

单表代换密码是指明文消息中相同的字母，在加密时都是用同一固定的字母来代换。单表代换密码又分为移位密码、基于密钥的单表代换密码和仿射密码 3 类，由于移位密码可以看成仿射密码特例，下面只介绍基于密钥的单表代换密码和仿射密码。

（1）基于密钥的单表代换密码

基于密钥的单表代换密码很多，其基本思想是类似的。首先选取一个英文单词或字母串作为密钥，去掉其中重复的字母得到一个无重复字母的字母序列，然后将字母表中的其他字母顺序依次写在此字母序列后面，如果密钥中的字母序列有重复则后出现的字母不再出现，从而使所有的字母建立一一对应关系，也就是字母代换表。这种单表代换密码的破译难度稍高，而且密钥更改便捷，增加了单表代换密码体制的灵活性。

（2）仿射密码

仿射密码的加密算法就是一个线性变换，即对任意的明文字符 x，对应的密文字符为 $y=e(x)=ax+b(\mathrm{mod}\ 26)$，其中 $a,b\in$字母表，并且要求 $\gcd(a,26)=1$，函数 $e(x)$称为仿射加密函数。仿射加密函数要求 $\gcd(a,26)=1$，即要求 a 和 26 互为素数，否则 $e(x)=ax+b(\mathrm{mod}\ 26)$就不是一个

单射函数。当 gcd(a,26)=1 时，仿射加密函数的解必然唯一。

2）多表代换密码

多表代换密码是以一系列代换表对明文消息的字母序列进行代换的加密方法，即明文消息中出现的同一个字母，在加密时不是完全被同一个固定的字母代换，而是根据其出现的位置次序用不同的字母代换。如果代换表序列是非周期的无限序列，则相应的密码称为非周期多表代换密码，它是理论上不可破译的密码体制。但实际应用中经常采用的是周期多表代换密码，它通常使用有限个代换表，代换表被重复使用以完成消息的加密，它是一种比单表密码体制更为安全的密码体制。

多表代换密码利用从明文字符到密文字符的多个映射隐藏单字母出现的统计特性（频率特性）。它将明文字符划分为长度相同的明文组，然后在对明文组进行替换。这样统一字母在明文序列中的位置不同就有不同的密文，能更好抵抗统计密码分析。多表代换密码体制有很多，比较典型的有 Playfair 密码和 Vigenere 密码。

（1）Playfair 密码

Playfair 密码（Playfair Cipher）是 1854 年由 Charles Wheatstone 提出的，此后由他的朋友 Lyon Playfair 将该密码公布，所以称为 Playfair 密码。

Playfair 密码将明文字母按两个字母一组分成若干个单元，然后将这些单元替换为密文字母组合，替换时基于一个 5×5 字母矩阵，该矩阵使用一个选定的关键词来构造，其构造方法如下。第一步是编制密码表。在这个 5×5 的密码表中，共有 5 行 5 列字母。第一列（或第一行）是密钥，其余按照字母顺序。密钥是一个单词或词组，若有重复字母，可将后面重复的字母去掉。当然也要把使用频率最少的字母去掉，假如密钥是“live and learn”，去掉后则为“liveandr”。如果密钥过长可以占用第二列或行。第二步是整理明文。将明文每两个字母组成一对，如果成对后有两个相同字母紧挨或最后一个字母是单个的，就插入一个字母 X。最后编写密文。对明文加密规则如下：

若 p_1p_2 在同一行，对应密文 c_1c_2 分别是紧靠 p_1p_2 右端的字母。其中第一列被看做是最后一列的右方。

若 p_1p_2 在同一列，对应密文 c_1c_2 分别是紧靠 p_1p_2 下方的字母。其中第一行被看做是最后一行的下方。

若 p_1p_2 不在同一行，不在同一列，则 c_1c_2 是由 p_1p_2 确定的矩形的其他两角的字母（至于横向替换还是纵向替换要事先约好，或自行尝试）。

Playfair 解密算法首先将密钥填写在一个 5×5 的矩阵中（去除重复字母），矩阵中其他未用到的字母按顺序填在矩阵剩余位置中，根据替换矩阵由密文得到明文。

对密文解密规则如下：

若 c_1c_2 在同一行，对应明文 p_1p_2 分别是紧靠 c_1c_2 左端的字母。其中最后一列被看做是第一列的左方。

若 c_1c_2 在同一列，对应明文 p_1p_2 分别是紧靠 c_1c_2 上方的字母。其中最后一行被看做是第一行的上方。

若 c_1c_2 不在同一行，不在同一列，则 p_1p_2 是由 c_1c_2 确定的矩形的其他两角的字母。

（2）Vigenere 密码

Vigenere 密码是由法国密码学家 Blaise de Vigenere 于 1858 年提出的一种密码代换，它是

多表代换密码的典型代表。

定义 1.3　设 m 为某一固定的正整数，P，C 和 K 分别为明文空间、密文空间和密钥空间，并且 $P=K=C=(Z_{26})^m$，对于一个密钥 $k=(k_1,k_2,\cdots,k_m)$，定义 Vigenere 密码的加密函数为：$ek(x_1,x_2,\cdots,x_m)=(x_1+k_1,x_2+k_2,\cdots,x_m+k_m)$，与之对应的解密函数为：$dk(y_1,y_2,\cdots,y_m)=(y_1-k_1,y_2-k_2,\cdots,y_m-k_m)$。

其中 $k=(k_1,k_2,\cdots,k_m)$是一个长为 m 的密钥字，密钥空间大小为 $26m$，所以对于一个相对小的 m，穷举密钥也需要很长的时间。当明文长度超过 m 时，可将明文串按长度 m 分组，然后对每一组使用密钥 k 加密。

1.2.2　现代密码学

随着科学的发展，密码学占据的位置越来越重要，基于数学模式下的密码学与越来越多的学科联系也更加紧密，密码学的应用越来越广泛，其主要研究内容如图 1.1 所示。

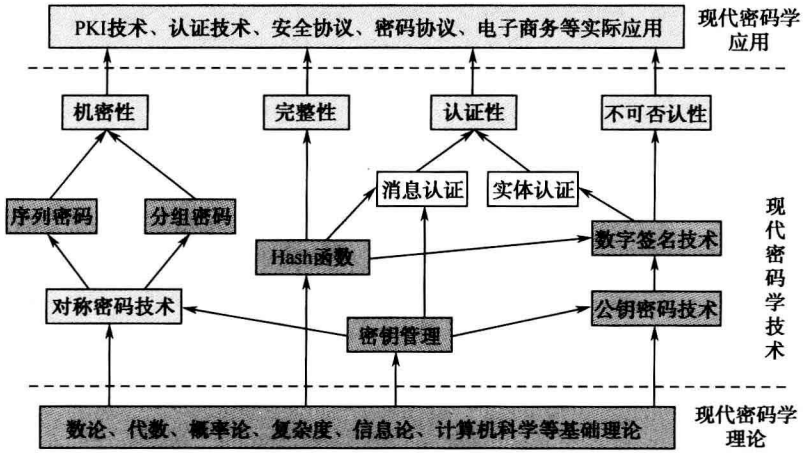


图 1.1　现代密码学的主要研究内容

1. 现代密码学理论

在密码学理论中，关键内容是从安全的需要出发，合理定义一些具备一定性质要求的对象，这些对象称为密码原语（Cryptographic Primitive），进而探讨使用密码原语解决安全问题的方式，这些解决安全问题的方式称为范式（Paradigm）。通常基于已证明存在或合理假设存在的原语，证明通过范式构造的解决方案（包括通用构造方法，以及基于某些具体困难问题或者数学结构构造的实际方案）满足预先定义的安全需求。常用范式总结如下。

① OAEP 变换，通过将明文填充，将明文转化为格式化的明文，原始明文扩散到这种格式化的明文中，并引入随机性，产生了概率加密和明文敏感性的效果，使得基于单射的单向陷门置换构造的公钥加密方案为 IND—CCA2 安全的方案。这种填充方法使用了伪随机发生器和 Hash 函数。

② 安全公钥加密的典型范式如混合加密（Hybrid Encryption），即用非对称密钥算法加密

临时的随机密钥，然后利用临时的随机密钥使用对称密钥算法加密消息。使用非对称加密作为原语。

③ IND—CCA2 安全的公钥加密的通用转化方法。包括：Fujisaki-Okamoto 转化方法（FO Conversion）、Pointcheval 转化方法和 Okamoto-Pointcheval 转化方法。

④ 安全数字签名的一个典型范式是 Hash-and-Sign 范式。所谓 Hash-and-Sign 范式就是先将消息用 Hash 函数求值，然后再对散列值进行签名。也有文献将这种范式称为 Hash-and-Decrypt 范式，它使用 Hash 函数作为原语。

⑤ 零知识证明中将交互零知识转变成非交互零知识的 Fiat-Shamir 启发式（Hurisitics），也称 Fiat-Shamir 范式。该变换是知识签名的基础，也是将基于身份的识别协议转化为签名方案的一般方法。

⑥ PSS 构造方法是使用 Hash-and-Sign 范式前的填充方法，该填充方法和 OAEP 填充方法具有某些相似性。

⑦ 基于随机预言模型，可以将原始明文随机化，从而得到更安全的公钥加密和签名。因为如果一个明文消息是随机化的，则从密文找到明文的任何信息（如一个比特）和求单向函数的逆一样困难。

⑧ 特定应用背景下的范式，如 E1Gamal 一般签名形式，Schnorr 缩短素数域元素的表示，但又不降低 DLP 的困难程度。

2. 密码系统的安全性测度

一个密码系统最起码的安全性要求是：破译者从截获的密文中，无法用穷举所有可能的密钥来破译该系统。如果破译者没有足够的时间来试每个密钥，或即使穷举了所有密钥，还是不能破译该系统，则称它是穷举破译安全的。对于密码分析，通常有如下三种攻击类型。

① 仅知密文攻击：密码分析者除了拥有所截获的密文外，没有其他可利用的信息。

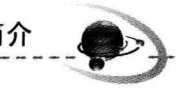
② 已知明文攻击：密码分析者仅知道当前密钥下的一明密对。

③ 选择明文攻击：密码分析者能获得当前密钥下的一些特定的明文所对应的密文。

密码的安全性表现在以下两个方面。

（1）完全保密性

设明文 M 出现的概率为 $p(M)$，密文 C 出现的概率为 $P(C)$，在收到密文 C 的条件下发送的明文为 M 的条件概率为 $P(M/C)$。如果对所有的 M 和 C 有 $p(M/C)=p(M)$，则称该密码是完全保密的。这就是说，如果不论截获多少密文，关于原明文仍一无所知，即密文与明文是统计独立的。一个密码系统是完全保密的充分必要条件是：对每个密文 C 都有 $P(C/M)=p(C)$，就是说，在给定发送明文 M 下（在某个密钥下加密）收到一个特定密文 C 的概率，和在发送其他消息 M 下（在另一个密钥下加密）收到 C 的概率相同。在一个完全保密的密码系统中，密钥数至少应等于明文数。否则，对于给定的密文 C，将会有一些明文 M 找不到密钥 K 将 C 解密为 M，这意味着 $p(M/C)=0$，于是，密码分析者可能从考虑的范围中除去某些可能的明文消息，这将导致破译该密码的机会增大。一次一密钥密码系统是完全保密的密码系统的一个例子。但是，由于一次一密钥密码系统所需要的密钥量至少应等于明文的数量，这就使得密钥的分配和管理极为困难。一旦密钥得不到安全的分配和管理，系统也就没有安全性可言，因而一次一密钥密码系统并不实用。在密码学中，绝大多数密码系统是不完全保密的。



（2）计算安全性

实际上，密码分析者不会拥有无限的计算能力，因此，一个实用的密码系统的安全性不依赖于破译该密码理论上的不可能性，而是极大地依赖于攻击的实际困难程度。如果一个针对该密码最佳攻击方法的困难程度超过了密码分析者的计算能力则称该密码系统是计算安全的，或实际安全的。Shannon 用密码的工作特性 $W(n)$就仅知密文攻击刻画了这样一种困难性。一个密码的工作特性 $W(n)$定义为当 n 个密文已知时确定所使用的密钥所需要的工作量，人们也可以针对其他攻击探讨密码的工作特性。说一个密码系统是计算安全的意义是指对该密码最佳攻击的复杂度（一般理解为实施该攻击所使用运行的平均次数）超过了密码分析者的计算能力。要证明一个密码是计算上安全的将意味着寻找一个关于解某个计算问题的复杂度下界。目前对实际中所有的计算问题，这都是难以做到的。因此，一个密码安全性的评估实际上依赖于目前已知道的关于该密码的最佳攻击的复杂度。

1.3 密码技术

自从人类有了战争，就有了密码，密码作为一种技术源远流长，可以追溯到远古时代。但其成为一门学科则是近 40 年的事，这是受计算机科学蓬勃发展刺激的结果。在今天计算机被广泛应用的信息时代，信息本身就是时间，就是财富。大量机密信息的泄露会造成不可挽回的损失。如何保护信息的安全已不仅仅是军事和政府部门感兴趣的话题，各企事业单位也愈感迫切。因为在网络化的今天，计算机犯罪每年造成的损失极其巨大，而且这种趋势还在不断发展中。给信息加密是有效而且可行的保护信息安全的方法，这里的有效是指给信息加密能做到使信息不被非法窃取、篡改或破坏；可行是说它需要付出的代价是可以接受的。

加/解密技术形成一门学科是在 20 世纪 70 年代。它的理论基础之一应该首推 1949 年 Shannon 的一篇文章“保密通信的信息理论”，这篇文章过了 30 年后才显示出它的价值。现在，密码学有了突飞猛进的发展，而且成为了某些学科的基础。特别是“电子商务”和“电子政府”的提出，使得近代密码学的研究成为热门的课题，也扩大了它的发展空间。

在近代密码学上值得一提的大事有两件：一是 1977 年美国国家标准局正式公布实施了美国的数据加密标准（DES），公开它的加密算法，并批准可用于非机密单位及商业上的保密通信，密码学的神秘面纱从此被揭开。二是 Diffie 和 Hellman 联合写的一篇文章“密码学的新方向”，提出了适应网络上保密通信的公钥密码思想，拉开了公钥密码研究的序幕。受他们的思想启迪，各种公钥密码体制被提出，特别是 RSA 公钥密码的提出在密码学上是一个里程碑。

1.3.1 对称密码

对称（Symmetric）密码系统是加密者和解密者使用相同的密钥或密钥容易相互导出，由于对称密码的效率高，因此它常用于数据量较大的保密通信中。对称密码系统如图 1.2 所示。

现在，通常使用分组密码（Block Cipher）或序列密码（Stream Cipher）实现对称密码，下面将讨论这两种密码。

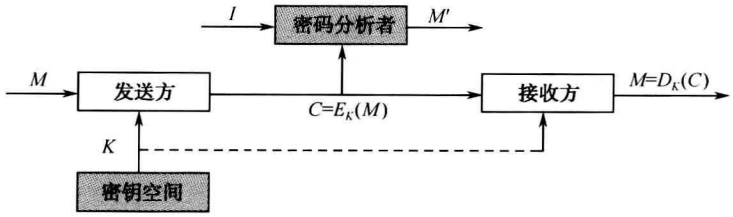


图 1.2　对称密码系统

1. 分组密码

分组密码将定长的明文块转换成等长的密文，这一过程是在密钥的控制之下完成的。使用逆向变换和同一密钥来实现解密。对于当前的许多分组密码，分组大小为 64 位，但随着计算机性能的不断提升，分组大小也会增加。

分组密码取用明文的一个区块和钥匙，输出相同大小的密文区块。由于信息通常比单一区块还长，因此有了各种方式将连续的区块编织在一起。 DES 和 AES 是美国联邦政府核定的分组密码标准，目前 AES 已基本取代了 DES，而且 DES 将会从分组密码标准上废除，但 DES 依然很流行（triple-DES 变形仍然相当安全），被广泛使用在非常多的应用系统上，从自动交易机、电子邮件到远端存取。除了 DES 和 AES 外，也有许多其他的区块加密被发明、公开，它们在品质与应用上各有不同，其中还有不少已经被破解了。

迭代的分组密码是指其加密过程有多次循环的分组密码，由于循环了多次，故提高了其安全性。在每个循环中，可以通过使用特殊的函数从初始密钥派生出的子密钥来应用适当的变换。该附加的计算需求必然会影响加密的速度，因此在安全性需要和执行速度之间需要寻求一种平衡。

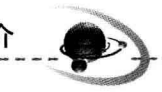
2. 序列密码

与分组密码相比，序列密码的速度要快一些，尽管某些方式下工作的一些分组密码（如 CFB 或 OFB 中的 DES）可以与序列密码一样有效地运作，但通常情况下还是序列密码的速度快。序列密码作用于由若干位组成的一些小型组，通常使用称为密钥流的一个位序列作为密钥对，它们逐位应用“异或”运算。有些序列密码基于一种称为“线性反馈移位寄存器”（Linear Feedback Shift Register，LFSR）的机制，该机制生成一个二进制位序列。

序列密码是由一种专业的密码——Vernam 密码［也称为一次性密码本（One-Time Pad）］，发展而来的。序列密码的示例包括 RC4 和“软件优化加密算法”（Software Optimized Encryption Algorithm，SOEA），以及 Vernam 密码或一次性密码本的特殊情形。

3. 对称密码的安全

对称密码加密（秘密钥匙加密）是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密。因此对称密码系统的安全性依赖于以下两个因素：第一，加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；第二，加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性，因此，我们没有必要确保算法的秘密



性，而需要保证密钥的秘密性。对称加密系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。因为算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有着广泛的应用前景，适合于大规模生产。

对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。如对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了大问题。对称加密算法的另一个缺点是不能实现数字签名。

4. DES 简介

数据加密算法（Data Encryption Algorithm，DEA）的数据加密标准（Data Encryption Standard，DES）是规范的描述，它出自 IBM 的研究工作，并在 1997 年被美国政府正式采纳。它以前是使用最广泛的密钥系统，特别是在保护金融数据的安全中，最初开发的 DES 是嵌入硬件中的。通常，自动取款机（Automated Teller Machine，ATM）都使用 DES。

DES 使用一个 56 位的密钥以及附加的 8 位奇偶校验位，产生最大 64 位的分组大小。这是一个迭代的分组密码，使用称为 Feistel 的技术，其中将加密的文本块分成两半。使用子密钥对其中一半应用循环功能，然后将输出与另一半进行“异或”运算；接着交换这两半，这一过程会继续下去，但最后一个循环不交换。DES 共使用 16 个循环。

攻击 DES 的主要形式被称为蛮力或彻底密钥搜索，即重复尝试各种密钥直到有一个符合为止。如果 DES 使用 56 位的密钥，则可能的密钥数量是 2 的 56 次方。随着计算机系统能力的不断发展，DES 的安全性比它刚出现时会弱得多，然而从非关键性质的实际出发，仍可以认为它是足够的。不过，DES 现在仅用于旧系统的鉴定，而更多选择新的加密标准——高级加密标准（Advanced Encryption Standard，AES）。

DES 的常见变体是三重 DES，使用 168 位的密钥对资料进行三次加密的一种机制，它通常（但不是始终）提供极其强大的安全性。如果三个 56 位的子元素都相同，则三重 DES 向后兼容 DES。

5. AES 简介

高级加密标准（Advanced Encryption Standard，AES），又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。经过五年的甄选流程，高级加密标准由美国国家标准与技术研究院 （NIST）于 2001 年 11 月 26 日发布于 FIPS PUB 197，并在 2002 年 5 月 26 日成为有效的标准。2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

该算法为比利时密码学家 Joan Daemen 和 Vincent Rijmen 所设计，结合两位作者的名字，以 Rijndael 命名之，投稿高级加密标准的甄选流程。

AES 的基本要求是，采用对称分组密码体制，密钥长度为 128，192，256 位，分组长度为 128 位，算法应易于各种硬件和软件实现。1998 年 NIST 开始 AES 第一轮分析、测试和征集，共产生了 15 个候选算法。1999 年 3 月完成了第二轮 AES2 的分析和测试。2000 年 10 月 2 日美国政府正式宣布选中比利时密码学家 Joan Daemen 和 Vincent Rijmen 提出的一种密码算法