第1章 绪 论

1.1 网络安全的需求分析

信息网络国际化、社会化、开放化和个人化的特点，在提供人们“信息共享”，给人类带来高效率的同时，也投下了不安全的阴影。计算机联成网络，开始进入了每一台计算机都可能被另外的计算机攻击的时期，网络安全问题突现出来。

网络安全包括物理安全和逻辑安全。物理安全指网络系统中各通信设备、计算机设备及相关设施的物理保护，使之免于被破坏、丢失等。逻辑安全包含网络系统中信息的完整性、保密性、非否认性、可用性和可控性。这是一个涉及网络、操作系统、数据库、应用系统、人员管理等诸多方面的事情，必须综合考虑。

保密性是一个古老的概念，近代成为战争的情报手段和政府专用技术。在传统信息环境中，普通人通过邮政系统发信件，为了个人隐私还要装上信封。可是到了使用数字化电子信息时代，以0、1位串编码，在网上传来传去，连个“信封”都没有，发的电子邮件都是“明信片”，哪还有什么秘密可言。对网上信息进行保护，这就是网络信息安全中的保密性需求。

人们进一步认识到，在传统社会中，不相识的人们相互建立信任需要介绍信，并且在上面签上名盖上章。但是在电子信息环境中如何签名盖章，怎么知道信息真实的发送者和接收者，怎么知道信息没有被伪造和篡改，并且在法律意义上做到责任的不可抵赖，这就成为人们归纳的网络信息安全中的完整性和非否认性需求。

人们还意识到信息和信息系统都是它的所有者花费了代价建设起来的。但是，存在着由于计算机病毒或其他人为的原因可能造成的对主人的拒绝服务，以及被他人滥用信息的情况。这就提出网络信息安全中的可用性需求。

由于社会中存在不法分子，地球上各国之间还时有由于意识形态和利益冲突

造成的敌对行为。政府对社会的执法管理行为（如搭线监听犯罪分子的通信），在社会广泛使用信息安全设施和装置时可能受到严重影响，以至不能实施。这就出现了信息安全中的可控性需求。

网络中的安全威胁主要有：

（1）身份窃取，指用户身份在通信时被非法截取。

（2）假冒，指用户假冒合法用户身份获取敏感信息的行为。

（3）数据窃取，指非法用户截获通信网络的数据。

（4）否认，指通信方事后否认曾经参与某次活动的行为。

（5）对网上资源的非授权访问。

（6）拒绝服务，指合法用户的正当申请被拒绝、延迟、更改等。

（7）错误路由。

（8）病毒传播。

目前网络安全已不再是军方和政府要害部门的一种特殊需求。实际上，所有的网络应用环境包括银行、电子交易（无密级的）、公共电信载体和互联／专用网络，都有网络安全的需求。关于这些典型环境的安全需求参见表1.1。

表 1.1　　典型的网络安全需求

应用环境	需　求	应用环境	需　求
所有网络	阻止外部的入侵（黑客）	电子政务	避免无密级而敏感的信息的未授权泄漏或修改 为政府文件提供电子签名
银　行	避免欺诈或交易的意外修改 识别零售的交易顾客 保护个人识别号（PIN）以免泄漏，确保顾客的秘密	公共电信载体	对授权的个人限制访问管理功能 避免服务中断 保护用户的秘密
电子交易	确保交易的起源和完整性 保护客户、商户、银行的秘密 为交易提供合法的电子签名	互联／专用网络	保护团体／个人的秘密 确保消息的真实性

1.2 密码学的主要研究内容

密码学经历了漫长的发展过程，近30年来随着信息技术的发展，得到了飞速的发展。

当前，密码理论与技术主要包括两部分，即基于数学的密码理论与技术（包括序列密码、分组密码、公钥密码、认证码、数字签名、哈希函数、身份识别、密钥管理、PKI技术等）和非数学的密码理论与技术（包括信息隐形、量子密码、基于生物性的识别理论与技术等）。

序列密码虽然主要用于政府、军方等国家要害部门，而且用于这些部门的理论和技术都是保密的，但由于一些数学工具（比如代数、数论、概率等）可用于研究序列密码，其理论和技术相对而言比较成熟。从20世纪80年代中期到90年代初，出现了序列密码研究的热潮，在序列密码的设计、生成和分析方面出现了一大批有价值的成果。虽然，近年来序列密码不是一个研究热点，但有很多有价值的公开问题需要进一步解决，比如自同步流密码的研究，有记忆前馈网络密码系统的研究，混沌序列密码和新研究方法的探索等。另外，虽然各国还没有制定序列密码标准，但在一些系统中已将序列密码比如 RC4 广泛应用于存储加密。事实上，欧洲的NESSIE计划中已经包括了序列密码标准的制定，这一举措有可能导致序列密码研究的新热潮。

美国早在1977年就制定了自己的数据加密标准（是一种分组密码），但除了公布具体的算法之外，从来不公布详细的设计规则和方法。随着美国的数据加密标准的出现，人们对分组密码展开了深入的研究和讨论，设计了大量的分组密码，给出了一系列的评测准则。其他国家比如日本和前苏联也纷纷提出了自己的数据加密标准。但在这些分组密码中能被人们普遍接受和认可的算法却寥寥无几。何况一些算法已经被攻破或已经不适用于技术的发展要求。比如美国的数据加密标准（DES）已经于1997年6月17日被攻破。美国从1997年1月起，征集、制定和评估新一代数据加密标准（称作 AES），经过多轮评审已终选出算法 Rijndael，将作为替代 DES 的新一代数据加密标准。AES活动使得国际上又掀起了一次研究分组密码的新高潮。继美国征集 AES活动之后，欧洲和日本也不甘落后，启动了相关标准的征集和制定，看起来比美国更宏伟。

自从1976 年公钥密码的思想提出以来，国际上已经提出了许多种公钥密码体制，但比较成熟的主要有两类：一类是基于大整数因子分解问题的，其中最典型的代表是 RSA 。另一类是基于离散对数问题的，比如 ElGamal公钥密码和影响比较大

的椭圆曲线公钥密码。由于分解大整数的能力日益增强，所以对 RSA 的安全带来了一定的威胁。目 前768位模长的 RSA 已不安全,一般建议使用 1 024位模长,预计要保证20年的安全就要选择1 280位的模长，增大模长带来了实现上的难度。而基于离散对数问题的公钥密码在目前技术下512位模长就能够保证其安全性。特别是椭圆曲线上的离散对数的计算要比有限域上的离散对数的计算更困难，目前技术下只需要160位模长就可以取得相当于1 024位模长的 RSA 的安全性，适合于智能卡的实现，因而受到国际上的广泛关注。国际上制定了椭圆曲线公钥密码标准 IEEE P1363,RSA 等一些公司声称它们已开发出了符合该标准的椭圆曲线公钥密码。公钥密码的快速实现是当前公钥密码研究中的一个热点，包括算法优化和程序优化。另一个人们所关注的问题是椭圆曲线公钥密码的安全性论证问题，包括安全椭圆曲线的选择问题。

公钥密码主要用于数字签名和密钥分配。当然，数字签名和密钥分配都有自己的研究体系，形成了各自的理论框架。目前数字签名的研究内容非常丰富，除了普通签名外,还有如盲签名,代理签名,群签名,不可否认签名,公平盲签名,门限签名,具有消息恢复功能的签名等特殊签名,它们与具体应用环境密切相关。显然,数字签名的应用涉及法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准（ DSS），部分州已制定了数字签名法。法国和德国都已制定了自己的数字签名法，其他国家也正在实施之中。在密钥管理方面，国际上已有一些大的举动，比如1993年美国提出的密钥托管理论和技术、国际标准组织制定的 X.509标准（已经发展到第 3版本）以及麻省理工学院开发的 Kerboros 协议（已经发展到第 5版本）等，这些工作影响很大。密钥管理中还有一种很重要的技术就是秘密共享技术，它是一种分割秘密的技术，目的是阻止秘密过于集中。自从1979年 Shamir 提出这种思想以来，秘密共享理论和技术达到了空前的发展和应用，特别是其应用至今人们仍十分关注。目前，人们关注的是数字签名和密钥分配的具体应用问题。

认证码是一个理论性比较强的研究课题，从20世纪80年代后期起在其构造和界的估计等方面已经取得了长足的发展。目前这方面的理论相对比较成熟，很难有所突破。另外,认证码的应用非常有限,几乎停留在理论研究上,已不再是密码学中的研究热点。

哈希函数主要用于完整性校验和提高数字签名的有效性，目前已经提出了很多方案，各有千秋。美国已经制定了哈希标准一 SHA-1,与其数字签名标准匹配使

用。由于技术的原因,美国目前正准备更新其哈希标准,加之,欧洲也要制定哈希标准，这必然导致哈希函数的研究特别是实用技术的研究将成为热点。

在身份识别的研究中，最令人瞩目的识别方案有两类：一类是1984年Shamir提出的基于身份的识别方案，另一类是1986年Fiat等人提出的零知识身份识别方案。随后，人们在这两类方案的基础上又提出了一系列实用的身份识别方案，比如，Schnorr识别方案、Okamoto识别方案、Guillou-Quisquater识别方案、Feige-Fiat-Shamir识别方案等。目前人们所关注的是身份识别方案与具体应用环境的有机结合。

目前，最为人们所关注的实用密码技术是公开密钥基础设施（PKI）技术。国外的PKI应用已经开始,开发PKI的厂商也有多家。许多厂家,如Baltimore,Entrust等推出了可以应用的PKI产品,有些公司如VeriSign等已经开始提供PKI服务。许多网络应用已经在使用PKI技术以保证网络的认证、不可否认、加解密和密钥管理等。尽管如此,总的说来PKI技术仍在发展中。按照国外一些调查公司的说法，PKI系统仅仅还是在做示范工程。IDC公司的因特网安全资深分析家认为：PKI技术将成为所有应用的计算基础结构的核心部件，包括那些越出传统网络界限的应用。电子商务、电子政务活动需要的认证、不可否认等,只有PKI产品才有能力提供这些功能。

目前，国际上对非数学的密码理论与技术（包括信息隐形，量子密码，基于生物特征的识别理论与技术等)非常关注,讨论也非常活跃。信息隐藏是在网络环境下把机密信息隐藏在大量信息中不让对手发觉的一种方法，它将在未来网络中保护信息不受破坏起到重要作用。特别是图像叠加、数字水印、潜信道、隐匿协议等的理论与技术的研究已经引起人们的重视。1996年以来，国际上召开了多次有关信息隐藏的专业研讨会。基于生物特征（比如手形、指纹、语音、视网膜、虹膜、脸形、DNA等）的识别理论与技术已有所发展，形成了一些理论和技术，也形成了一些产品，这类产品往往由于成本高而未被广泛采用。1969年美国哥伦比亚大学的Wiesner创造性地提出了共轭编码的概念，遗憾的是他的这一思想当时没有被人们接受。十年后，源于共轭编码概念的量子密码理论与技术才取得了令人惊异的进步，已先后在自由空间和商用光纤中完成了单光子密钥交换协议，英国IBT实验室通过30km的光纤信道,实现了20k位每秒的密钥分配。近年来,英国、美国、日本等国的许多大学和研究机构竞相投入到量子密码的研究之中，更大的计划同时在欧洲进行。目前为止，主要有三大类量子密码实现方案：一是基于单光子量子信道中测不准原理的；二是基于量子相关信道中Bell原理的；三是基于两个非正交量子态性质

的。但有许多问题还有待于研究。比如，寻找相应的量子效应以便提出更多的量子密钥分配协议，量子加密理论的形成和完善，量子密码协议的安全性分析方法研究,量子加密算法的开发,量子密码的实用化等。总的来说,非数学的密码理论与技术还处于探索之中。

1.3 密码学在网络安全中的作用和地位

密码技术是信息安全技术中的核心技术。国家关键基础设施中不可能引进或采用别人的密码技术，只能自主开发。实用密码技术的基础是密码基础理论。没有好的密码理论不可能有好的密码技术，也不可能有先进的、自主的、创新的密码技术。因此,首先必须持之以恒地坚持和加强密码基础理论研究,与国际保持同步。另一方面，密码理论研究也是为了应用，没有应用的理论是没有价值的。我们应在现有理论和技术基础上,充分吸收国外先进经验,形成自主的、创新的密码技术,以适应国民经济的发展。

目前,在市场上比较流行,而又能够代表未来发展方向的安全产品大致有以下几类：

（1）防火墙。防火墙在某种意义上可以说是一种访问控制产品。它在内部网络与不安全的外部网络之间设置障碍，阻止外界对内部资源的非法访问，防止内部对外部的不安全访问。主要技术有:包过滤技术,应用网关技术,代理服务技术。防火墙能够较为有效地防止黑客利用不安全的服务对内部网络进行攻击，并且能够实现数据流的监控、过滤、记录和报告功能，较好地隔断内部网络与外部网络的连接。但它本身可能存在安全问题，也可能会是一个潜在的瓶颈。

（2）安全路由器。由于广域网络（WAN)连接需要专用的路由器设备,因而可通过路由器来控制网络传输。通常采用访问控制列表技术来控制网络信息流。

（3）虚拟专用网(VPN）。VPN是在公共数据网络上，通过采用数据加密技术和访问控制技术，实现两个或多个可信内部网之间的互联。VPN的构筑通常都要求采用具有加密功能的路由器或防火墙，以实现数据在公共信道上的可信传递。

（4）安全服务器。安全服务器主要针对一个局域网内部信息存储、传输的安全保密问题，其实现功能包括对局域网资源的管理和控制，对局域网内用户的管理，以及局域网中所有安全相关事件的审计和跟踪。

（5）电子签证机构（CA）和 PKI产品。CA作为通信的第三方，为各种服务提供可信任的认证服务。 CA可向用户发行电子签证证书，为用户提供成员身份验证和密钥管理等功能。PKI产品可以提供更多的功能和更好的服务，将成为所有应用的计算基础结构的核心部件。

（6）用户认证产品。由于集成电路（IC）卡技术的日益成熟和完善，IC卡被更为广泛地用于用户认证产品中，用来存储用户的个人私钥，并与其他技术如动态口令相结合，对用户身份进行有效的识别。同时，还可利用 IC卡上的个人私钥与数字签名技术结合，实现数字签名机制。随着模式识别技术的发展，诸如指纹、视网膜、脸部特征等高级的身份识别技术也将投入应用，并与数字签名等现有技术结合，必将使得对于用户身份的认证和识别更趋完善。

（7）安全管理中心。由于网上的安全产品较多，且分布在不同的位置，这就需要建立一套集中管理的机制和设备，即安全管理中心。它用来给各网络安全设备分发密钥，监控网络安全设备的运行状态，负责收集网络安全设备的审计信息等。

（8）入侵检测系统（ IDS）。入侵检测，作为传统保护机制（比如访问控制，身份识别等）的有效补充，形成了信息系统中不可或缺的反馈链。

（9）安全数据库。由于大量的信息存储在计算机数据库内，有些信息是有价值的，也是敏感的，需要保护。安全数据库可以确保数据库的完整性、可靠性、有效性、机密性、可审计性及存取控制与用户身份识别等。

（10）安全操作系统。给系统中的关键服务器提供安全运行平台，构成安全环球网（WWW）服务，安全文件传输协议（FTP）服务，安全简单邮件传送协议（SMTP）服务等，并作为各类网络安全产品的坚实底座，确保这些安全产品的自身安全。

可见，解决网络安全问题的主要途径是利用密码技术和网络访问控制技术。密码技术用于隐蔽传输信息、认证用户身份等。网络访问控制技术用于对系统进行安全保护，抵抗各种外来攻击。在上述所有主要的发展方向和产品种类上，都包含了密码技术的应用，并且是非常基础性的应用。很多的安全功能和机制的实现都建立在密码技术的基础之上，甚至可以说没有密码技术就没有真正的安全可言。但是，我们也应该看到密码技术与通信技术、计算机技术以及芯片技术的融合正日益紧密，其产品的分界线越来越模糊，彼此也越来越不能分割。在一个计算机系统中，很难简单地划分某个设备是密码设备，某个设备是通信设备。而这种融合的最终目的还是在于为用户提供可高度信任的、安全的计算机和网络信息系统。

随着芯片技术和集成化程度的不断发展与提高，密码安全设备与通信设备必

然会日趋一体化。密码算法的硬件化（特别是芯片集成）以及密码设备与通信设备的紧密结合对于提高网络的安全性，网络安全与网络系统的集成度来说都有非常重要的意义。同时，加密编程接口与系统软件也将日趋一体化，作为系统软件的一部分提供给用户。

第 2 章　信息保密技术

信息的保密性是信息安全性的一个重要属性。保密的目的是为了防止敌手截获信息系统中的机密信息。加密是实现信息的保密性的一种重要手段。所谓加密就是使用数学方法对消息实施变换，使得除了合法的接收者外，任何其他人要想恢复原先的“消息”(将原先的消息称做“明文”)或读懂变化后的“消息”(将变化后的消息称做“密文”)是非常困难的。将密文变换成明文的过程称做解密。可见，加密技术可使一些重要数据存储在一台不安全的计算机上或在一个不安全的信道上传送而不会被泄露。本章主要介绍目前国际上比较流行的各种加密技术。

2.1　密码体制的分类及基本要求

密码体制分为算法和密钥两大部分。所谓加密算法就是对明文进行加密时所采用的一组规则。类似地，所谓解密算法就是对密文进行解密时所采用的一组规则。加密和解密算法的操作通常都是在一组密钥控制下进行的，分别称为加密密钥和解密密钥。严格地说，一个密码体制通常由5部分组成：明文空间——由全体明文所组成的集合；密文空间——由全体密文所组成的集合；密钥空间——包括加密密钥空间和解密密钥空间，分别代表由全体加密密钥和解密密钥所组成的集合；由加密密钥所确定的加密规则（算法）的集合以及由解密密钥所确定的解密规则（算法）的集合。但加密规则和解密规则之间必须相匹配，即每一个加密规则都对应一个解密规则，以使得对任意的一个明文先加密后解密仍是该明文。

根据加密密钥和解密密钥是否相同或本质上等同，即从其中一个容易推出另一个，可将现有的密码体制分为两类：一类是单钥(私钥或对称)加密体制，这类体制的加密密钥和解密密钥或者相同或者本质上等同，即从其中一个容易推出另一个，其典型代表是美国的数据加密标准（DES）和高级加密标准（AES）；另一类是

双钥（公钥或非对称）加密体制，这类体制的加密密钥和解密密钥不相同，并且除设计者本人外，从其中一个很难推出另一个，这样加密密钥可以公开，而解密密钥则由用户自己秘密保存，其典型代表是RSA体制。DES的研究和以RSA为代表的公钥密码体制的研究大大地推动了密码技术的深入研究和社会应用。

根据对明文的加密方式的不同，又可将单钥加密体制分为两类：一类是序列密码,又称流密码,在这类体制中,明文按字符逐位地被加密;另一类是分组密码,又称块密码,在这类体制中,先将明文分组(每组含有多个字符),然后对明文逐组地进行加密。粗略地讲，分组密码是用一个固定的变换对一个比较大的明文数组进行操作；而序列密码是用一个时变的变换对单个明文字符进行操作。公钥密码体制大都是分组密码，一般不再按明文的加密方式对其进行分类。我们通常所说的分组密码特指私钥分组密码。序列密码主要用于高速干线加密，分组密码主要用于包交换数据加密，公钥密码主要用于密钥交换和数字签名。

一个敌手虽然不知道系统所用的密钥（假定密码算法是公开的），但可能通过从所截获的密文或其他信息推断出明文或所用的密钥，这一过程称做密码分析。为了保护信息的机密性，抵抗密码分析，一个密码体制至少应满足以下要求：

（1）从截获的密文或明—密文对,要确定密钥或任意密文的明文在计算上是不可行的。

（2）系统的保密性不依赖于对密码体制的保密，而依赖于密钥的保密。

（3）加密和解密算法适用于密钥空间中所有的元素。

（4）系统易于实现和使用方便。

2.2 密码分析的一般方法

密码分析中有一个基本的假设称为Kerckhoff假设，该假设假定密码分析者拥有所使用的算法的全部知识，密码系统的安全性完全寓于密钥之中。也就是说，密码分析者除了不知道所使用的密钥之外，他了解整个密码系统。

根据进行密码攻击的密码分析者所获得的信息类型，人们通常将密码攻击分成以下4类：

（1）唯密文攻击。密码分析者拥有一个或更多的用同一密钥加密的密文，通过对这些截获的密文进行分析得出明文或密钥。

（2）已知明文攻击。除待解的密文之外，密码分析者有一些明文以及用同一密钥加密这些明文所对应的密文。

（3）选择明文攻击。密码分析者可得到所需要的任何明文所对应的密文，这些密文与待解的密文是用同一密钥加密得来的。

（4）选择密文攻击。密码分析者可得到所需要的任何密文所对应的明文，解密这些密文所使用的密钥与解密待解的密文的密钥是一样的。

以上4种攻击对密码分析者来说，所具有的条件是不同的，进行密码分析的难易程度也是不同的。

根据Shannon的观点，研究密码体制的安全性有两种方法：一种是理论安全性（也称无条件安全性），假定密码分析者具有无限的资源如时间、设备、资金等，对这种安全性是用概率的方法来研究的，并针对某种具体攻击而言。在这种条件下安全的密码体制称为理论上安全的，或无条件安全的。另一种是实际安全性（也称计算安全性），假定密码分析者具有有限的资源如时间、设备、资金等，对这种安全性是用计算复杂性的方法来研究的。当破译一个密码体制所花的代价超过了敌手的计算能力如时间、设备、资金等时，就认为该体制实际上是安全的。实际中，设计密码体制的目标是设计实际上安全的密码体制，除了少数密码体制如一次一密体制外，大部分密码体制都是实际上安全的。

所谓一个攻击成功意味着什么呢？当密码分析者无需花过高的代价诸如时间、空间和金钱就能利用所获得的信息推导出密码系统所使用的密钥以及所对应的明文。

2.3 序列密码

序列密码主要应用于政府和军方等国家的一些要害部门。各国政府和军方都竭力控制和垄断这一技术，这就大大地阻碍了这种技术的发展和交流。这里介绍一些公开的序列密码技术。

2.3.1 序列密码分类

序列密码是一种一次将1位明文变化为1位密文的算法。现在我们来给出一种产生序列密码的最简单方法，通常称之为二元加法序列密码。由一个被称做“密钥流生成器”的器件生成密钥位流 $k_1, k_2, k_3, \cdots, k_s$，设明文位流为 $p_1, p_2, p_3, \cdots, p_s$，在加密端，将密钥位流与对应的明文位流进行异或产生密文位流 $c_1, c_2, c_3, \cdots, c_s$，即 $c_i = k_i \oplus p_i, 1 \leqslant i \leqslant s$。在解密端，将密文位流与对应的密钥位流相异或来恢复明文位流，即 $p_i = c_i \oplus k_i, 1 \leqslant i \leqslant s$。

这种体制的安全性完全取决于密钥流生成器的内部结构。参见图2.1。

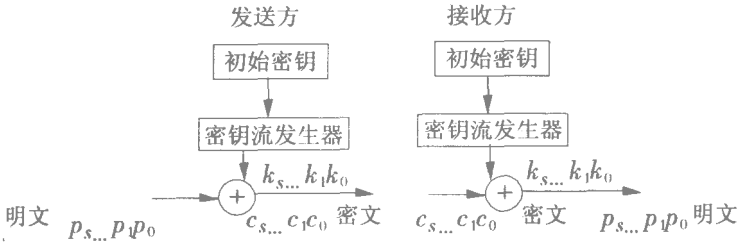

图 2.1 序列密码

根据密钥流是否依赖于明文流，可将序列密码分为两种，一种是同步序列密码，另一种是自同步序列密码。在同步序列密码中，生成的密钥流独立于明文流。这意味着若传输过程中丢失一个密文字符，发送端和接收端在进一步进行传送之前必须将它们的密钥流产生器重新同步。线性反馈移位寄存器（LFSR）、输出反馈（OFB）模式、计数模式是产生同步序列密码的几种常用的方法。同步序列密码具有不传播错误的优点，一个传播错误只影响一个字符，不会影响相继的字符。但这也是一个缺点，因为敌手修改一个字符比修改一组字符要容易。

在自同步序列密码中，生成的每个密钥流字符都从以前密文的固定 n个字符中导出。因此，在传输中若一个字符丢失或被改变，错误就向前传播 n 个字符,但在收到 n 个正确的密文字符之后密码就自行重新同步。虽然自同步序列密码当错误出现时不要求重新同步，但传输错误的传播不能忽略。自同步序列密码的观点可追溯到16世纪维吉尼亚发明的第二种自身密钥密码，这种密码是通过将密文的每个字符附加在启动密钥 k_1之后来形成密钥。当然，按今天的标准来看，这种密码是不安全的。现在产生自同步序列密码的常用方法是采用密文反馈（CFB)模式。实际上,分组密码的多种模式都能用来产生序列密码，其安全性由分组密码算法来保障。

2.3.2 序列密码的设计和度量

从二元加法序列密码我们可以看出，密钥流生成器所生成的密钥流必须“很好”，看上去应该像随机的。密钥流生成器的输出越随机，密码分析者就越难破译，但产生看上去随机的密钥流并非是一件容易的事情。由于加解密两端的密钥生成器必须产生同样的输出，所以密钥流生成器必须是确定的。许多密钥流生成器可视作自治有限状态机，它的输出将最终重复，这些密钥流生成器被称之为终归周期

的。实际上，现实中所用的密钥流生成器都是周期的。这就希望密钥流生成器的周期长，随机性好。但周期长，随机性好的生成器未必适用于作密钥流生成器， m-序列生成器就是一个例子，给定少量的（相对而言）明文-密文对，密码分析者就可能很容易地推出整个密钥流。为此，人们引入了各种衡量序列密码强度的度量指标。尤其值得一提的是线性复杂度这一指标，它是度量序列密码的安全性能的一个重要而有效的指标，之所以说它有效，是因为存在计算这一指标的快速算法——B-M综合算法。所谓一个序列的线性复杂度是指生成这个序列的最短线性反馈移位寄存器的级数。通常来说，序列的线性复杂度越高，密码强度就越高。

根据 Rueppel 的观点，目前设计序列密码的方法可分为4种 系统论方法，复杂性理论方法，信息论方法和随机化方法。下面简要介绍这4种方法。

1)系统论方法

在序列密码的系统论方法的设计中，密码设计者所设计的密钥流生成器具有可测试的密码特性，比如周期、游程分布和线性复杂度等，而不是数学理论证明。密码设计者也将研究破译这些生成器的各种密码分析技术，以便确信这些生成器能经得住这些攻击。目前，已对密钥流生成器提出了 系列的设计准则，主要有：

（1）周期准则。大的周期，这样就不易重复。

（2）线性复杂度准则。大的线性复杂度，好的线性复杂度轮廓等。

（3）统计准则。比如理想的0、1分布，游程分布等。

（4）混乱和扩散准则。使初始密钥的影响散布到生成器产生的密钥中，并使两者关系复杂化。

（5）布尔函数的非线性准则。比如相关免疫，非线性度，雪崩效应等。

系统论方法就是直接设计满足这些准则的序列密码，但不能证明其安全性。即使密钥流生成器满足所有的这些准则，它也可能是不安全的。在这种方法中，线性反馈移位寄存器是设计密钥流生成器的一个基本部件。其典型代表有滤波序列密码生成器，组合序列密码生成器和钟控序列密码生成器。

2)复杂性理论方法

在序列密码的复杂性理论方法的设计中，密码设计者试图利用复杂性理论来证明他所设计的序列密码生成器的安全性。就像设计公钥密码一样，使用已有的数学难题来设计序列密码生成器，这样做所带来的问题是：所设计的序列密码生成器速度慢，而且不实用。

3)信息论方法

在序列密码的信息论方法的设计中，假定密码分析者具有无限的计算时间和计算能力。用这种方法设计的惟一实用的序列密码生成器是一次一密密码，它能经得住敌手的攻击。一次一密密码一般适用于机密性比较高的通信。用这种方法设计的其他序列密码只具有高的理论价值，而没有实用价值。

4 随机化方法

在序列密码的随机化方法的设计中，密码设计者试图相信密码分析者有待于解决的问题具有不现实的规模，当秘密密钥很小时，设计者的目标是增加密码分析者必须使用的位数。用这种方法设计的序列密码生成器可证明几乎是安全的，但不实用。如果你乐意花上百万年来解读密文，那么要做到敌手需花上千年来破译这个密码是很容易的一件事情。

2.3.3 随机生成器

一个伪随机序列（或流）是指具有随机序列的某些随机特性的一个确定的序列（可预先确定，可重复产生），通常将产生伪随机序列的生成器称做伪随机生成器。序列密码生成器是一种伪随机生成器。在密码学中,特别是密码协议中,往往需要真随机序列或随机数。目前常用的产生办法有以下几种：使用RAND表,使用计算机时钟，使用键盘的等待时间，使用随机噪声等。我们无法证明这些技术所产生的序列是否是随机的，但这些技术可产生不重复的序列，使你的敌手不能猜测它。

2.3.4 序列密码的分析方法

现在我们来介绍一些分析序列密码的基本方法。

1)分别征服攻击方法

分别征服攻击方法是 Siegenthaler于1985年提出的一种相关分析方法，它是一种唯密文攻击方法。这种方法的基本思想是：通过分析密文序列与每个子线性反馈移位寄存器的输出序列之间的相关性来恢复每个子线性反馈移位寄存器。

2)线性攻击方法

Rueppel于1986年首次使用线性攻击方法对分组密码 DES的 *S*-盒作了分析。我国学者肖国镇和丁存生等于1987年将这种方法用于分析两类序列密码体制。他们将其称之为 BAA攻击方法，这种方法是一种已知明文攻击方法。其基本思想是：利用已知的有关密码系统的信息构造一个新的级数不太高的线性反馈移位寄存器，

以此来近似代替原密钥流生成器，从而达到对密文的近似解密。

3）线性伴随式攻击方法

线性伴随式攻击方法是由我国学者曾肯成等研制的，它是一种已知明文攻击方法。线性伴随式攻击方法的基本思想是 对给定某段具有形式为 $B=A+X$ 的序列,其中A是由一个已知的反馈多项式产生的递归序列， X 是未知的，而且 A 在 B 中的错误率小于 $1/2$，利用已有的信息设计一个极大似然纠错算法，通过有限次迭代修正从 B 中析出 A.

4 其他攻击方法

除了上述介绍的攻击方法之外，还有一些别的攻击方法，比如线性一致性攻击方法,快速相关攻击方法,线性时序逻辑逼近方法,熵漏分析方法等等。这里就不再介绍。

2.4 分组密码

一个分组密码有两个重要的参数：一个是密钥的大小，称做密钥长度；另一个是每次操作的组的大小，称做分组长度。在密钥 K控制之下的加密算法 E记为 E_k，明文消息 m对应的密文记为 $E_k(m)$。类似地,在密钥 K控制之下的解密算法 D记为 D_k,密文消息 c对应的明文记为 $D_k(c)$。显然,对所有的明文 m,都有 $D_k(E_k(m))=m$。参见图2.2。

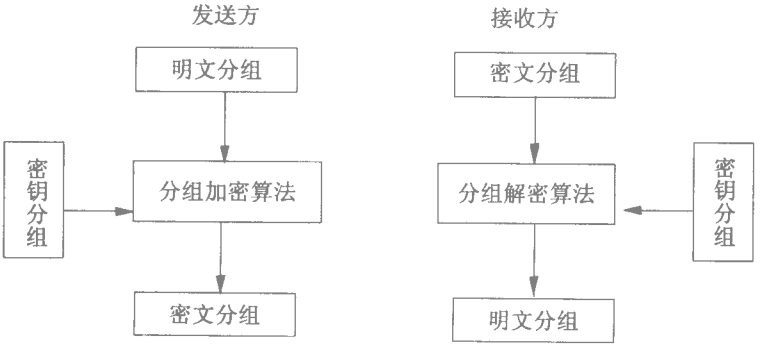

图2.2 分组密码

2.4.1 设计分组密码的一般原则

1)混淆和扩散原则

1949年,Shannon发表的论文《保密通信的信息理论》用信息论的观点对信息保密问题作了全面的阐述。Shannon以概率统计的观点对消息源、密钥源、接收和截获的消息进行数学描述和分析,用不确定性和惟一解距离度量密码体制的保密性,阐明了密码系统、完善保密性、纯密码、理论保密性和实际保密性等重要概念,将密码学的研究纳入了科学的轨道。为了使密码抵抗统计分析,Shannon建议采用混淆和扩散方法。所谓混淆就是使密文和明文的统计独立性之间的关系复杂化。所谓扩散就是将每一位明文数字的影响尽可能迅速地散布到较多个输出的密文数字中,以便隐蔽明文数字的统计特性。混淆和扩散原则是设计分组密码的基本准则。当然,它也是设计序列密码的基本准则。

2 实现原则

分组密码可以用硬件和软件来实现。基于硬件和软件的不同性质,分组密码的设计原则可根据预定的实现方法来考虑。

(1)关于硬件实现的设计原则:加密和解密可用同样的器件来实现,尽量使用规则结构。

(2)关于软件实现的设计原则:使用子块和简单的运算,使用易于软件实现的运算,诸如加法、乘法和移位等,要求子块的长度自然地适用于软件编程,诸如8、16和32等。

2.4.2 分组密码算法

1)DES算法

计算机通信网的发展对信息的安全保密的要求日益增长,未来的数据传输和存储都要求有密码保护。为了实现同一水平的安全性和兼容性,提出了数据加密标准化。为此美国商业部所属国家标准局(NBS)于1972年开始了一项计算机数据保护标准的发展规划。NBS在1973年5月13日的联邦记录(FR1973)中公布了一项公告,征求在传输和存储数据中保护计算机数据的密码算法的建议,这一举措最终导致了DES的研制和产生。DES算法是由美国IBM公司研制的一种分组密码算法,它于1975年3月17日首次被公布在联邦记录中,在作了大量的公开讨论后于1977年1月15日正式批准并作为美国联邦信息处理标准,即FIPS-46,同年7月15日开始生

效。规定每隔5年由美国国家保密局（NSA)做出评估,并重新批准它是否继续作为联邦加密标准。最近一次评估是在1994年1月。由于DES密钥仅为56位,已难以对抗密钥穷举攻击，美国已经征集和评估新的数据加密标准，该标准被称做高级加密标准（AES）,准备替代到期的DES,入选的是比利时人提出的Rijndael算法。

（1）算法概述。DES是一个使用了56位有效密钥的64位分组密码。它是一个16-轮的迭代Feistel型密码。加、解密算法一样，但加、解密时各轮所使用的子密钥的顺序刚好相反，各轮的子密钥是由56位的工作密钥经过运算产生的。

DES的轮函数f对32位的串作如下操作：首先将这32位的串扩展成48位的串。其次将这48位的串和48位的子密钥进行结合并将结合结果作为8个不同S-盒的输入。每个S-盒的输入是6位,输出是4位。然后将S-盒的32位做置换作为轮函数f的输出。

DES有56位的有效密钥，64位密钥中的第8位、第16位、…、第64位为校验位。对DES最尖锐的批评之一是DES的密钥太短。

（2）现状。目前人们仍然不知道DES中是否存在陷门。所谓陷门,通俗地讲,就是在算法的设计中设计者留了一个后门，知道某一秘密的人可进入这一后门获得使用该算法的用户的秘密密钥。有关DES的一些重要事件或事实如下：

①DES的设计准则除了极少数被公布外，其余的仍然是保密的。

②围绕S-盒人们讨论了一系列问题包括设计准则和构造等。

③Campbell和Wiener于1992年证明了“DES不成群”这个事实。

④DES至少有4个弱密钥，12个半弱密钥。

⑤1993年Wiener给出了一个详细的设计密钥搜索机的方案，他估计耗资100万美元制造一台机器，搜索一个DES密钥平均大约需花3.5小时。

⑥差分分析破译16一轮DES需要2^{47}个选择明文，破译8-轮DES需要2^{14}个选择明文。

⑦线性分析破译16-轮DES需要2^{43}个已知明文，破译8-轮DES需要2^{21}个已知明文。

⑧网络用户联网可破译DES。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，分别悬赏1 000美金、5 000美金和10 000美金用于攻破不同密钥长度的RC5密码算法，同时还悬赏10 000美金破译密钥长度为56位的DES算法。RSA发起这场挑战赛是为了调查因特网上分布式计算的能力，并测试不同密钥长度的RC5算法和密钥长度为56位的DES算法的相对