第3章

密码技术

学习目标

通过本章的学习，能够——

- 了解密码与密码学的概念；
- 了解现代密码技术的发展和应用；
- 知道密码技术的典型加密算法；
- 知道密码技术的应用；
- 掌握 Office 文件加密与解密的方法。

引导案例

公元前 405 年，雅典和斯巴达之间的伯罗奔尼撒战争已进入尾声。斯巴达军队逐渐占据了优势地位，准备对雅典发动最后一击。这时，原来站在斯巴达一边的波斯帝国突然改变态度，停止了对斯巴达的援助，意图是使雅典和斯巴达在持续的战争中两败俱伤，以便从中渔利。在这种情况下，斯巴达急需摸清波斯帝国的具体行动计划，以便采取新的战略方针。

正在这时，斯巴达军队捕获了一名从波斯帝国回雅典送信的雅典信使。斯巴达士兵仔细搜查这名信使，可搜查了好大一阵，除了从他身上搜出一条布满杂乱无章的希腊字母的普通腰带外，别无他获。情报究竟藏在什么地方呢？斯巴达军队统帅莱桑德把注意力集中到了那条腰带上，情报一定就在那些杂乱的字母之中。他反复琢磨研究这些天书似的文字，把腰带上的字母用各种方法重新排列组合，怎么也解不出来。最后，莱桑德失去了信心，他一边摆弄着那条腰带，一边思考着弄到情报的其他途径。当他无意中把腰带呈螺旋形缠绕在手中的剑鞘上时，奇迹出现了。原来腰带上那些杂乱无章的字母，竟组成了一段文字。这便是雅典间谍送回的一份情报，它告诉雅典，波斯军队准备在斯巴达军队发起最后攻击时，突然对斯巴达军队进行袭击。斯巴达军队根据这份情报马上改变了作战计划，先以迅雷不及掩耳之势攻击毫无防备的波斯军队，并一举将它击溃，解除了后顾之忧，随后，斯巴达军队回师征伐雅典，终于取得了战争的最后胜利。

二战期间，纳粹特工在探测盟军机密军事情报后，将这些情报传递给他们的负责人，

从而决定作战方针。一次，盟军的检查员截获了一张设计图纸。这张设计草图上是3位年轻的模特，她们穿着时尚的服装。

表面上看起来，设计草图很寻常，然而这张看似“清白”的图纸没能瞒过英国反间谍专家们的眼睛。英国安全局的官员们识破了纳粹特工的诡计，命令密码破译员和检查员迅速破译这些密码。

“大批敌方援军随时可能到来。”最终从这张设计图纸上密码破译员们读出了这样的信息。

原来纳粹特工利用莫尔斯电码的点和长横等符号作为密码，把这些密码做成装饰图案，藏在图上诸如模特的长裙、外套和帽子等图案中。

可见掌握密码技术有着至关重要的作用。

3.1 密码技术概述

随着计算机通信被广泛地应用于商业、金融、政府及军事部门，如何防止日益严重的计算机犯罪，防止信息在通信过程中被非法泄露、删除和修改，已成为全社会关心的问题。密码技术作为信息加密、鉴别和签名的手段，已经成为数学家和计算机学家的主要研究课题。同时密码学也促进了计算机科学，特别是计算机与网络安全所使用的技术，如访问控制与信息的机密性。密码技术已被应用在日常生活，包括自动柜员机的芯片卡、计算机使用者存取密码、电子商务等，密码技术的发展已与人们的日常生活息息相关。

本节主要介绍密码与密码学的基本概念，密码技术的产生与发展历程，密码体制的分类和密码协议。

3.1.1 密码与密码学

1. 密码的基本概念

(1) 密码。

密码是按特定法则编成，用于对通信双方的信息进行明密变换的符号。换而言之，密码是隐蔽了真实内容的符号序列。就是把用公开的、标准的信息编码表示的信息通过一种变换手段，将其变为除通信双方以外其他人所不能读懂的信息编码，这种独特的信息编码就是密码。

密码的基础解释为，主要限定于个别人明白(如一则电文)的符号系统。如密码电报、密码式打字机。作为技术而言，密码是一种用来混淆的技术，它希望将正常的(可识别的)信息转变为无法识别的信息。当然，对相关人来说，这种无法识别的信息是可以再加工并恢复的。

密码在中文里是“口令”(password)的通称。登录网站、电子邮箱和银行取款时输入的“密码”严格来讲应该仅被称作“口令”，它不是本来意义上的“加密代码”，可以称为秘密的号码。

(2) 明文与密文。

明文是原始信息,即信息的原始形式。密文是明文经加密变换后的结果,即信息被加密处理后的形式。

(3) 加密与加密方式。

加密是指将原始正常的信息(明文)使用某种规则(加密算法)变换为不被外人理解的非正常信息(密文)的过程,加密是防止有价值的信息被拦截和窃取。

传统加密方式主要采用按字符逐位加密(称为流密码)与按字符分组加密(称为分组密码)。

现代加密方式主要采用按比特加密,每次只加密一个比特(称为序列密码)与按比特序列分组加密,每次处理一个比特分组(称为分组密码)。

(4) 加密算法。

进行明密变换的法则,即加密时使用的变换规则称为加密算法,复杂的规则可以用函数来表示并进行计算。

加密算法的基本类型可以分为以下四种:

① 换位——按照规定的图形和线路,改变明文字母或数码等的位置成为密文;

② 代替——用一个或多个代替表将明文字母或数码等代替为密文;

③ 密本——用预先编定的字母或数字密码组,代替一定的词组单词等,变明文为密文;

④ 加乱——用有限元素组成的一串序列作为乱数,按规定的算法,同明文序列相结合变成密文。

以上四种加密算法,既可以单独使用,也可以混合使用,以编制出各种复杂度很高的实用密码。

(5) 解密与解密算法。

加密的逆过程称为解密,其目的是将密文破译为明文。解密是由某种解密算法实现的。解密算法是将密文恢复为明文的规则或变换函数。

(6) 密钥。

为了有效控制加密和解密算法的实现,在其处理过程中要有通信双方掌握的专门信息参与,这种专门信息称为密钥,是函数运算中使用的参数。

2. 密码学

随着密码被广泛用于战争,交战双方为了保护自己的通信安全,窃取对方的情报,研究了各种方法,逐渐形成了密码学。它以研究秘密通信为目的,即对所要传送的信息采取一种秘密保护,以防止第三者对信息的窃取。密码学主要包含两部分内容:一是为保护自己的通信安全进行加密算法的设计和研究;二是为窃取对方情报而进行密码分析,即密码破译技术。

密码学作为一门学科,属于数学的一个分支,是密码编码学和密码分析学的统称。

密码编码学(简称编码学)主要研究密码变化的客观规律,设计难以被敌方或对手攻破,只能被己方知道的以不同加密算法构成的安全密码体制,即怎样编码,采用什么样的

密码体制以保证信息被安全地加密，是研究信息保密的科学和技术。

密码分析学（简称破译学）主要研究在未知密钥的情况下如何从密文推演出明文或密钥，破译敌方或对手已有的密码体制，应用于破译密码以获取通信情报，是研究破译密文的科学和技术。密码分析人员一般需要凭借经验，通过统计分析等方法，而不是通过逻辑导出。密码分析学通常采用两种方法：演绎法和归纳法。近年来，使用计算机进行密码分析从很大程度上提高了破译的能力。

3. 密码体制

密码体制也称密码系统，是指能完整地解决信息通信安全中的机密性、数据完整性、认证、身份识别、可控性及不可抵赖性等问题一个或几个的系统。一个密码体制的正确描述，需要用数学方法清楚地描述其中的各种对象、参数、解决问题所使用的算法等。

任何一种密码体制都包含 5 个要素：明文、密文、密钥、加密算法和解密算法。

（1）明文：是加密输入的原始信息，通常用 m 或 p 表示。所有可能明文的有限集称为明文空间，通常用 M 或 P 来表示。

（2）密文：是加密处理后输出的信息，通常用 c 表示。所有可能密文的有限集称为密文空间，通常用 C 来表示。

（3）密钥：是参与密码变换的参数，通常用 k 表示。一切可能的密钥构成的有限集称为密钥空间，通常用 K 表示。

（4）加密算法：是将明文变换为密文的变换函数，相应的变换过程称为加密，即编码的过程，通常用 E 表示，即 $c=E(K_E,p)$。

（5）解密算法：是将密文恢复为明文的变换函数，相应的变换过程称为解密，即解码的过程，通常用 D 表示，即 $p=D(K_D,c)$。

对于有实用意义的密码体制而言，总是要求它满足：$p=D(K_D,E(K_E,p))$函数，即用加密算法得到的密文总是能用一定的解密算法恢复出原始的明文来。而密文消息的获取同时依赖于初始明文和密钥的值，如图 3-1 所示。

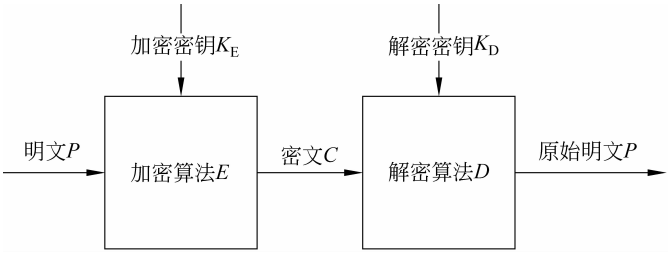

图 3-1　秘密通信过程

秘密通信的过程用文字可以表述为：若发送者要传送的明文 p，在传送前，利用密钥 K 将 p 经加密算法变换为密文 c 由通信通道发给接收者，接收者根据密钥 K 利用解密算法变换将密文 c 变为明文 p。

从以上过程可以看出，一个密码体制的安全性依赖于密钥 K 的个数和加密算法的复杂程度。密钥太少，敌方可以根据其截获的密文用不同的 K 逐个试译即可得到明文。也

不能太多，太多则不利于管理。加密算法太简单则容易找出解密算法，太复杂则导致解密过程耗费时间太多，不利于通信。

一个密码系统要是实际可用的，必须满足如下特性：

（1）每一个加密函数 E 和每一个解密函数 D 都能有效地计算。

（2）破译者取得密文后将不能在有效的时间或成本范围内破解出密钥或明文。

（3）一个密码系统是安全的必要条件——穷举密钥搜索是不可行的，因为密钥空间非常大。

3.1.2 密码学的发展

密码学的发展历程大致经历了三个阶段：古代手工加密阶段、古典机械密码阶段和现代密码学阶段。

1. 古代手工加密阶段

源于应用的无穷需求是推动技术发明和进步的直接动力。存于石刻或史书中的记载表明，许多古代文明，包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统。从某种意义上说，战争是密码技术进步的催化剂。人类自从有了战争，就面临着通信安全的需求，密码技术源远流长。

古代手工加密方法大约起源于公元前 440 年出现在古希腊战争中的隐写术。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发长长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。

公元前 400 年，斯巴达人发明了“塞塔式密码”，即把长条纸螺旋形地斜绕在一个多棱棒上，将文字沿棒的水平方向从左到右书写，写一个字旋转一下，写完一行再另起一行从左到右写，直到写完。解下来后，纸条上的文字消息杂乱无章、无法理解，这就是密文，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的消息，这是最早的密码技术。

我国古代的烽火也是一种传递军情的方法。古代的“兵符”就是用来传达信息的密令。

宋曾公亮、丁度等编撰的《武经总要》“字验”记载，北宋前期，在作战中曾用一首五言律诗的 40 个汉字，分别代表 40 种情况或要求，这种方式已具有了密本体制的特点。

连闯荡江湖的侠士和被压迫起义者都各自有一套秘密的黑道行话和地下联络的暗语。

2. 古典密码阶段（机械阶段）

古典密码的加密方法一般是文字置换，通过手工或机械变换方式实现。古典密码系统已经初步体现出现代密码体制的雏形，它比古代手工加密方法复杂。

公元前 1 世纪，著名的恺撒（Caesar）密码被用于高卢战争中，这是一种简单易行的单字母代换密码。

公元 9 世纪，阿拉伯的密码学家阿尔·金迪（Al’ Kindi，也被称为伊沙克 Ishaq，

801？—873 年，同时还是天文学家、哲学家、化学家和音乐理论家）提出解密的频度分析方法，通过分析计算密文字符出现的频率破译密码。

公元 16 世纪中期，意大利的数学家卡尔达诺（G. Cardano，1501—1576）发明了卡尔达诺漏格板，覆盖在密文上，可从漏格中读出明文，这是较早的一种分置式密码。

公元 16 世纪晚期，英国的菲利普斯（Philips）利用频度分析法成功破解苏格兰女王玛丽的密码信，信中策划暗杀英国女王伊丽莎白，这次解密将玛丽送上了断头台。

1834 年，伦敦大学的实验物理学教授惠斯顿发明了电机，这是通信向机械化、电气化跃进的开始，也为密码通信能够采用在线加密技术提供了前提条件。1881 年世界上的第一个电话保密专利出现。电报、无线电的发明使密码学成为通信领域中不可回避的研究课题。

1914 年第一次世界大战爆发，德俄相互宣战。在交战过程中，德军破译了俄军第一军发给第二军的电文，从中得知，第一军的给养已经中断。根据这一重要情报，德军在这次战役中取得了全胜。这说明当时交战双方已使用电机开展了密码战。

在第一次世界大战进行到关键时刻，英国破译密码的专门机构“40 号房间”利用缴获的德国密码本破译了著名的“齐默尔曼电报”，促使美国放弃中立参战，改变了战争进程。

1918 年，美国数学家吉尔伯特·维那姆发明一次性便笺密码，它是一种理论上绝对无法破译的加密系统，被誉为密码编码学的圣杯。但产生和分发大量随机密钥的困难使它的实际应用受到很大限制，从另一方面来说安全性也更加无法保证。

1920 年，美国电报电话公司的弗纳姆发明了弗纳姆密码。其原理是利用电传打字机的五单位码与密钥字母进行模 2 相加。如若信息码（明文）为 11010，密钥码为 11101，则模 2 相加得 00111 即为密文码。接收时，将密文码再与密钥码模 2 相加得信息码（明文）11010。这种密码结构在今天看起来非常简单，但由于这种密码体制第一次使加密由原来的手工操作进入到由电子电路来实现，而且加密和解密可以直接由机器来实现，因而在近代密码学发展史上占有重要地位。

在第二次世界大战初期，德国使用了一种命名为“恩尼格玛”（Enigma），也称“谜”的密码机，能产生 220 亿种不同的“密钥”组合，如果一个人每分钟测试一个密码，则需要 1.2 万年才能将所有的“密钥”可能组合试完。因此，希特勒完全相信其安全性。盟军对德军加密的信息有好几年一筹莫展，“恩尼格玛”密码机似乎是不可破的。

但是经过盟军密码分析学家的不懈努力，“恩尼格玛”密码机被攻破，英国却获知了“谜”型机的密码原理。英国在伦敦北边一百千米处征集了一块空地，如图 3-2 所示，在那里集结了一大批杰出的数学家、语言学家和象棋大师。其中包括计算机的开山鼻祖图灵（A. Turing）和创办世界上第一个人工智能系统的米基（D. Michie）。他们专门负责截获、破译“谜”型机的密码。由于这个组织的努力，特别是图灵出色的工作，使他们掌握了一整套破译该密码的方法，并完成了一部专门针对“谜”型机的绰号叫“炸弹”的密码破译机，每秒可处理 2000 个字符，几乎可破译截获德国的所有情报。后来又研制出一种每秒可处理 5000 个字符的“巨人”型密码破译机，并投入使用。至此，英方几乎掌握了德国纳粹的绝大多数军事密码和情报，从而掌握了战争的主动权，而德国军方却一无所知。图灵等人为英美联军击败德军做出了突出的贡献。有人估算，如果没有他们的贡献，第二次世界大战

至少还要再打 10 年。

图 3-2　图灵在二战期间英国破译德军密码的基地

在太平洋战争中，由于美国破译了日本海军的九七式机械密码，就在日本舰队司令官山本五十六命令换炸弹的五分钟内，美军在中途岛彻底击溃了日本海军，导致了太平洋战争的决定性转折，日本海军大将山本五十六也因密码电报被美国截获破译而被击毙在飞机上。因此，密码学为战争的胜利立下了大功。

古典密码的代表密码体制主要有单表代换密码、多表代换密码及转轮密码。古典密码体制的主要特点是数据的安全基于算法的保密。

古典密码的发展历史悠久，尽管这些密码比较简单，但它在今天仍有其参考价值。

3. 现代密码学（计算机阶段）

（1）密码体制模型。

1949 年前密码的研究还称不上是一门科学。直到 1949 年香农在《贝尔系统技术》（bell system technical）杂志上发表了一篇题为“保密系统的通信理论”（communication theory of secrecy system）的著名论文，该文首先将信息论引入了密码，从而把已有数千年历史的密码学推向了科学的轨道，奠定了密码学的理论基础，从而密码成为一门科学。该文利用数学方法对信息源、密钥源、接收和截获的密文进行了数学描述和定量分析，提出了通用的密码体制模型。

需要提出的是，由于受历史的局限，20 世纪 70 年代中期以前的密码学研究基本上是秘密地进行，而且主要应用于军事和政府部门，1949—1975 年这段时间内，密码学的理论进展不大。

（2）数据加密标准 DES。

密码学的真正蓬勃发展和广泛的应用是从 20 世纪 70 年代中期开始的。这是受计算机科学蓬勃发展刺激和推动的结果。快速电子计算机和现代数学方法一方面为加密技术提供了新的概念和工具，另一方面也给破译者提供了有力武器。计算机和电子学时代的到来给密码设计者带来了前所未有的自由，他们可以轻易地摆脱原先用铅笔和纸进行手工设计时易犯的错误，也不用再面对用电子机械方式实现的密码机的高额费用。

1975 年 1 月 15 日，对计算机系统和网络进行加密的数据加密标准（data encryption standard，DES）由美国国家标准局颁布为国家标准，这是密码术历史上一个具有里程碑意义的事件。

特别是 1977 年美国国家标准局颁布了数据加密标准 DES 用于非国家保密机关，该

系统完全公开了加密、解密算法。此举突破了早期密码学的信息保密的单一目的，使得密码学得以在商业等民用领域广泛应用，从而给这门学科以巨大的生命力。

(3) 公钥密码体制。

在密码学发展的进程中的另一件值得注意的事件是在 1976 年，美国密码学家迪菲(Diffie)和赫尔曼(Hellman)在一篇题为“密码学的新方向”(new directions in cryptography)一文中提出了一个崭新的思想，建立了著名的公钥密码体制，引发了密码学上的一次革命性的变革。不仅加密算法本身可以公开，甚至加密用的密钥也可以公开。但这并不意味着保密程度的降低。因为如果加密密钥和解密密钥不一样，将解密密钥保密就可以。若存在这样的公钥体制，就可以将加密密钥像电话簿一样公开，任何用户当他想经其他用户传送加密信息时，就可以从这本密钥簿中查到该用户的公开密钥，用它来加密，而接收者能用只有他所具有的解密密钥得到明文。任何第三者不能获得明文。

1978 年，由美国麻省理工学院的里维斯特(Rivest)，沙米尔(Shamir)和阿德曼(Ademan)三人提出了 RSA 公钥密码体制，它是第一个成熟的、迄今为止理论上最成功的公钥密码体制。它的安全性是基于数论中的大整数因子分解。该问题是数论中的一个困难问题，至今没有有效的算法，这使得该体制具有较高的保密性。

公钥密码体制的主要特点是数据的安全基于密钥而不是算法的保密。

1985 年，英国牛津大学物理学家戴维·多伊奇(David Deutsch)提出量子计算机的初步设想，这种计算机一旦造出来，可在 30 秒钟内完成传统计算机要花上 100 亿年才能完成的大数因子分解，从而破解 RSA 运用这个大数产生公钥来加密的信息。

1985 年，美国的贝内特(Bennet)根据他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。尽管通信距离只有 30cm，但它证明了量子密码术的实用性。与一次性便笺密码结合，同样利用量子的神奇物理特性，可产生连量子计算机也无法破译的绝对安全的密码。

2003，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 30cm 的商业产品。市面上已有产品能够将密钥通过光纤传送几十千米。

(4) 认证体制。

按照人们对密码的一般理解，密码是用于将信息加密而不易破译，但在现代密码学中，由于网络的应用，除了信息保密外，还有另一方面的要求，即信息安全体制还要能抵抗对手的主动攻击。所谓主动攻击指的是攻击者可以在信息通道中注入他自己伪造的消息，以骗取合法接收者的相信。主动攻击还可能篡改信息，也可能冒名顶替，这就产生了现代密码学中的认证体制。该体制的目的就是保证用户收到一个信息时，他能验证消息是否来自合法的发送者，同时还能验证该信息是否被篡改。在许多场合中，如电子汇款，能对抗主动攻击的认证体制甚至比信息保密还重要。

(5) 现代密码编码学的特点。

现代密码编码学主要致力于信息加密、信息认证、数字签名和密钥管理方面的研究。信息加密的目的在于将可读信息转变为无法识别的内容，使得截获这些信息的人无法阅读；信息认证的目的在于信息的接收人能够验证接收到的信息是否被敌方篡改或替换过；

数字签名就是使信息的接收人能够确定接收到的信息是否确实是由所希望的发信人发出的;密钥管理是信息加密中最难的部分,因为信息加密的安全性在于密钥。历史上,各国军事情报机构在猎取别国的密钥管理方法上要比破译加密算法成功得多。

(6) 现代密码分析学的特点。

现代密码分析学与密码编码学不同,它不依赖数学逻辑的不变真理,必须凭经验,依赖客观世界觉察得到的事实。因而,密码分析更需要发挥人们的聪明才智,更具有挑战性。

现代密码学是一门迅速发展的应用科学。随着因特网的迅速普及,人们依靠它传送大量的信息,但是这些信息在网络上的传输都是公开的。因此,对于关系到个人利益的信息必须经过加密之后才可以在网上传送,这将离不开现代密码技术。

3.1.3 密码技术的应用领域

密码技术是在编码与破译的斗争实践中逐步发展起来的,从手工技术、机械技术到计算机技术,随着先进科学技术的应用,已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果,特别是各国政府现用的密码编制及破译手段都具有高度的机密性。

密码技术有着悠久的历史。在古代密码技术就被用于传递秘密消息。在近代和现代战争中,传递情报和指挥战争均离不开密码技术,外交斗争中也离不开密码技术。

随着计算机和信息技术的发展,密码技术的应用领域不断扩展。密码技术除了用于信息加密外,也用于数据信息签名和安全认证。因此,密码的应用不再局限于为军事、外交斗争服务,它被广泛应用在社会和经济活动中。

具体来说,密码技术主要应用于信息的保密、身份的确认、数据的完整性等领域。

1. 通信中的数据保护

密码技术应用于通信线路上信息的保护。一方面,防止传输中的信息被非法窃听导致失密,另一方面,防止信息的内容被恶意攻击者非法地篡改,并且在发生此类事件后能迅速发现。

2. 存储信息的保护

信息用密码技术加密处理后进行存储,保证只有掌握解密密钥的合法用户才能够存取数据,得到正确的明文。在许多用户的系统中,保护个人秘密、防止文件被破坏。

3. 通信双方的身份验证

密码技术不仅广泛应用于防止传输中的信息和记录存储的信息不被攻击者非法窃听、浏览和篡改,同时,也可以用于识别通信双方的真实性。这种对存取数据和发来电文的对方的合法性进行确证的方法叫“验证”。

4. 非否认性

密码技术还应用于不可否认性服务。它包含对源和目的双方的证明,通常的情况下,

不可否认服务是一种数字签名服务。

除此之外，密码技术还广泛地应用于计算机网络安全领域的其他方面，出现了密码技术应用的社会化和个人化趋势。例如，可以将密码技术应用在电子商务中，对网上交易双方的身份和商业信用进行识别，防止网上电子商务中的“黑客”和欺诈行为；应用于增值税发票中，可以防伪、防篡改，杜绝了各种利用增值税发票偷、漏、逃、骗国家税收的行为，并大大方便了税务稽查；应用于银行支票鉴别中，可以大大降低利用假支票进行金融诈骗的金融犯罪行为；应用于个人移动通信中，大大增强了通信信息的保密性等。

3.1.4 密码学的新概念和新技术

密码学的进一步发展，涌现了大量的新概念和新技术，这里主要介绍零知识证明技术、盲签名、比特承诺和量子密码技术。

1. 密码协议

(1) 协议的含义。

本书中的协议是指两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。协议具有以下三个特征：

① 协议自始至终是有序的过程，每一步骤必须依次执行，在前一步骤没有执行完之前，后面的步骤不可能执行。

② 协议至少需要两个参与者，一个人可以通过执行一系列的步骤来完成某项任务，但它不构成协议。

③ 通过执行协议必须能够完成某项任务。

(2) 协议的特点。

① 协议中的每个人都必须了解协议，并且预先知道所要完成的所有步骤。

② 协议中的每个人都必须同意遵循它。

③ 协议必须是不模糊的，每一步必须明确定义，并且不会引起误解。

④ 协议必须是完整的，对每种可能的情况必须规定具体的动作。

(3) 密码协议。

密码协议，也称作安全协议，是使用密码技术的协议。参与密码协议的人可能是朋友和完全信任的人，也可能是敌人和互相完全不信任的人，相互之间不信任的各方能够在网络上完成这些协议。

密码协议包含某种密码算法，但通常，协议的目的不仅仅是为了简单的秘密性。参与协议的各方可能为了计算一个数值想共享它们的秘密部分，共同产生随机系列，确定互相的身份，或者同时签署合同。在协议中使用密码的目的是防止或发现偷听者和欺骗。

2. 零知识证明

20 世纪 80 年代初，S. Goldwasser 等人提出了零知识证明这一概念。从本质上讲，零知识证明是一种协议。

零知识证明必须包括两个方面，一方为证明者，另一方为验证者。证明者试图向验证