第 2 章 企业应用安全的银弹——密码学

通过对第1章内容的学习，我们基本了解了这枚解决企业应用安全的银弹——密码学。密码学并不是最近才兴起的新学科，它的历史最早可以追溯到几千年以前，而且古今中外都有密码学运用的记载。在《破译者》一书中戴维·卡恩曾说过：“人类使用密码的历史几乎与使用文字的时间一样长”。在经历战火的洗礼，步入现代以后，计算机科学与数学应用科学的快速发展，促进了密码学的进步。密码学成为应对计算机系统安全问题当之无愧的安全卫士，它广泛应用于计算机与网络安全领域，并逐步进入我们的日常生活：自动柜员机芯片卡、公交IC卡、电子商务等等，都是密码学应用的实例。计算机科学的迅速发展，使得密码学在我们的生活中变得越来越重要。

2.1 密码学的发家史

可以这么说，密码学是靠着战争发家的。自从有了战争，就有了密码学的应用环境。在战争中，对阵双方要保护自己的通信安全并窃取、破译对方的情报，于是就有了密码学。用著名的密码学专家罗纳德·李维斯特（Ronald L. Rivest）的话说，“密码学是关于如何在敌人存在的环境中通信”。纵观密码学的发展历程，我们大体可以将其分为三个阶段，即手工加密阶段、机械加密阶段和计算机加密阶段。

2.1.1 手工加密阶段

密码学很早就广泛应用于古代战争中，使用手工方式完成加密操作，以确保战争中军事信息的秘密传送，这一阶段称为手工加密阶段。这一阶段是古典密码学蓬勃发展的时期，称为古典加密阶段。

周朝兵书《六韬·龙韬》中记载了公元前1000年左右，即武王伐纣时期，周朝著名军事家姜子牙为战时通信制定的两种军事通信密码：阴符和阴书。阴符是使用双方在通信前事先制造的一套尺寸不等、形状各异的“符”，共八种，每种都代表一定的意义，只有通信双方知道。阴符可算是密码学中的替代法。阴书是在阴符的基础上继续发展而来的，它应用“一合而再离，三发而一知”的理论，也就是密码学中的移位法。将一份完整的军事文书一分为三，分三人传递，必须要把三份文书重新合并后才能获得完整的军事信息。即使途中一人或二人被捕，也不

至于暴露军事机密。

公元前480年，波希战争。波斯大量军队秘密集结，意图对雅典和斯巴达发动一次突袭。恰逢希腊人狄马拉图斯（Demaratus）在波斯的苏萨城内看到了这次集结，于是他在木板上记录了波斯突袭希腊的意图，然后用蜡把木板上的字封住。这块木板就这样在蜡封的掩盖下送到了希腊，最终使得波斯海军覆没于雅典附近的萨拉米湾，这就是著名的萨拉米湾海战。

公元前404年，斯巴达征服希腊。斯巴达在波斯帝国的帮助下，征服了希腊。斯巴达北路军司令莱萨德还没来得及庆祝就接到密探送来的信函。莱萨德接过密探的腰带，将其缠绕在斯巴达密码棒（Scytale）上，得知波斯帝国意图吞并他的城池。莱萨德当机立断，成功反击了波斯帝国的进攻。斯巴达密码棒实际上是一个指挥棒，将羊皮纸卷在密码棒上，把要保密的信息写在羊皮纸上。由上述“腰带”的含义可知，羊皮纸沿卷轴绕行方向做了切割，切割后的羊皮纸上的信息杂乱无章，信息得以加密。

公元前100年，高卢战争。罗马帝国的凯撒大帝（Caesar）使用以自己的名字命名的密码——凯撒密码，对重要的军事信息进行加密，这是一种简单的单字母替代密码，属于替代法。在当时，凯撒的敌人大多数是目不识丁的，对于这种“移形换位”大法，可谓是根本不知所云。凯撒密码的加密强度，在当时来看是相当有效的。

公元1040年，北宋时期。火药鼻祖曾公亮（999—1078年）与北宋文字训诂学家丁度（990—1053年）等奉敕集体编撰了《武经总要》，共40卷，该书详细记载了中国古代已知的军事情报通信密码。其中，收集了军队中常用的40种战斗情况，编成40条短语，分别编码产生密码本。这套密码的使用方法是，由军事部门指定一首没有重复字的五言律诗（40字），作为解密密钥。诗中的每个字都与短语一一对应，短语顺序在战前临时随机排列。密码本由战时前后两方高级将领保管，前后方通过该密码本进行战时通信。

公元1578年，玛丽女王被伊丽莎白女王软禁，安东尼·贝平顿（Anthony Babington）及其同党意图营救。英国人菲力普·马尼斯（Philip van Marnix）利用频度分析法，成功破解了安东尼发给玛丽的密码信。信件除了包括营救玛丽女王的计划外，还计划行刺伊丽莎白女王。因为信件的破解才得以将安东尼及其同党一举抓获，审判并处死了玛丽女王。

2.1.2 机械加密阶段

19世纪末至20世纪初，工业革命促进了机械和机电技术的发展，密码学进入机械加密阶段。工业革命为密码学的发展提供了基础，世界大战的爆发为密码学的飞跃提供了契机。

在第一次世界大战中，密码分析有了重大突破，它是战争能否取得胜利的重要决定因素之一；在第二次世界大战中，密码学经历了它的黄金时代，在战争中扮演了更重要的角色。

1. 第一次世界大战

19世纪末，无线电技术的发明和使用使通信工具发生了革命性的变革。由此产生了以密码技术为核心的包括侦察、测向、信号分析、通信分析等一整套无线电信号侦察以及对抗这种侦察的信号保密技术。军事电报的加密与破解成为同盟国与协约国之间成败的关键。

1914年8月，俄国在芬兰湾口击沉德国“马格德堡”轻巡洋舰，在德国军舰残骸里，俄国

潜水员意外发现了一份德国海军的密码本，并将其提供给英国，使英国人轻而易举地破译了德国海军的无线电密码。1916年5月30日下午，英国情报部门凭借截获的德国海军无线电密码，破译德国海军电报，日德兰海战以英国皇家海军胜利告终。

1917年1月16日，德意志帝国外交秘书阿瑟·齐默尔曼向德国驻墨西哥大使亨尼希·冯·艾克哈尔特（Heinrich von Eckardt）发出一份加密电报——齐默尔曼电报，电报内容建议墨西哥与德意志帝国结成对抗美国的军事联盟。在这个紧要关头，电报内容被英国破译密码的专门机构“40号房间”所截获，利用缴获的德国密码本破译了电报的内容，此次事件被称为“情报史上最伟大的密码破译事件”。“齐默尔曼电报”的破译，促使美国放弃中立而直接参战，改变了战争进程。

2. 第二次世界大战

20世纪初，机械及机电技术的快速发展，加速了密码设备的变革，最具代表性的就是转轮密码机的发明。转轮密码机的出现是密码学的重要标志之一，促进了传统密码学的进展，提高了机密系统的加密复杂度。转轮密码机Enigma㊀（别名“谜”或恩尼格玛密码机）的出现，成为密码学界划时代的丰碑。德国发明家亚瑟·谢尔比乌斯（Arthur Scherbius）发明了Enigma；波兰数学家马里安·雷耶夫斯基（Marian Rejewski）初步破解了简单的Enigma；而英国数学家阿兰·图灵（Alan Turing）㊁彻底终结了最高难度的Enigma。

1941年12月8日，美国对日本宣战。在整个太平洋上，美军与日军展开了全面的岛屿争夺战。在电影《风语者》中，日军因成功破解美军军事通信密码，占据战场上的优势，极大地阻碍了美军前进的步伐。1942年，美军征召纳瓦霍人（Navajo，美国最大的印第安部落）加入海军，并训练他们使用纳瓦霍语言作为通信密码。所谓“风语者”，就是使用纳瓦霍语言的通信兵。这是密码学和语言学的成功结合，使得纳瓦霍语成为唯一没有被日本破获的密码，并且成为赢得这场战争的关键。

1942年1月，大西洋海战进入第二阶段。德军以高人一等的密码通信能力，使用“狼群”战术发动大规模无限制潜艇战，致使同盟国节节受挫。在电影《猎杀U-571》中，美军为截获德军密码机在大西洋上与德军潜艇U-571展开了殊死的斗争，最终以截获德军密码机告终。德军密码机的截获，使美军迅速破译了德军指令，扭转了大西洋战事，有力地回击了德军的无限制大规模潜艇战争，加速了第二次世界大战的终结。

2.1.3 计算机加密阶段

第二次世界大战后，计算机与电子学快速发展，促进并推动了密码学进入计算机加密阶段。

㊀ Enigma在密码学界绝对是划时代的丰碑。而且，它所凝聚而成的不是一座丰碑，而是两座：研究并制造出Enigma是一座，研究并破解掉Enigma是另一座。只要稍微了解Enigma的历史的人就会被其中闪耀的人类智慧之美所折服。如果要向这样辉煌的智慧敬献花环，主要应该献给3个人：首先是德国人亚瑟·谢尔比乌斯，其次是波兰人马里安·雷耶夫斯基，然后是英国人阿兰·图灵。

㊁ 英国数学家、逻辑学家，被称为人工智能之父。1931年图灵进入剑桥大学国王学院，毕业后到美国普林斯顿大学攻读博士学位，第二次世界大战爆发后回到剑桥，后曾协助军方破解德国的著名密码系统Enigma，进而帮助盟军取得了第二次世界大战的胜利。

在这一阶段，计算机成为密码设计与破译的平台：利用计算机可以设计出更为复杂的加密算法，避免了徒手设计时容易造成的错误；利用计算机可以对加密算法进行破译，缩短了破译时间。当然，许多设计高明的加密算法的运算速度通常都很快而且占用资源少，但破解它却需要消耗大量的资源，破解通常以失败告终。在1949年之前，密码学是一门艺术；在1949～1975年，密码学成为科学；1976年以后，密码学有了的新方向——公钥密码学；1977年以后，密码学广泛应用于各种场所。

1949年，信息论始祖克劳德·艾尔伍德·香农（Claude Elwood Shannon）发表了《保密系统的通信理论》一文，把密码学建立在严格的数学基础之上，为密码学的发展奠定了理论基础。密码学由此成为一门真正的科学。在此之前，密码学完全是一门艺术，密码的设计和分析完全依赖于密码专家的直觉。

1976年，密码学专家迪菲（Whitfield Diffie）和赫尔曼（Martin E. Hellman）两人发表了《密码学的新方向》一文，解决了密钥管理的难题，把密钥分为加密的公钥和解密的私钥，提出了密钥交换算法（Diffie-Hellman，D-H），这是密码学的一场革命。

1977年，美国国家标准技术研究所（National Institute of Standards and Technology，NIST）制定数据加密标准（Data Encryption Standard，DES），将其颁布为国家标准，这是密码学历史上一个具有里程碑意义的事件。

同年，密码学专家罗纳德·李维斯特（Ronald L. Rivest）、沙米尔（Adi Shamir）和阿德勒曼（Len Adleman）在美国麻省理工学院，共同提出第一个较完善的公钥密码体制——RSA体制，这是一种建立在大数因子分解基础上的算法。RSA为数字签名奠定了基础。RSA源于整数因子分解问题，DSA源于离散对数问题。RSA和DSA是两种最流行的数字签名机制。数字签名是公钥基础设施（Public Key Infrastructure，PKI）以及许多网络安全机制（SSL/TLS，VPNs等）的基础。自此以后，密码学成为通信、计算机网络、计算机安全等方面的重要工具。

1985年，英国牛津大学物理学家戴维·多伊奇（David Deutsch）提出了量子计算机的初步设想。利用量子计算机，仅需30秒即可完成传统计算机要花上100亿年才能完成的大数因子分解，从而使破解RSA加密的信息成为可能。

同年，物理学家贝内特（Charles H. Bennett）根据多伊奇关于量子密码术的协议，在实验室第一次实现了量子密码加密信息的通信。尽管通信距离仅有30厘米，但仍旧证明了量子密码术的实用性。

1997年1月，美国国家标准技术研究所征集新一代数据加密标准，即高级数据加密标准（Advanced Encryption Standard，AES）。最终，比利时密码学家兼计算机科学家Vincent Rijmen和Joan Daemen设计的Rijndael加密算法入选，因此AES算法也称为Rijndael算法。高级数据加密标准用以替代原先的DES，谋求更加安全的加密算法。2002年5月26日，美国国家标准技术研究所将其定为有效的加密标准。

2003年，位于日内瓦的id Quantique公司和位于纽约的MagiQ技术公司，推出了传送量子密钥的距离超越了贝内特实验中30厘米的商业产品。由此，量子密码学进入商业化。

进入计算机加密阶段后，密码学应用不再局限于军事、政治和外交领域，逐步扩大到商务、

金融等社会的其他各个领域。密码学的研究和应用已大规模扩展到了民用方面。

2.2 密码学定义、术语及其分类

历经四千多年的风风雨雨，密码学逐步发展成为一门学科，对于它的定义也越来越清晰，那么什么是密码学呢？

- 密码学：主要是研究保密通信和信息保密的学科，包括信息保密传输和信息加密存储等。密码学包含密码编码学（Cryptography）和密码分析学（Cryptanalyst）两个分支。编码学与分析学相互促进，又相互制约。一方面，两者在加强密码分析的安全上相互促进；另一方面，两者在实施更为有效的攻击方面也相互影响。
- 密码编码学：主要研究如何对信息进行编码，如何实现对信息的隐蔽，是密码学理论的基础，也是保密系统设计的基础。
- 密码分析学：主要研究加密消息的破译或消息的伪造，是检验密码体制安全性最为直接的手段，只有通过实际密码分析考验的密码体制，才是真正可用的。

2.2.1 密码学常用术语

在简要了解了密码学的一些基本概念后，让我们来看一下密码学常用术语，如下所示：

- 明文（Plaintext）：指待加密信息。明文可以是文本文件、图片文件、二进制数据等。
- 密文（Ciphertext）：指经过加密后的明文。密文通常以文本、二进制数据等形式存在。
- 发送者（Sender）：指发送消息的人。
- 接收者（Receiver）：指接收消息的人。
- 加密（Encryption）：指将明文转换为密文的过程。
- 加密算法（Encryption Algorithm）：指将明文转换为密文的算法。
- 加密密钥（Encryption Key）：指通过加密算法进行加密操作用的密钥。
- 解密（Decryption）：指将密文转换成明文的过程。
- 解密算法（Decryption Algorithm）：指将密文转换为明文的算法。
- 解密密钥（Decryption Key）：指通过解密算法进行解密操作用的密钥。
- 密码分析（Cryptanalysis）：指截获密文者试图通过分析截获的密文从而推断出原来的明文或密钥的过程。
- 密码分析者（Cryptanalyst）：等同于密码破译者，指从事密码分析的人。
- 被动攻击（Passive Attack）：指对一个保密系统采取截获密文并对密文进行分析和攻击的行为。这种攻击对密文没有破坏作用。
- 主动攻击（Active Attack）：指攻击者非法入侵密码系统，采用伪造、修改、删除等手段向系统注入假消息进行欺骗的行为。这种攻击对密文具有破坏作用。
- 密码体制（Cipher System）：由明文空间、密文空间、密钥空间、加密算法和解密算法五部分构成。

- 密码协议（Cryptographic Protocol）：有时又称安全协议，是指以密码学为基础的消息交换的通信协议，其目的是在网络环境中提供各种安全服务。密码协议与密码算法同等重要，是当今密码学研究的两大课题。密码学是网络安全的基础，但网络安全不能单纯依靠安全的密码算法。密码协议是网络安全的一个重要组成部分，通过密码协议可以进行实体之间的认证、在实体之间安全地分配密钥或其他各种秘密、确认发送和接收的消息的不可否认性等。
- 密码系统（Cryptography）：指用于加密和解密的系统。加密时，密码系统输入明文和加密密钥，进行加密变换后，输出密文；解密时，密码系统输入密文和解密密钥，进行解密变换后，输入明文。一个密码系统由信源、加密变换、解密变换、信宿和攻击者组成。密码系统强调密码方案的实际应用，通常应当是一个包含软、硬件的系统。
- 柯克霍夫原则（Kerckhoffs'Principle）：又称柯克霍夫假说、公理或定律，是由奥古斯特·柯克霍夫（Auguste Kerckhoffs）在19世纪提出的密码理论，即数据的安全基于密钥而不是算法的保密。换句话说，系统的安全性取决于密钥，对密钥保密，对算法公开。信息论始祖克劳德·艾尔伍德·香农（Claude Elwood Shannon）将其改为“敌人了解系统”，这样的说法称为香农箴言。柯克霍夫原则是现代密码学设计的基本原则。

柯克霍夫原则：

- 即使非数学上不可破解，系统也应在实质（实用）程度上无法破解。
- 系统内不应含任何机密物，即使落入敌人手中也不会造成困扰。
- 密匙必须易于沟通和记忆，而无须写下，且双方可以很容易地改变密匙。
- 系统应可以用于电讯。
- 系统应可以携带，不应需要两个人或两个人以上才能使用（应只要一个人就能使用）。
- 系统应容易使用，不致让使用者的脑力过分操劳，也无须记得长串的规则。

2.2.2 密码学分类

密码学起源于古代，发展于现代。随着时间的推移，密码学不断完善，逐步拥有了众多分类。对密码学进行分类时，可以按时间划分，也可以按保密内容的算法划分，还可以按密码体制划分，下面详细介绍。

1. 按时间划分

从时间上密码学可以分为古典密码学和现代密码学，古典密码学以字符为基本加密单元，2.4节中会有详细的阐述；现代密码以信息块为基本加密单元。

2. 按保密内容的算法划分

根据保密内容的算法密码学可分为受限制算法密码学和基于密钥算法密码学。

- 受限制（Restricted）算法：算法的保密性基于保持算法的秘密。一般不赞成使用这种算法，除非应用于类似军事一类的应用，算法由专业机构开发、验证，确保其算法的安全性。这是古典密码学的主要特征。

- 基于密钥（Key-Based）算法：算法的保密性基于对密钥的保密。这其实是基于柯克霍夫原则设计的算法，这样做不但算法的公开有助于算法安全性的验证，算法的漏洞得以及时修正，还避免了算法的设计者在算法上留下后门。这正是现代密码学的主要特征。

3. 按密码体制划分

根据密码体制密码学可分为对称密码体制密码学和非对称密码体制密码学。

- 对称密码体制（Symmetric Cryptosystem）：又称单钥密码体制或私钥密码体制，将在2.5节详细阐述。该密码体制中的加密密钥与解密密钥相同，即加密过程与解密过程使用同一套密钥。
- 非对称密码体制（Asymmetric Cryptosystem）：又称双钥密码体制或公钥密码体制。该密码体制中的加密密钥与解密密钥不同，密钥分为公钥与私钥。公钥对外公开，私钥对外保密。

与上述密码体制对应的算法有对称密码算法和非对称密码算法。

- 对称密码算法（Symmetric Cipher）：又称单钥密码算法或私钥密码算法，指对应于对称密码体制的加密、解密算法。常见的DES、AES算法都是对称密码算法的典范。
- 非对称密码算法（Asymmetric Cipher）：又称双钥密码算法或公钥密码算法，指对应于非对称密码体制的加密、解密算法。大名鼎鼎的RSA算法就是非对称密码算法，多应用于数字签名、身份认证等。当然，非对称密码算法相对于对称密码算法有着更高的安全性，但也有着不可回避的加密、解密耗时长的问题。

4. 按明文的处理方法划分

根据明文的处理方法密码学可分为分组密码学和流密码学。

- 分组密码（Block Cipher）：指加密时将明文分成固定长度的组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。分组密码多应用于网络加密。
- 流密码（Stream Cipher）：又称序列密码，指加密时每次加密一位或一个字节的明文。手机平台对应用使用的系统资源有着极为苛刻的要求，这恰恰给了对系统资源要求极低的流密码以用武之地。RC4是相当有名的流密码算法。

在手工加密阶段和机械加密阶段，流密码曾是当时的主流。现代密码学的研究主要关注分组密码和流密码及其应用。在对称密码体制中，大部分加密算法属于分组密码。关于分组密码和流密码的详细内容，请阅读2.5节。

2.3 保密通信模型

密码学并不是孤立存在的，它需要有一个环境——保密通信模型。在了解了密码学的基本术语后，我们来讨论保密通信模型。

密码学的目的在于确保信息的保密传送。通常这样理解这层含义：信息的发送者和接收者在不安全的信道上进行通信，而破译者不能理解他们通信的内容。用保密通信模型来诠释这种

信息传送方式，如图2-1所示。

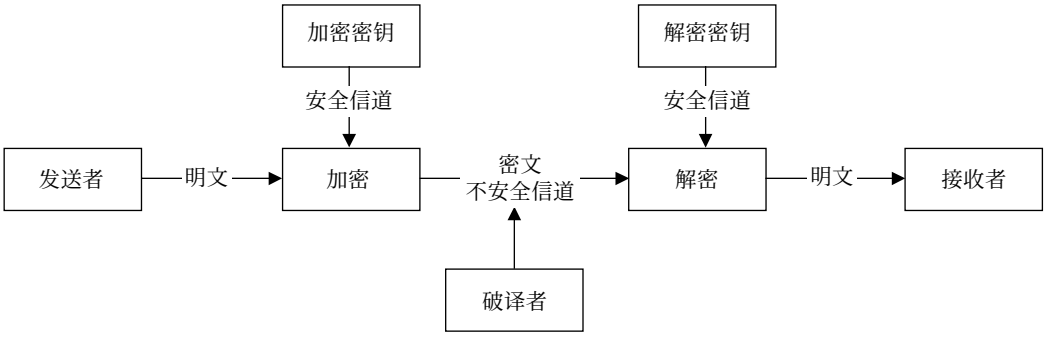

图2-1 保密通信模型

在上述模型中，信息的发送者和接收者要在不安全的信道上交换机要信息，为避免破译者窃听，需要对机要信息进行加密和解密处理。加密信息在传送过程中即使被破译者截获，也不能被破译。基于柯克霍夫原则，只要密钥安全，即便破译者知道该密码系统的加密算法，也无法对加密信息进行破译。在这个模型中，加密密钥很可能和解密密钥是同一个密钥，或者说由一方密钥可以推导出另一方密钥，这就是对称加密密码体制；反之，加密密钥与解密密钥不同，由一方密钥难以推导出另一方密钥，这就是非对称密码体制。

2.4 古典密码

古典密码（Classical Cipher）起始于古代终止于19世纪末，是现代密码的基础。当时生产力水平较低，普遍采用纸、笔或简单器械完成加密、解密操作，正是密码学发展史上手工加密阶段迅速发展的时期。虽然，古典密码由于安全性较低、效率低等多种缺陷已经退出了历史舞台，但古典密码对于密码学的研究却有着不可替代的作用。

古典密码受限于当时的环境，以语言学为基础对文字进行字符变化，也就是对字符加密，以达到信息加密的目的。古典加密算法最常用、最核心的两种加密技巧是移位和替代，这同样是对称加密算法最常用的方法。

- 移位密码（Transposition Cipher）：又称错位密码，即将字符的顺序重新排列。例如，将“1234567890”变成“3216549870”。这种加密算法看似简单，但却十分有效。如果不能领会其中的规律，很难辨别其内容的真正含义。
- 替代密码（Substitution Cipher）：又称置换密码，即将明文中的一组字符替代成其他的字符，形成密文。例如，“Encryption algorithm”变成“Fodszqujpo bmhpsjuin”（每个字母用下一个字母替代）。接收者对密文做反向替代就可以恢复明文。著名的凯撒密码就应用了替代式算法。

在古典加密时代，替代密码发展迅速，而且变得更加复杂，拥有众多分支，具体如下。

- 单表替代密码（Monoalphabetic Cipher）：又称简单替代密码。明文的一个字符用相应

的一个密文字符代替。加密过程就是从明文字母表到密文字母表一一映射的过程。主要包括移位（shift）密码、乘数（multiplicative）密码、仿射（affine）密码、多项式（Polynomial）密码、密钥短语（Key Word）密码。

- 同音替代密码（Homophonic Substitution Cipher）：又称多名替代密码。与单表替代系统相似，唯一的不同是单个字符明文可以映射成密文的几个字符之一，例如，A可能对应于5、13、25或56，“ B ”可能对应于7、19、31或42，所以，同音代替的密文并不唯一。电影《风语者》中，美军征召纳瓦霍人加入海军，训练他们使用纳瓦霍语言作为通信密码，这实际上就是应用了多名替代密码。
- 多表替代密码（Ployalphabetic Substitution Cipher）：明文中的字符映射到密文空间的字符还依赖于它在上下文中的位置。其由多个简单的代替密码构成，例如，可能有5个被使用的不同的简单代替密码，单独的一个字符用来改变明文的每个字符的位置。弗吉尼亚（Vigenere）密码、博福特（Beaufort）密码、滚动密钥（running-key）密码、弗纳姆 （Vernam）密码、转子机（rotor machine）密码均为多表替代密码。第二次世界大战中，德军用的转子加密机——Enigma，正是多表替代密码应用的典范。
- 多字母替代密码（Polygram Substitution Cipher）：明文中的字符被成组加密，例如“ ABA ”可能对应于“ RTQ ”，ABB可能对应于“ SLL ”等。希尔（Hill）密码、Playfair密码均为多字母替代密码。在第一次世界大战中英国就采用了这种密码。

不管是移位算法还是替代算法，终究脱离不开人类语言。针对该特点，通过对密文进行语义分析使得古典密码在破译上有章可循。例如，凯撒密码是单表替代密码，要破解凯撒密码，只要以语言学为基础，找出使用频度最高的字符，如' '（空格符）和 'e'，用ASCII码表示就是32和101，差值为69。如果明文中两个出现频率最高的字符的ASCII码相差69，那么加密后密文中相应出现频率最高的字符的ASCII码相差也一定是69。很显然，通过这样的分析方法，只要找出密文中与之对应的字符，计算偏移量——密钥，就可以破译密文，这就是著名的频度分析法。公元1578年，玛丽女王营救计划因密信被破解而以失败告终，当时使用的破解方法就是频度分析法。

2.5 对称密码体制

对称密码体制并不是现代密码学的新生产物，它是古典密码学的进一步延续。古典密码常用的两种技巧——替代和移位，仍然是对称密码体制中最重要的加密技巧。

对称密码体制的保密通信模型如图2-2所示。对称密码体制要求加密与解密使用同一个共享密钥，解密是加密的逆运算，由于通信双方共享同一个密钥，这就要求通信双方必须在通信前商定该密钥，并妥善保存该密钥。该密钥称为秘密密钥。秘密密钥的存在使得对称密码体制开放性变差。

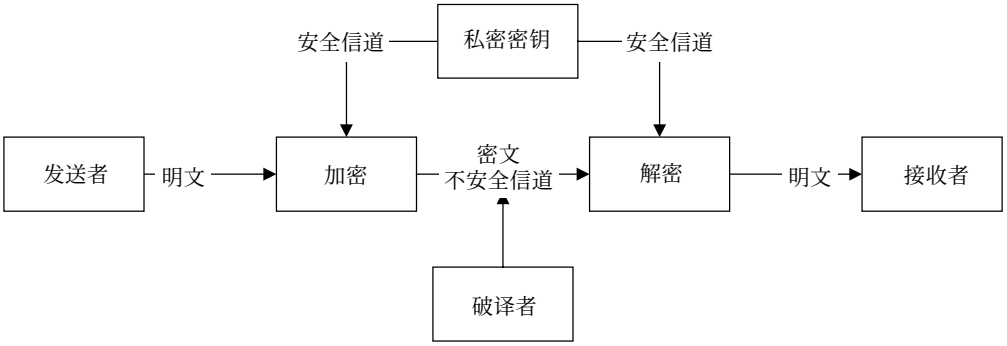

图2-2 对称密码体制的保密通信模型

对称密码体制分为两种：一种是对明文的单个位（或字节）进行加密和解密，称为流密码，又称为序列密码；另一种是把明文信息划分成不同的组（或块）结构，分别对每个组（或块）进行加密和解密，称为分组密码。

2.5.1 流密码

流密码是军事、外交等机要部门中应用最为广泛的对称密码体制。同时，它也是手机应用平台最常用的加密手段。流密码实现较为简单，加密时将明文按字符（或字节）逐位进行加密，解密时将密文按字符（字节）逐位解密。加密、解密可以是简单的位运算，如模n运算。明文加密后，生成的密文几乎和明文保持同样的长度。流密码加密与解密的流程如图2-3所示。

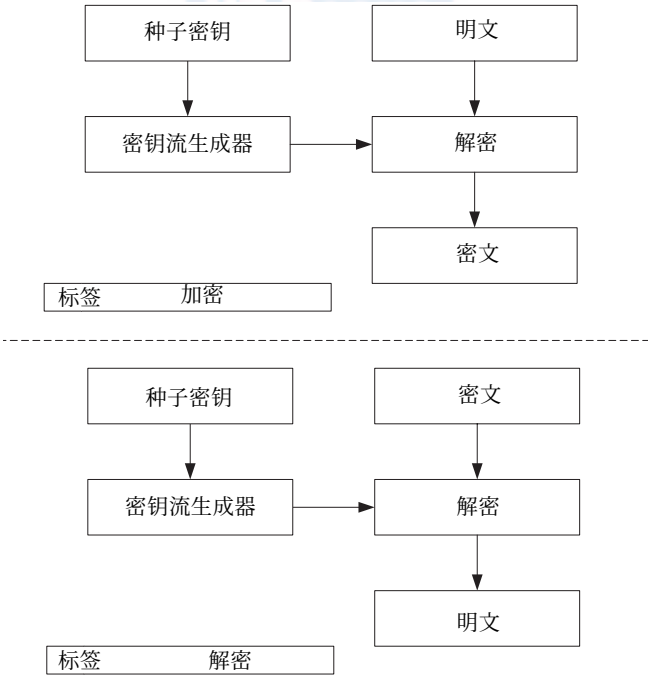

图2-3 流密码加密与解密流程

流密码分为同步流（序列）密码和自同步流（序列）密码。

1. 同步流密码

应用同步流密码，信息发送方和接收方在传递信息时，同步进行加密解密操作，明文与密文一一对应。密文的内容如果在传输过程中被篡改、删除或插入，可导致同步失效，以致密文解密失败，必须通过重新同步来实现解密、恢复密文。在密文传输过程中，如果一个密文位发生变化，那么该位的变化只影响该位的恢复，对后续密文位不影响，这是同步流密码的一个重要特点。但是，根据该特点主动攻击者可以有选择地对密文字符进行改动，并准确知道这些改动对明文的影响。因此，同步流密码具有同步性、无错误传递性及主动攻击性三种特性。同步流密码适用于为音频和视频数据提供版权保护。

2. 自同步流密码

与同步流密码相比，自同步流密码是一种有记忆变换的密码。每一个密钥与已产生的固定数量的密文位有关，密钥由已生成的密文决定。在密文传输过程中，如果一个密文位发生变化，那么该位的变化会影响到后续有限（如n位）的密文位的正确解密。所以，自同步流密码有错误传递现象。但是，在接收n位正确密文字符后，密码自身会实现重新同步。基于这一特点，如果主动攻击者对密文做了修改，接收方仍然不能检测出密文的完整性。与同步流密码相比，自同步流密码的密码分析更加困难，安全性更高。因此，自同步流密码具有自同步性、错误传递有限性、主动攻击性及明文统计扩散性四种特性。

流密码具有实现简单、便于硬件计算、加密与解密处理速度快、错误传播率低等优点。但是，流密码对错误的产生不够敏感，这是流密码的缺点。为了弥补这一缺点，流密码通常配合其他技术验证信息的完整性。流密码涉及大量的理论知识，受限于应用场合（目前主要用于军事和外交等机要部门），许多研究成果并未完全公开。目前使用较多的流密码是自同步流密码。流密码的常用算法有RC4和SEAL等。

流密码的安全强度依赖于密钥流生成器所产生的密钥流序列的特征，关键在于密钥生成器的设计以及信息收发两端密钥流产生的同步技术。

2.5.2 分组密码

分组密码多应用于网络加密，是对称密码体制中发展最为完善的密码体制。分组密码对固定长度的一组明文进行加密，这一固定长度称为分组长度。分组长度是分组密码的一个参数，它与分组算法的安全性成正比，其取值范围取决于实际应用的环境。为保证分组算法的安全性，分组长度越长越好，分组长度越长，密码分析越困难；为保证分组密码的实用性，分组长度越短越好，分组长度越短，越便于操作和运算。分组长度的设定需要权衡分组算法的安全性与实用性，一般设置为56位。但随着密码学的发展，分组长度只有56位的分组密码已经不能确保算法的安全性。目前，分组密码多选择128位作为算法的分组长度。

分组密码的加密过程是对一个分组长度为n的明文分组进行加密操作，相应地产生一个n位的密文分组，由此可见，不同的n位明文分组共有2^n个。考虑到加密算法的可逆性（即保证解

密过程的可行性），每一个不同的n位明文分组都应该产生一个唯一的密文分组，加密过程对应的变换称为可逆变换或非奇异变换。所以，分组密码算法从本质上来说是定义了一种从分组的明文到相应的密文的可逆变换。

分组密码是现代密码学的重要组成部分，具有代表性的分组加密算法有DES、AES等。我们将在后续章节具体探讨如何实现分组密码。

1. 分组密码设计原则

分组密码的设计原则包括安全性和实现性两个方面。前者主要研究如何设计安全算法、分组长度和密钥长度，后者主要讨论如何提高算法的执行速度。

（1）针对安全的一般设计原则

安全性原则又称不可破译原则，它包含理论上不可破译和实际上不可破译两重含义。香农认为：在理想密码系统中，密文的所有统计特性都与所使用的密钥独立。实用密码的两个一般的设计原则是指香农提出的混乱原则和扩散原则。

- 扩散（Diffusion）原则：人们所设计的密码应使得密钥的每一位数字影响到密文的多位数字，以防止对密钥进行逐段破译，而且明文的每一位数字也影响密文的多位数字以便隐藏明文数字的统计性。
- 混乱（Confusion）原则：人们所设计的密码应使得密钥和明文以及密文之间的信赖关系相当复杂以至于这种信赖性对密码分析者来说是无法利用的。

如何衡量一个密码体制的安全性？

主要在以下几个方面：

- 密码体制的破译所需要的时间和费用超出了现有的资源和能力。
- 密码体制的破译所需要的时间超过了该体制所保护的信息的有效时间。
- 密码体制的破译所需要的费用超过了该体制所保护的信息的价值。

（2）针对实现的设计原则

分组密码可以用软件和硬件来实现。硬件实现的优点是可获得高效率，而软件实现的优点是灵活性强、代价低。

- 软件实现的设计原则：使用子块和简单的运算。密码运算在子块上进行，要求子块的长度能自然地适应软件编程，如8位、16位、32位等。应尽量避免按位置换，在子块上所进行的密码运算尽量采用易于软件实现的运算。最好是用处理器的基本运算，如加法、乘法、移位等。
- 硬件实现的设计原则：加密和解密的相似性，即加密和解密过程的不同应局限于密钥使用方式上，以便采用同样的器件来实现加密和解密，以节省费用和体积。尽量采用标准的组件结构，以便能适应于在超大规模集成电路中实现。

2. 分组密码工作模式

我们以DES算法工作模式为例，DES算法根据其加密算法所定义的明文分组的大小（56位），将数据分割成若干56位的加密区块，再以加密区块为单位，分别进行加密处理。最后剩下的不足

一个区块的大小，我们称之为短块，短块的处理方法有填充法、流密码加密法、密文挪用技术。

1980年12月，DES算法工作模式被美国联邦信息处理标准组织（Federal Information Processing Standard，FIPS）标准化。加密算法应用的复杂性，有的强调效率，有的强调安全，有的强调容错性。根据数据加密时每个加密区块间的关联方式来区分，可以分为4种工作模式：电子密码本模式（Electronic Code Book，ECB）、密文链接模式（Cipher Book Chaining，CBC）、密文反馈模式（Cipher Feed Back，CFB）、输出反馈模式（Output Feed Back，OFB）。AES标准除了推荐上述4种工作模式外，还推荐了一种新的工作模式——计数器模式（Counter，CTR）。这些工作模式可适用于各种分组密码算法。

（1）电子密码本模式——ECB

电子密码本模式如图2-4所示，它是最基本、最易理解的工作模式。每次加密均产生独立的密文分组，每组的加密结果不会对其他分组产生影响，相同的明文加密后对应产生相同的密文，无初始化向量（也称为加密向量）。可以认为有一个非常大的电码本，对任意一个可能的明文分组，电码本中都有一项对应于它的密文，这也是该模式名称的由来。

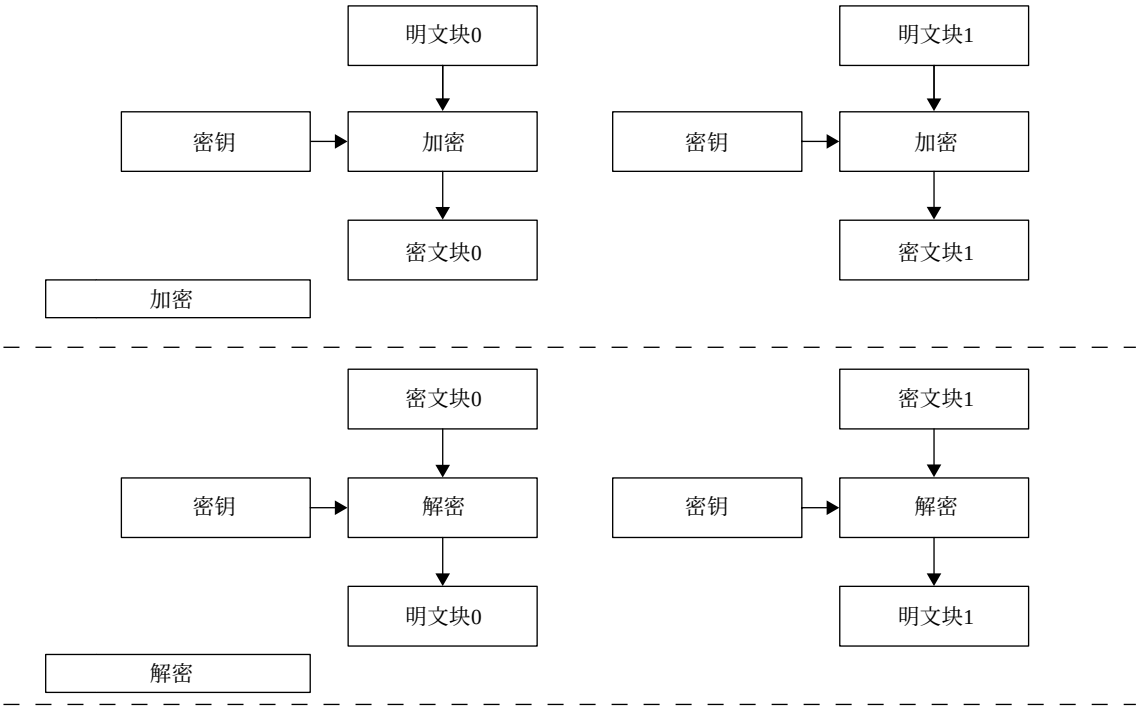

图2-4 电子密码本模式

- 优点：易于理解且简单易行；便于实现并行操作；没有误差传递的问题。
- 缺点：不能隐藏明文的模式，如果明文重复，则对应的密文也会重复，密文内容很容易被替换、重排、删除、重放；对明文进行主动攻击的可能性较高。
- 用途：适合加密密钥、随机数等短数据。例如，安全地传递DES密钥，ECB是最合适的模式。

（2）密文链接模式——CBC（已丧失安全性，不推荐使用）

密文链接模式如图2-5所示，它是目前应用最广泛的工作模式。明文加密前需先与前面的密文进行异或运算（XOR）后再加密，因此只要选择不同的初始向量，相同的明文加密后产生不同的密文。

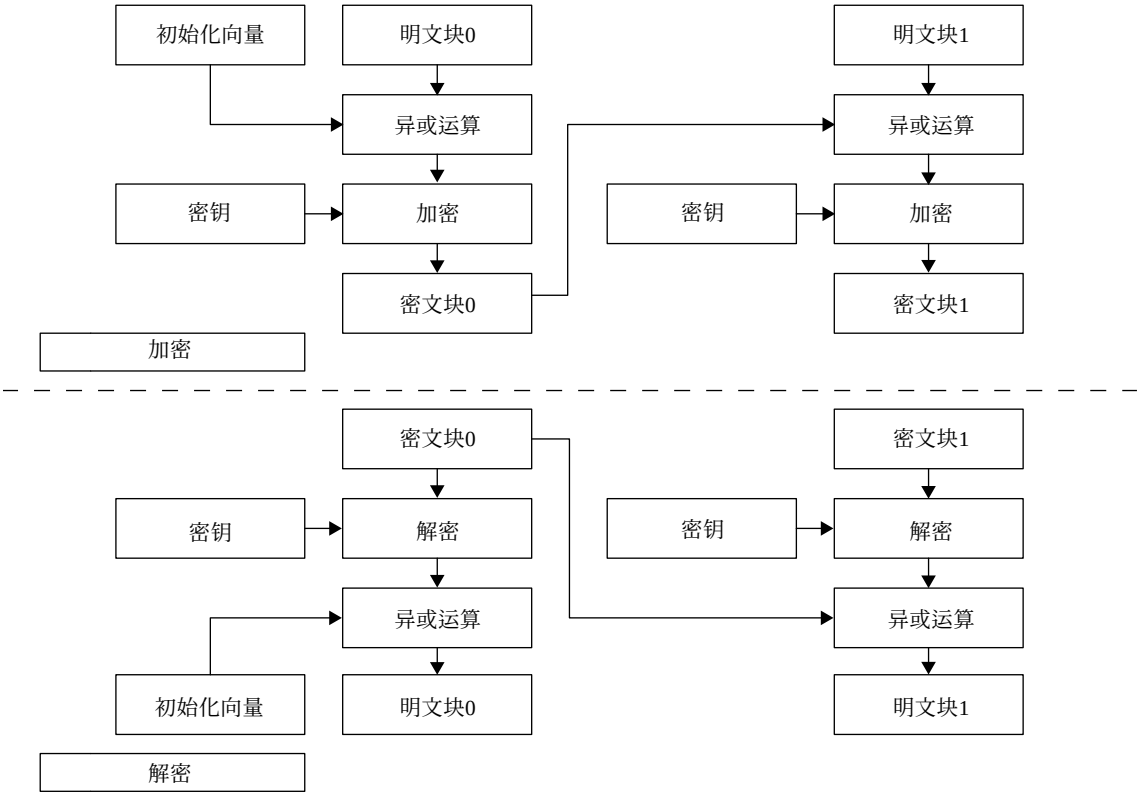

图2-5 密文链接模式

- 优点：密文链接模式加密后的密文上下文关联，即使在明文中出现重复的信息也不会产生相同的密文；密文内容如果被替换、重排、删除、重放或网络传输过程中发生错误，后续密文即被破坏，无法完成解密还原；对明文的主动攻击的可能性较低。
- 缺点：不利于并行计算，目前没有已知的并行运算算法；误差传递，如果在加密过程中发生错误，则错误将被无限放大，导致加密失败；需要初始化向量。
- 用途：可加密任意长度的数据；适用于计算产生检测数据完整性的消息认证码Mac。

（3）密文反馈模式——CFB

密文反馈模式如图2-6所示，它类似于自同步流密码，分组加密后，按8位分组将密文和明文进行移位异或后得到输出同时反馈给移位寄存器。它的优点是可以按字节逐个进行加密解密，也可以按*n*位字节处理。CFB是上下文相关的，明文的一个错误会影响后面的密文（错误扩散）。CFB需要一个初始化向量，加密后与第一个分组进行异或运算产生第一组密文；然后，对第一组密文加密后再与第二个分组进行异或运算取得第二组密文；以此类推，直到加密完毕。

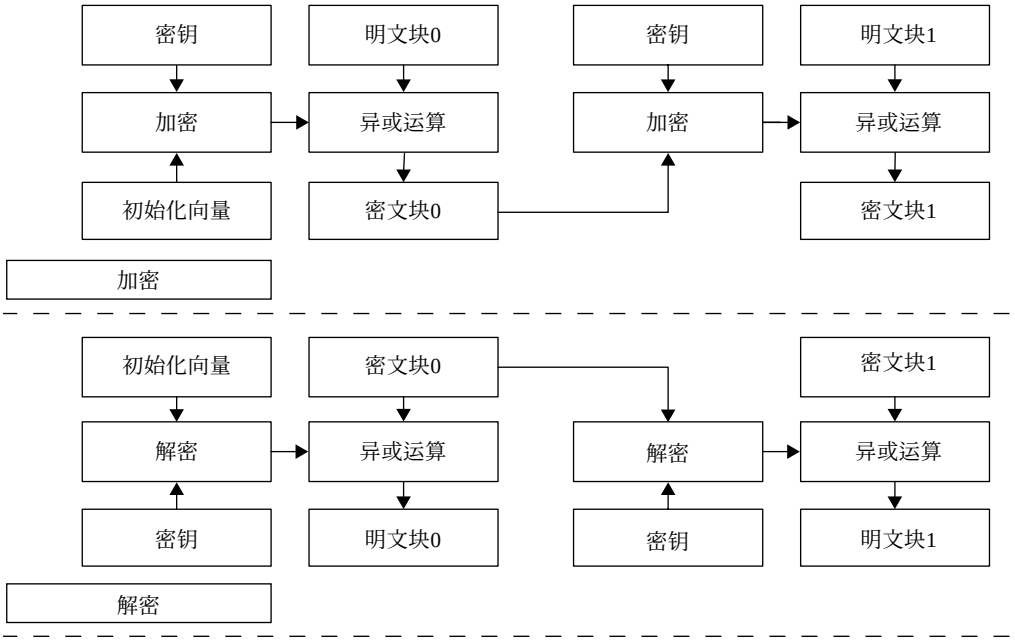

图2-6 密文反馈模式

- 优点：隐藏了明文的模式，每一个分组的加密结果必受其前面所有分组内容的影响，即使出现多次相同的明文，也均产生不同的密文；分组密码转化为流模式，可产生密钥流；可以及时加密传送小于分组的数据。
- 缺点：与CBC相类似。不利于并行计算，目前没有已知的并行运算算法；存在误差传送，一个单元损坏影响多个单元；需要初始化向量。
- 用途：因错误传播无界，可用于检查发现明文密文的篡改。

（4）输出反馈模式——OFB

输出反馈模式如图2-7所示，它将分组密码作为同步流密码运行，和CFB相似，不过OFB用的是前一个n位密文输出分组反馈给移位寄存器，OFB没有错误扩散问题。该模式产生与明文异或运算的密钥流，从而产生密文，这一点与CFB大致相同，唯一的差异是与明文分组进行异或的输入部分是反复加密后得到的。

- 优点：隐藏了明文的模式；分组密码转化为流模式；无误差传送问题；可以及时加密传送小于分组的数据。
- 缺点：不利于并行计算；对明文的主动攻击是可能的，安全性较CFB差。
- 用途：适用于加密冗余性较大的数据，比如语音和图像数据。

（5）计数器模式——CTR

计数器模式如图2-8所示，它的特点是将计数器从初始值开始计数所得到的值发送给分组密码算法。随着计数器的增加，分组密码算法输出连续的分组来构成一个位串，该位串被用来与明文分组进行异或运算。计数器模式是用来提取分组密码的最大效能以实现保密性的。在AES的实际应用中，经常会选择CBC模式和CTR模式，但更多的是选择CTR模式。

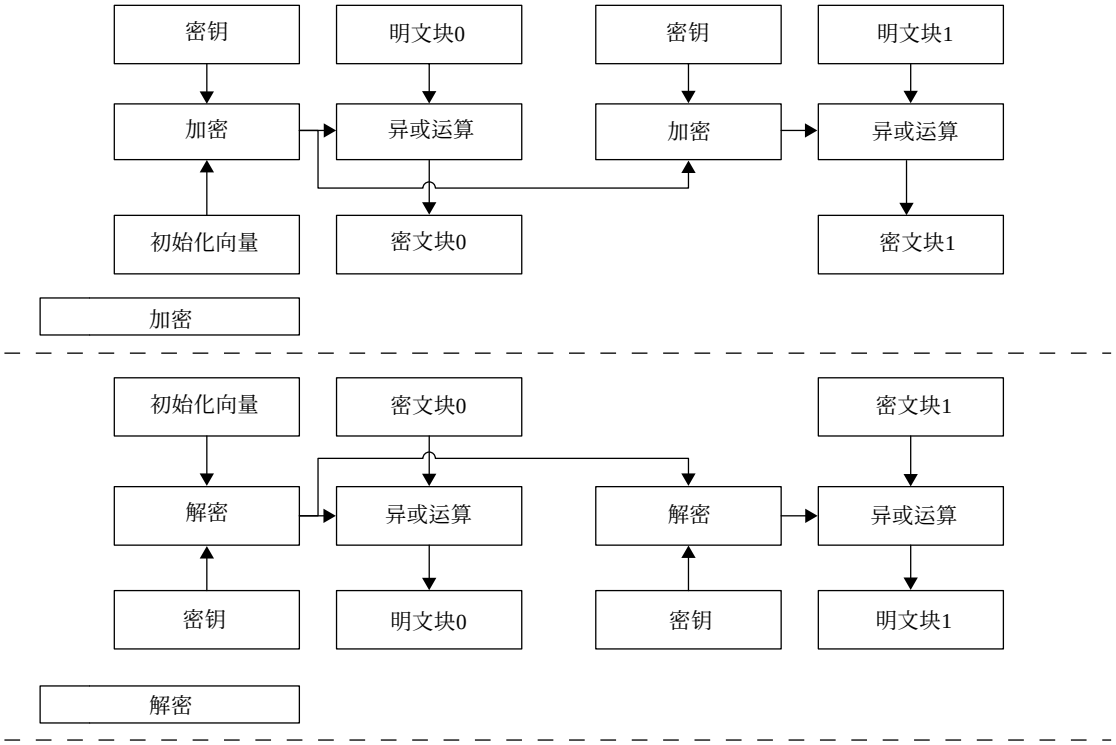

图2-7 输出反馈模式

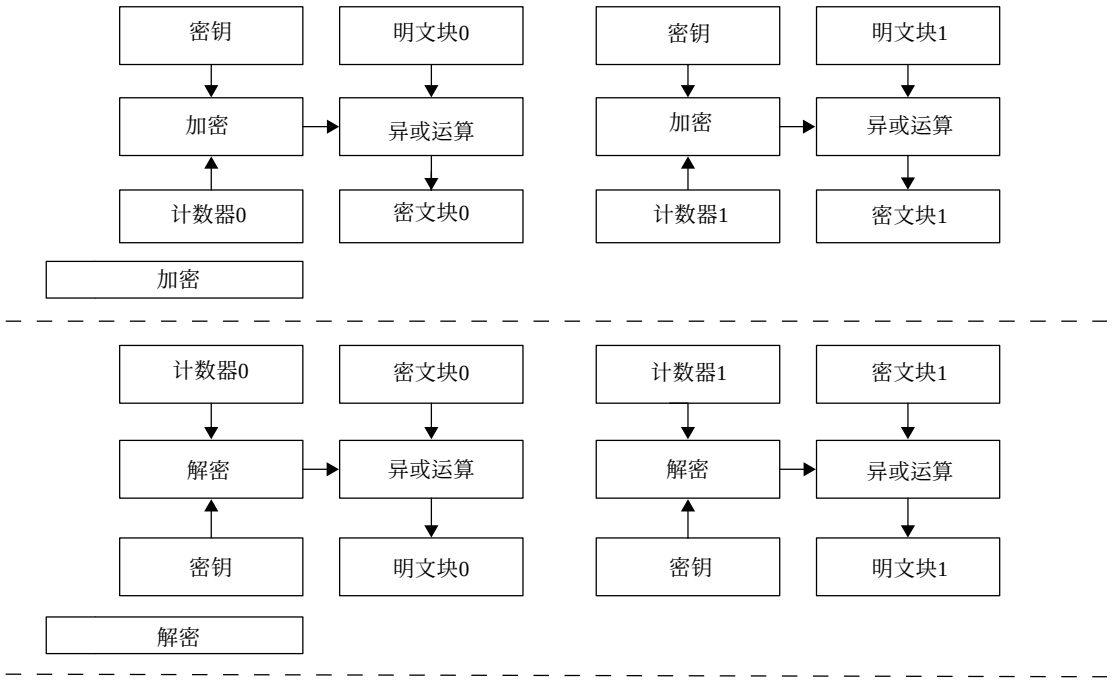

图2-8 计数器模式

- 优点：可并行计算；安全性至少与CBC模式一样好；加密与解密仅涉及密码算法的加密。
- 缺点：没有错误传播，因此不易确保数据完整性。
- 用途：适用于各种加密应用。

2.6 非对称密码体制

1976年，密码学专家Diffie和Hellman在《密码学的新方向》一文中提出了公开密钥密码体制的思想，开创了现代密码学的新领域，非对称密码体制的篇章由此揭开。

非对称密码体制的保密通信模型如图2-9所示。非对称密码体制与对称密码体制相对，它们的主要区别在于：非对称密码体制的加密密钥和解密密钥不相同，分为两个密钥，一个公开，一个保密。公开的密钥称为公钥，保密的密钥称为私钥。因此，非对称密码体制又称公钥密码体制。非对称密码体制使得发送者和接收者之间以无密钥传输的方法进行保密通信成为了可能，弥补了对称密码体制的缺陷。

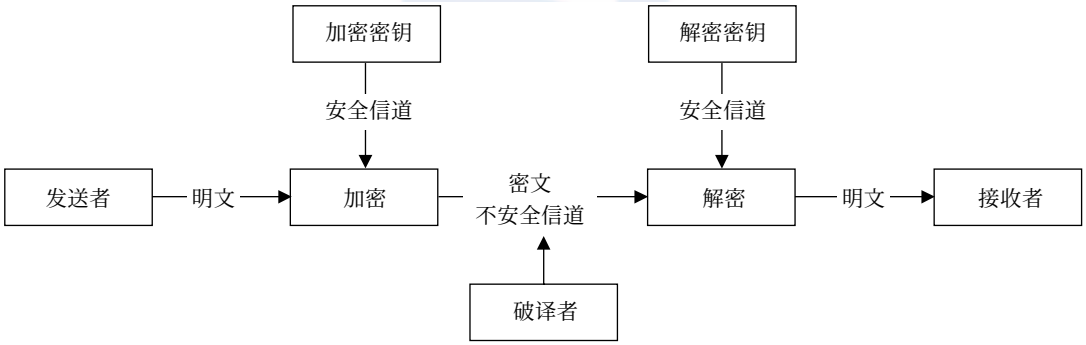

图2-9 非对称密码体制的保密通信模型

在非对称密码体制中，公钥和私钥均可用于加密与解密操作，但它与对称密码体制有极大的不同。公钥与私钥分属通信双方，一份消息的加密与解密需要公钥与私钥共同参与。公钥加密需要私钥解密，反之，私钥加密需要公钥解密。我们把通信双方定义为甲乙两方，甲乙两方分场景扮演信息发送者或接收者。公钥与私钥分属甲乙两方，甲方拥有私钥，乙方拥有公钥。为了更好地描述非对称密码体制通信流程，我们下面通过图的形式来说明甲乙双方如何完成一次完整的会话。

甲方（发送方）用私钥加密数据向乙方发送数据，乙方（接收方）接收到数据后使用公钥解密数据，如图2-10所示。

乙方（发送方）用公钥加密数据向甲方发送数据，甲方（接收方）接收到数据后使用私钥解密数据，如图2-11所示。

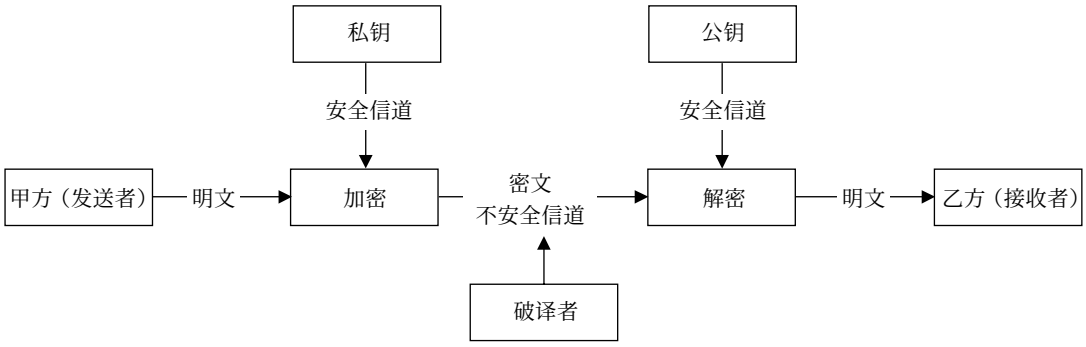

图2-10　私钥加密 - 公钥解密的保密通信模型

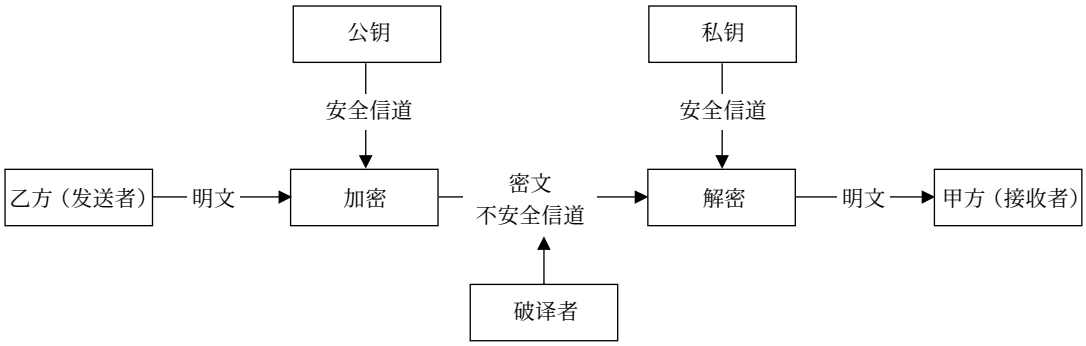

图2-11　公钥加密-私钥解密的保密通信模型

非对称密码体制的主要优点是可以适应开放性的使用环境，密钥管理问题相对简单，可以方便、安全地实现数字签名和验证。RSA是非对称密码体制的典范，它不仅可以完成一般的数据保密操作，同时它也支持数字签名与验证。关于数字签名，请参见2.8节。除了数字签名，非对称密码体制还支持数字信封等技术。我们将在后续章节详细讲述该类技术的具体实现。

非对称密码算法的安全性完全依赖于基于计算复杂度上的难题，通常来自于数论。例如，RSA源于整数因子分解问题；DSA —— 数字签名算法，源于离散对数问题；ECC —— 椭圆曲线加密算法，源于离散对数问题。由于这些数学难题的实现多涉及底层模数乘法或指数运算，相对于分组密码需要更多的计算资源。为了弥补这一缺陷，非对称密码系统通常是复合式的：用高效率的对称密码算法对信息进行加密解密处理；用非对称密钥加密对称密码系统所使用的密钥。通过这种复合方式增进效率。

2.7　散列函数

在讲到对称密码体制的流密码实现方式时，曾经提到过对于信息完整性验证需要其他技术来支持，这种技术就是由散列函数提供的消息认证技术。

散列函数，又称哈希函数、消息摘要函数、单向函数或杂凑函数。与上述密码体制不同的

是，散列函数的主要作用不是完成数据加密与解密的工作，它是用来验证数据完整性的重要技术。通过散列函数，可以为数据创建“数字指纹”（散列值）。散列值通常是一个短的随机字母和数字组成的字符串。消息认证流程如图2-12所示。

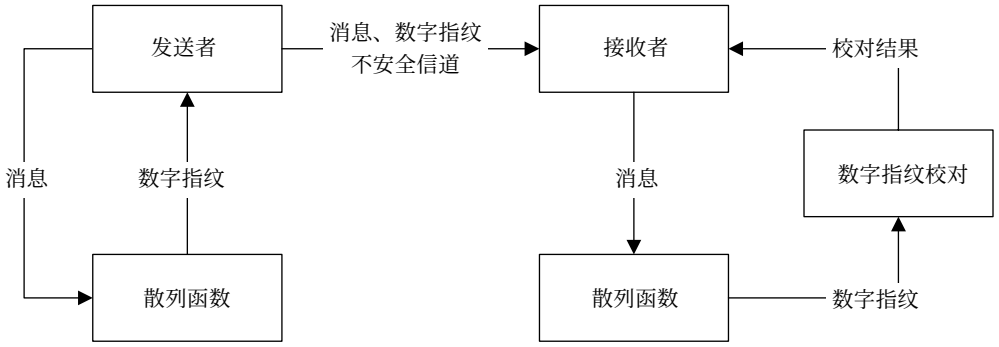

图2-12 消息认证流程

在上述认证流程中，信息收发双方在通信前已经商定了具体的散列算法，并且该算法是公开的。如果消息在传递过程中被篡改，则该消息不能与已获得的数字指纹相匹配。

散列函数具有以下一些特性：

- 消息的长度不受限制。
- 对于给定的消息，其散列值的计算是很容易的。
- 如果两个散列值不相同，则这两个散列值的原始输入消息也不相同，这个特性使得散列函数具有确定性的结果。
- 散列函数的运算过程是不可逆的，这个特性称为函数的单向性。这也是单向函数命名的由来。
- 对于一个已知的消息及其散列值，要找到另一个消息使其获得相同的散列值是不可能的，这个特性称为抗弱碰撞性。这被用来防止伪造。
- 任意两个不同的消息的散列值一定不同，这个特性称为抗强碰撞性。

散列函数广泛用于信息完整性的验证，是数据签名的核心技术。散列函数的常用算法有MD（消息摘要算法）、SHA（安全散列算法）及Mac（消息认证码算法）。我们将在后续章节详述上述散列函数的算法实现。

2.8 数字签名

通过散列函数可以确保数据内容的完整性，但这还远远不够。此外，还需要确保数据来源的可认证（鉴别）性和数据发送行为的不可否认性。完整性、可认证性和不可否认性，正是数字签名的主要特征。数字签名针对以数字形式存储的消息进行处理，产生一种带有操作者身份信息的编码。执行数字签名的实体称为签名者，签名过程中所使用的算法称为签名算法

（Signature Algorithm），签名操作中生成的编码称为签名者对该消息的数字签名。发送者通过网络将消息连同其数字签名一起发送给接收者。接收者在得到该消息及其数字签名后，可以通过一个算法来验证签名的真伪以及识别相应的签名者。这一过程称为验证过程，其过程中使用的算法称为验证算法（Verification Algorithm），执行验证的实体称为验证者。数字签名离不开非对称密码体制，签名算法受私钥控制，且由签名者保密；验证算法受公钥控制，且对外公开。RSA算法则既是最为常用的非对称加密算法，又是最为常用的签名算法。DSA算法是典型的数字签名算法，虽然其本身属于非对称加密算法不具备数据加密与解密的功能。

数字签名满足以下3个基本要求：

- ❑ 签名者任何时候都无法否认自己曾经签发的数字签名。
- ❑ 信息接收者能够验证和确认收到的数字签名，但任何人无法伪造信息发送者的数字签名。
- ❑ 当收发双方对数字签名的真伪产生争议时，通过仲裁机构（可信赖的第三方）进行仲裁。

数字签名认证流程如图2-13所示。在这里要提醒大家注意：私钥用于签名，公钥用于验证。签名操作只能由私钥完成，验证操作只能由公钥完成；公钥与私钥成对出现，用公钥加密的消息只能用私钥解密，用私钥加密的消息只能用公钥解密。

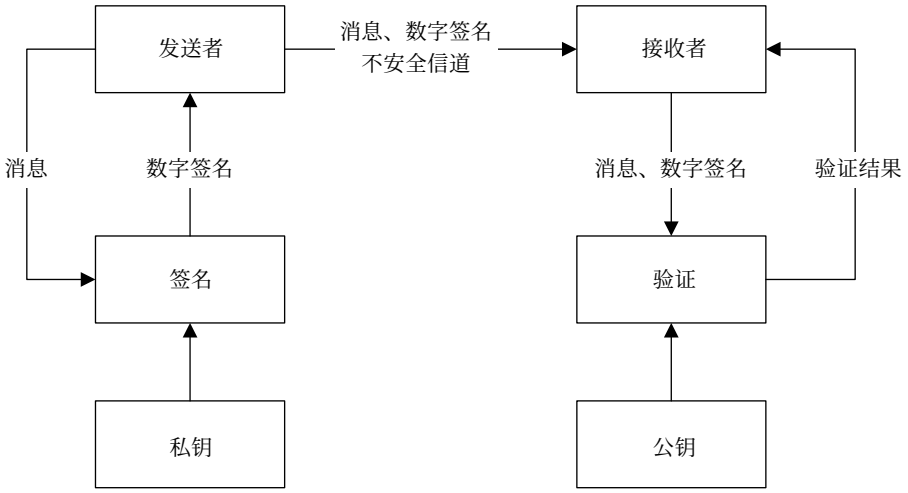

图2-13 数字签名认证流程

那么，数字签名认证是怎样一个流程呢？我们暂定甲方拥有私钥，并且甲方将公钥发布给乙方；当甲方作为消息的发送方时，甲方使用私钥对消息做签名处理，然后将消息加密后连同数字签名发送给乙方。乙方使用已获得的公钥对接收到的加密消息做解密处理，然后使用公钥及数字签名对原始消息做验证处理。

注意 当然，我们可以对消息先加密，然后对加密后的消息做签名处理，这样乙方获得消息后，先做验证处理，如果验证通过则对消息解密。反之，验证失败则抛弃消息。这样做显然可以提高系统的处理速度，但即便如此，作者仍建议大家对消息先做签名，再做加密处理。加密与签

名都应该只针对原始消息（明文）做处理。加密是为了确保消息在传送过程中避免被破解，签名是为了确保消息的有效性。消息本身可能就是一个可执行的文件，消息的接收方通过对消息的验证来判别该文件是否有权执行，而这个文件本身是不需要加密的。

由于签名不可伪造，甲方不能否认自己已发送的消息，而乙方可验证消息的来源以及消息是否完整。数字签名可提供OSI参考模型5种安全服务中的3种：认证（鉴别）服务、抗否认服务和数据完整性服务。正因如此，数字签名成为公钥基础设施以及许多网络安全机制的基础。

在上述认证过程的描述中，有些人可能会有这样的疑问：当乙方作为发送方，通过公钥将消息加密后发送给甲方时，由于算法、公钥公开，任何一个已获得公钥的窃听者都可以截获乙方发送的消息，替换成自己的消息发送给甲方，而甲方无法辨别消息来源是否是乙方。也就是说，上述的认证方式是单向的，属于单向认证。如果有两套公私钥，甲乙两方都对数据做签名及验证就可以避免这一问题。没错，这种认证方式正是双向认证。以网银交易为例，一般的网银交易使用的都是单向认证方式，无法验证使用者的身份；而要求较高的网银交易则都是双向认证方式，交易双方身份都可以得到验证。

2.9 公钥基础设施

公钥基础设施（Public Key Infrastructure，PKI）是一个基于X.509的、用于创建、分配和撤回证书的模型。PKI能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。换言之，PKI利用公钥密码技术构建基础设施，为网上电子商务、电子政务等应用提供安全服务。PKI技术是信息安全技术的核心，也是电子商务的关键和基础技术。如今大家所熟悉的网银交易系统就是PKI技术的具体体现。

PKI由公钥密码技术、数字证书、证书认证中心和关于公钥的安全策略等基本成分共同组成，对密钥和证书进行管理。因此，PKI技术涉及对称加密算法、非对称加密算法、消息摘要算法和数字签名等密码学算法。

我们目前所使用到的电子商务平台大部分都是基于PKI技术实现的。

2.9.1 PKI的标准

RSA公司定义了PKCS（Public Key Cryptography Standards，公钥加密标准），并定义了许多PKI基础组件，如数字签名和证书请求格式；IETF（Internet Engineering Task Force，互联网工程任务组）和PKIWG（Public Key Infrastructure Working Group，PKI工作组）定义了一组具有可操作性的公钥基础设施协议PKIX（Public Key Infrastructure Using X.509，公钥基础设施X.509）。

PKCS共有15项标准。

- PKCS#1：RSA公钥算法加密和签名机制
- PKCS#3：DH密钥交换协议
- PKCS#5：PBE加密标准

- PKCS#6：公钥证书（X.509证书的扩展格式）标准语法
- PKCS#7：加密消息语法标准
- PKCS#8：私钥信息格式
- PKCS#9：选择属性格式
- PKCS#10：证书请求语法
- PKCS#11：密码装置标准接口
- PKCS#12：个人信息交换语法标准
- PKCS#13：椭圆曲线密码体制标准
- PKCS#14：伪随机数生成标准
- PKCS#15：密码令牌信息格式标准

其中，PKCS#2和PKCS#4标准已被撤销，合并至PKCS#1中；较为常用的是PKCS#7、PKCS#10和PKCS#12。

上述标准主要用于用户实体通过注册机构（RA）进行证书申请、用户证书更新等过程。当证书作废时，注册机构通过认证中心向目录服务器发布证书撤销列表。上述标准还用于扩展证书内容、数字签名、数字签名验证和定义数字信封格式等情况。在构建密钥填充方式时，考虑到不同的安全等级，也会选择不同PKCS标准。

PKIX作为操作性标准涉及证书管理协议(Certificate Management Protocol，CMP)、安全多用途邮件扩展（S/MIME）和在线证书状态协议（Online Certificate Status Protocol，OCSP）等。

2.9.2 PKI系统的组成

PKI系统由认证中心（Certificate Authority，CA）、数字证书库（Certificate Repository，CR）、密钥备份及恢复系统、证书作废系统，以及应用程序接口（Application Programming Interface，API）五部分组成。其中，认证中心CA和数字证书库是PKI技术的核心。

1. 认证中心

CA是PKI的核心之一，是数字证书的申请及签发机构，且机构必须具有权威性，以确保公钥管理公开透明。

认证中心的主要功能如下：

- 证书发放
- 证书更新
- 证书撤销
- 证书验证

认证中心主要由注册服务器、注册机构（Registry Authority，RA），和认证中心服务器三部分组成。

2. 数字证书库

数字证书库用于存储已签发的数字证书及公钥，包括LDAP（Light Direct Access Protocol，轻量级目录访问协议）目录服务器和普通数据库。用户可通过数字证书库进行证书查询，并可

获得其他用户的证书及公钥。

3. 密钥备份及恢复系统

若用户丢失密钥则无法对数据解密，这将造成数据的丢失。为避免此类情况，PKI技术提供密钥备份及恢复功能。密钥的备份与恢复需要可信的权威机构来完成，这也是认证机构存在的必要条件。

4. 证书作废系统

为了确保证书的有效性，证书具有使用时效性，以确保证书所属环境的安全性。从另一个角度来讲，如果证书持有机构存在一定的安全性问题，即便证书未超过有效期，亦需要作废。PKI技术通过将证书列入作废证书列表（Certificate Revocation List，CRL）来完成证书作废操作。用户可以通过查询CRL来验证证书的有效性。

5. 应用程序接口API

为了便于用户能够方便地使用加密、签名验证等安全服务。PKI技术必须提供良好的应用程序接口，使得各式各样的应用，不同的系统架构都能以安全、一致、可信的方式与PKI进行交互，且能快速完成交互过程，以确保安全网络环境的完整性和易用性。

2.9.3 数字证书

数字证书是网络用户的身份标表，包含ID、公钥和颁发机构的数字签名等内容。其形式主要有X.509公钥证书、SPKI（Simple Public Key Infrastructure，简单PKI）证书、PGP（Pretty Good Privacy，译为“很好的私密”）证书和属性（Attribute）证书。其中，X.509证书最为常见。我们俗称的数字证书，通常指的是X.509公钥证书。

目前，我们所使用的X.509证书通常由VeriSign、GeoTrust和Thawte三大国际权威认证机构签发。VeriSign由RSA控股，借助RSA成熟的安全技术提供了较为广泛的PKI产品，其产品活跃在电子商务平台中。当我们在淘宝或者亚马逊上购物时，总能看到熟悉的VeriSign字样，如图2-14所示。

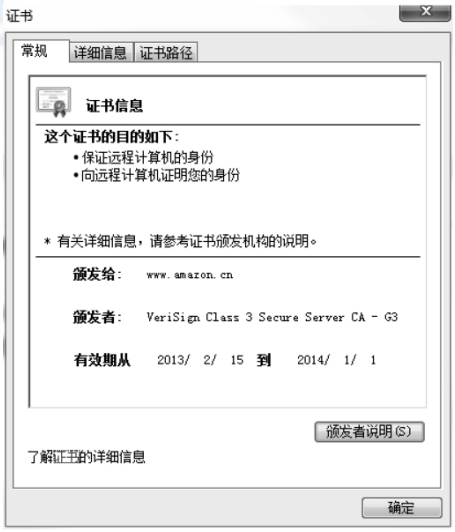

图2-14 VeriSign签发的数字证书

由于证书存在时效性，证书持有机构需要定期向认证机构申请证书签发。根据证书持有机构的证书使用范畴，认证机构会对不同的证书签发收取不同的费用。由此，证书持有机构需要每年向认证机构缴纳高额的年费。为了加强系统安全性，证书的密钥长度也会随着其费用递增。其中，价格最高的是商业网站的证书认证费用。上述的费用是认证机构得以生存的经济来源，同时也是电子商务平台等机构构建系统架构必须支付的安全成本之一。

2.10 PGP、OpenPGP与GPG

1991年Phil Zimmermann发布了一种用于数据加密和数字签名的程序，它使得一般人也可以很容易地对数据文件、邮件进行加密，这套程序就是PGP。PGP拥有“信任网络（Web of Trust）”的美称。PGP主要的特点是它可以在一个非安全的网络环境下，使得从未谋面的人取得信任。相比上面讲到的PKI，PGP根本不需要HTTPS，也不需要CA，仅需要一个可信赖的密钥托管服务器（基于LDAP的服务器）。

在PGP成为协议之前，它仅是一个软件，当然PGP还是PGP公司的注册商标。由于PGP被广泛应用，最终形成一个开放的标准——OpenPGP。GPG则是实现了该标准的一个开源免费程序。通过GPG可以对密钥进行管理、对文件和电子邮件进行加密/解密和数字签名等。

按照PKI的定义，PGP并不能完全看做基于X.509标准的某种实现，但却是X.509标准的有力补充。

对比X.509与PGP，有以下区别：

- X.509依赖于CA的信任链，即群签名；PGP不依赖于CA，依赖于可信赖的环签名。
- X.509主要应用于可信任的、安全的网络环境中，如电子商务平台等；PGP可用于不安全的网络环境中，如电子邮件等。

如果甲方和乙方在需要不安全的网络中传递敏感数据，可以使用PGP。PGP依赖于非公钥体制，用公钥对数据加密，用私钥对加密后的数据解密，黑客却无法通过公钥破解密文。而我们已知的PKI，是通过非公钥体制进行对称密钥交换，转而使用对称密钥完成加密操作。

PKI和PGP作为两套相辅相成的安全技术，备受安全技术公司的青睐。2010年，Symantec收购了PGP和VeriSign两家公司，主要是为了形成统一的数字证书解决方案。

Symantec已完成对PGP Corporation和VeriSign两家公司的收购。

2010年4月，Symantec以3亿美元收购PGP Corporation，并以7000万美元收购了GuardianEdge Technologies。此次收购，势必提升电子邮件、文件、硬盘，以及移动设备的加密技术强度。

同年10月，Symantec以12.8亿美元收购了VeriSign，这标志着数字证书1024位时代正式提前结束。

VeriSign的SSL(Secure Socket Layer)证书服务在美国商业市场占有率超过60%，Symantec希望将这项服务整合到其服务器保护组件中。VeriSign的身份保护和用户认证系统是基于云的，它能够对Symantec的身份认证解决方案进行有力的补充，能对客户、雇员、合作伙伴的各种设备进行验证和区分。VeriSign的PKI与Symantec收购的PGP和GuardianEdge融合，形成统一的数字证书解决方案。

2.11 密码学的未来

密码学历经四千年的锤炼，从古代走到了现代，从军用走向了民用，逐步贴近我们生活领域的每一个角落。密码学也有“新陈代谢”，当各种著名的国际级的密码算法被攻破时，就预

示着更加安全的密码算法即将诞生。

2.11.1 密码算法的破解

密码算法并不像我们想象的那么安全，我们所熟知的、常用的各种算法竟然都在历史的昨天就被破解。

1997年1月28日，美国的RSA数据安全公司在RSA安全年会上公布了一项“秘密密钥挑战”竞赛，其中包括悬赏1万美元破译密钥长度为56位的DES。位于美国科罗拉多州的程序员Verser从1997年2月18日起，用了96天时间，在网络上数万名志愿者的协同工作下，成功地找到了DES的密钥，赢得了悬赏的1万美元。

1998年7月，电子前沿基金会（EFF）使用一台当时价值25万美元的电脑在56小时内破译了密钥长度为56位的DES。

1999年1月，RSA数据安全会议期间，电子前沿基金会用22小时15分钟就宣告破解了一个DES的密钥。

2004年8月，在美国加州圣芭芭拉召开的国际密码大会（Crypto'2004）上，山东大学王小云教授宣告她和她的团队已经破解了MD5、HAVAL-128、MD4和RIPEMD四大国际著名密码算法。MD5算法的破解预示着SHA-1算法的末日。

2005年2月，较之MD5算法有着更高安全系数的SHA-1算法毫无悬念地被王小云教授破解了。MD5和SHA-1的破解，动摇了目前数字签名的理论根基，从理论上说明数字签名可以伪造。

2007年，Marc Stevens、Arjen K. Lenstra和Benne de Weger进一步指出通过伪造软件签名，可重复性攻击MD5算法。研究者使用前缀碰撞法（chosen-prefix collision），使程序前端包含恶意程序，利用后面的空间添上垃圾代码凑出同样的MD5散列值。

2008年，荷兰埃因霍芬技术大学科学家成功把两个可执行文件进行了MD5碰撞，使得这两个运行结果不同的程序被计算出同一个MD5。2008年12月一组科研人员通过MD5碰撞成功生成了伪造的SSL证书，这使得在HTTPS协议中服务器可以伪造一些根CA的签名。

2013年2月，NadhemAlFardan和Kenny Paterson发现了一种名为Luck13的攻击方式，这种攻击方式主要针对SSL/TLS中采取的CBC模式的块加密算法。攻击者可以通过阻断TLS连接的方式（比如通过恶意软件故意断掉链接，TLS会自动重发），让发送方反复发送同一加密内容（比如Cookie或者密码的密文），Luck13通过分析TLS发送错误信息的时间差异的分析，可以在较短时间内破解密文。所以建议在SSL/TLS中尽量不要使用CBC模式的块加密算法。

2013年3月，NadhemAlFardan、Dan Bernstein、Kenny Paterson、Bertram Poettering 和Jacob Schuldt共同宣布，采用RC4 加密的SSL/TLS也存在安全漏洞。目前网络上的SSL/TLS流量中大约50%是用RC4进行加密算法的。鉴于CBC模式的块加密方式以及RC4流加密都出现了漏洞，并且已经有了现实的攻击手法。建议企业最好是在SSL/TLS加密方式上选择更为安全的AES-GCM方式。

各种大名鼎鼎的密码算法的破解，更加带动了密码学前进的脚步。也许不久的将来，量子

密码学将成为密码学领域新一代的霸主！

2.11.2 密码学的明天

随着计算机网络应用的迅猛发展，人们对信息安全和保密的重要性认识不断提高，密码学在信息安全中起着的作用越来越重要，现在已成为信息安全中不可或缺的重要组成部分。从古代发展到现代，由军用转为民用，密码学有着广泛的发展前景。自动柜员机芯片卡、公交IC卡、电子商务等都离不开密码学的支持。甚至可以说有网络的地方，就有密码学的身影。随着各种具有高度安全系数的国际密码算法的破解，密码算法正经历着自己的“新陈代谢”。新的密码学理论层出不穷，新的密码算法崭露头角。我们坚信，密码学的明天将有无限可能。

2.12 小结

纵观密码学的发展史，它共经历了三个阶段，分别是手工加密阶段、机械加密阶段和计算机加密阶段。手工加密阶段最为漫长，期间孕育了古典密码，这为后期密码学的发展奠定了基础。机械工业革命发展的同时促进着各种科学技术的进步，密码学也不例外。加之两次世界大战，更加促进了密码学的飞速发展，密码学由此进入现代密码学阶段。尽管如此，在这一阶段的密码学仍旧未能摆脱古典密码学的影子，加密与解密操作均依赖于语言学的支持，转轮密码机Enigma的发明与破解更是将这一特点发挥到了极致。随着数据理论逐步介入，密码学逐渐成为一门学科，而非一门艺术。进入计算机加密阶段后，密码学应用不再局限于军事、政治和外交领域，逐步扩大到商务、金融和社会的其他领域。密码学的研究和应用已大规模扩展到了民用方面。

密码学主要包含两个分支：密码编码学和密码分析学。密码编码学针对于信息如何隐藏；密码分析学针对于信息如何破译。编码学与分析学相互影响，共同促进密码学的发展。

古典密码是现代密码的基础，移位和替代是古典密码最常用、最核心的两种加密技巧。由此，古典密码主要分为移位密码和替代密码。例如，凯撒密码就是替代密码的典范。替代密码其分支众多，包含单表替代密码、同音替代密码、多表替代密码和多字母替代密码。移位和替代技巧仍是现代密码学最常用的两种加密手段。

基于柯克霍夫原则，可对密码算法公开，也可对密钥保密。密码算法公开有助于提高算法的安全性，避免算法自身的漏洞，如算法的设计者为算法留有后门等。

从密码体制上划分，现代密码学共分为两种密码体制：对称密码体制和非对称密码体制。对称与非对称的差别源于加密密钥和解密密钥是否对称，即加密密钥与解密密钥是否相同（对称）。

在对称密码体制中，加密与解密操作使用相同的密钥，我们把这个密钥称为秘密密钥。DES、AES算法都是常用的对称密码算法。流密码和分组密码都属于对称密码体制。流密码实现简单，对环境要求低，适用于手机平台的加密，广泛应用于军事、外交领域。RC4算法就是典型的流密码算法。流密码的理论、算法受限于国家安全因素未能公布。分组密码在这一点上

与流密码恰恰相反，其理论、算法公开，分类众多。DES、AES算法等主要的对称密码算法均属于分组密码。分组密码共有5种工作模式：电子密码本模式（ECB）、密文链接模式（CBC）、密文反馈模式（CFB）、输出反馈模式（OFB）、计数器模式（CTR）。分组密码会产生短块，关于短块的处理方法有填充法、流密码加密法、密文挪用技术。

在非对称密码体制中，加密与解密操作使用不同的密钥。对外公开的密钥，称为公钥；对外保密的密钥，称为私钥。用公钥加密的数据，只能用私钥解密；反之，用私钥加密的数据，只能用公钥解密。RSA算法是常用的非对称密码算法。非对称密码体制同时支持数字签名技术，如RSA、DSA都是常用的数字签名算法。

散列函数可以有效地确保数据完整性，其是一项消息认证技术。常用的散列函数算法有MD5、SHA、Mac。散列函数也是数字签名技术中最重要的技术环节。数字签名离不开非对称密码体制，其私钥用于签名，公钥用于验证。基于数字签名的不可伪造性，数字签名技术成为5种安全服务中数据完整性服务、认证性服务和抗否认性服务的核心技术。通信双方只有一方提供数字签名的认证方式称为单向认证，通信双方都提供数字签名的认证方式称为双向认证。一般网银系统多采用单向认证方式，而要求较高的网银交易则都采用双向认证方式。

PKI和PGP是现代网络安全技术领域的两把锁。目前电子商务、电子政务使用PKI技术来确保平台安全性。PGP则多用于电子邮件、文件等的数据签名与加密。

密码学在不断地向前发展，只不过它的发展通常是以其密码算法的破解而引发，以更高安全系数算法的诞生而告一段落，密码学的明天将无可限量。