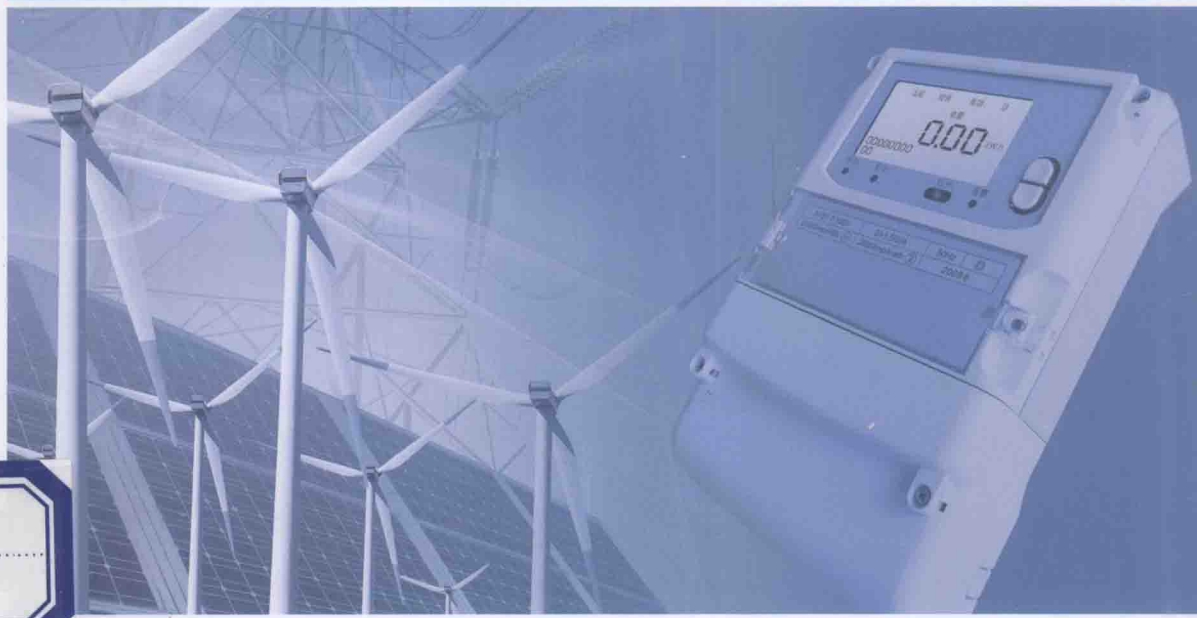
电能计量 采集及计费安全防护技术

DIANNENG JILIANG CAIJI
JI JIFEI ANQUAN FANGHU JISHU

主编 刘 鹰



中国电力出版社
CHINA ELECTRIC POWER PRESS

电能计量 采集及计费安全防护技术

DIANNENG JILIANG CAIJI
JI JIFEI ANQUAN FANGHU JISHU

主　编　刘　鹰
副主编　赵　兵　章　欣　吕英杰

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书围绕电能信息安全防护体系的建立展开，全面介绍信息安全技术、产品以及该技术在电能信息采集、计量及计费方面的典型应用。本书共分八章，主要内容包括电能计量、采集及计费安全概况，信息安全技术、信息安全产品、用电信息安全防护措施及典型应用、密钥管理系统设计、售电系统、电能计量检测系统、现场维护终端管理系统。

本书结构清晰、内容丰富、理论与应用相结合，突出介绍了我国在智能电网建设中使用的安全防护新技术，帮助读者了解电力用户用电信息采集系统的安全防护要求。

本书可作为电力营销人员了解电能计量新技术、新设备的参考用书，同时还可供相关专业技术人员参考。

图书在版编目（CIP）数据

电能计量、采集及计费安全防护技术/刘鹰主编. —北京：中国电力出版社，2014.7

ISBN 978-7-5123-5280-3

Ⅰ.①电… Ⅱ.①刘… Ⅲ.①电能计量-安全防护②用电管理-管理信息系统-安全防护 Ⅳ.①TM933.4②TM92-39

中国版本图书馆 CIP 数据核字（2013）第 285741 号

中国电力出版社出版、发行

（北京市东城区北京站西街 19 号 100005 http://www.cepp.sgcc.com.cn）

汇鑫印务有限公司印刷

各地新华书店经售

*

2014 年 7 月第一版 2014 年 7 月北京第一次印刷

710 毫米×980 毫米 16 开本 11.75 印张 202 千字

印数 0001—3000 册 定价 **36.00** 元

编 委 会

前 言

随着信息技术的发展，信息安全已成为全社会的需求，信息安全保障成为全社会关注的焦点。信息安全经历了漫长的发展过程。从某种意义上说，从人类开始信息交流，就涉及信息的安全问题。到目前为止，信息安全经历了通信保密、信息安全和信息保障三个阶段。信息安全是国家安全的重要组成部分，保护信息安全的实质是确保信息和信息系统免遭恶意或偶然的非授权破坏，即保护信息的机密性、完整性、可控性、可用性和不可否认性。

随着我国经济社会的迅速发展，人们的生活水平不断提高，用电量也在日益增加，电力在人们日常生活以及社会经济发展过程中发挥着不可替代的作用，电力信息化建设也在不断完善和进步中。电能计量系统中的电能表、采集终端等设备的计量数据是电力贸易结算的唯一依据，关系到广大用户和电力部门的经济利益，电能计量信息安全是我国电力信息化建设的一个重要方面，是保障我国电力事业稳定快速发展的关键，所以电能计量信息安全是一个至关重要的问题。

信息安全技术是电能信息系统安全保障体系的基础支撑技术。在电能信息采集、计量、计费领域应用加密解密、身份认证、授权管理与访问控制等安全防护技术，可保证电能计量计费数据、时段费率参数，支付、结算等重要信息的应用安全，保障电能供需双方的切身利益。

本书作者总结了我国十多年来建设电力用户用电信息采集系统的经验，针对系统建设及运行面临的各种风险，结合电能信息各业务系统的安全防护需求，研究提出了先进的密码技术，自主研制了专业密码设备，构建了一整套全面可靠的安全防护体系，从技术上保证了电能信息系统关键数据存储、传输和应用的安全。书中对系

统的安全防护基础设施即密钥管理系统、密钥的各个应用系统做了充分讲述。本书对指导新标准电能表、采集终端等关键设备制造厂商进行产品开发，电力系统各运行管理部门安全管理，增强业务系统安全防护能力，顺利推行国家阶梯电价调整政策具有重要的现实意义。

信息安全技术内容广泛，且发展迅速，智能电网业务应用安全需求也在不断变化，由于编者水平有限，书中难免有疏漏之处，敬请广大读者批评指正，以便进一步完善和提高。

编　者

2014 年 7 月

目 录

前言

第一章 电能计量、采集及计费安全概况 …… 1

第一节 基本概念 …… 1

第二节 电能计量信息安全威胁及攻击手段 …… 2

第三节 防护策略 …… 4

第二章 信息安全技术 …… 7

第一节 数据加密技术 …… 7

第二节 认证识别技术 …… 24

第三章 信息安全产品 …… 30

第一节 信息安全产品的分类 …… 30

第二节 安全芯片 …… 33

第三节 电能计量密码机 …… 41

第四章 用电信息安全防护措施及典型应用 …… 51

第一节 用电信息采集系统安全防护措施 …… 51

第二节 电动汽车运营计量计费系统及安全防护措施 …… 84

第五章 密钥管理系统设计 …… 103

第一节 密钥管理系统总体架构设计 …… 103

第二节 系统逻辑设计 …… 104

第三节 系统安全性设计 …… 105

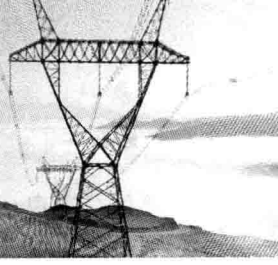
第四节 密钥管理系统的分级及建设 …… 114

第六章　售电系统 …… 134
第一节　售电系统组成 …… 134
第二节　售电系统的基本功能 …… 136
第三节　售电过程中密码设备的应用 …… 137

第七章　电能计量检测系统 …… 139
第一节　检测目标 …… 139
第二节　智能电能表的检测 …… 139
第三节　用电信息采集终端的检测 …… 148

第八章　现场维护终端管理系统 …… 152
第一节　概述 …… 152
第二节　技术方案 …… 153
第三节　现场维护终端功能 …… 157
第四节　工作流程 …… 160

参考文献 …… 171



第一章

电能计量、采集及计费安全概况

本章首先阐述了信息安全及电能计量信息安全的基本概念，然后介绍电能计量信息安全所面临的安全威胁及攻击手段，最后针对上述安全威胁分析了电能计量信息安全的防护策略。

第一节 基 本 概 念

国际标准化组织（ISO）对信息安全的定义是："信息安全是在技术上和管理上为数据处理系统建立的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露"。

电能计量信息安全是指电能计量信息在传输和应用过程中的安全，是保证用电信息采集系统中主站、采集终端和智能电能表等电能计量设备信息的保密性、完整性、可用性以及可控性。电能计量信息安全主要体现在从电能计量信息安全保护到信息安全保障的发展，用电信息采集系统的整体安全，以及在用电信息采集系统中将安全技术与密码技术结合等方面。电能计量信息安全是用电信息采集系统安全、电能计量信息自身安全和电能计量信息传递方式安全的总和，目的是保护电能计量信息和用电信息采集系统免遭偶发的或有意的非授权泄露、修改、破坏或丧失处理信息能力，实质是保护电能计量信息的安全性，即可靠性、机密性、完整性、可控性、有效性和不可否认性。

（1）可靠性，是指用电信息采集系统能够在规定的条件和时间内完成规定功能的特性。

（2）机密性，是指用电信息采集系统防止电能计量信息非法泄露的特性。

（3）完整性，是指电能计量信息在存储和传输过程中未经授权不能改变的特性。

（4）可控性，是指用电信息采集系统对电能计量信息内容和传输方式具有控制能力的特性。

（5）有效性，是指电能计量信息能够被授权实体访问并按要求使用，用电

信息采集系统能以人们所接受的质量水平持续运行，为人们提供有效的信息服务的特性。

（6）不可否认性，是指通信双方不能抵赖或否认已完成的操作和承诺，通常通过数字证书签名机制实现通信双方的不可否认性。

随着用电信息采集系统内信息集成度的进一步提高，实现对用电信息采集系统网络通信质量的实时监控和维护，并对网络内传输的信息进行保护，防止来自网内外的恶意攻击和窃取，及时响应网络故障并快速恢复网络设备等技术手段已经成为可能。除此之外，网络防火墙技术、数据加密技术、权限管理和存取控制技术、冗余和备份技术等信息安全防护技术的发展，也为电能计量信息安全防护策略带来了新的发展思路。

第二节　电能计量信息安全威胁及攻击手段

一、安全威胁

电能计量信息安全的基本目标就是实现电能计量信息的机密性、完整性、可用性和用电信息采集系统资源的合法使用。对电能计量信息安全的威胁就是对这些基本安全目标的威胁。电能计量信息安全威胁的主要来源包括内部人员（包括用电信息采集系统的使用者、管理者和决策者、用电信息采集系统的维护者和开发者等）、特殊身份人员（比如稽查人员、审计人员等具有特殊身份的人）、外部黑客、竞争对手等。任何威胁都有可能使系统受到非法入侵者的攻击，传输中的敏感数据有可能泄露或被修改，传输的信息可能被他人窃听或篡改等。信息安全威胁的主要表现如下：

（1）信息泄露。电能计量信息被无意或有意泄露给某个非授权的人或实体。如利用搭线窃听或电磁泄漏等方式截获主站与智能电能表或采集终端传递的信息，非法进入用电信息采集系统复制敏感信息，通过分析信息流通频度、信息长度、信息流向和信息流量分析出有用的信息而造成信息的泄露和丢失。

（2）完整性被破坏。以非法手段对电能计量数据进行修改、插入、删除或重发某些重要信息，以达到攻击者预期的响应效果，恶意修改，添加数据，以干扰用户的正常使用。对电能计量系统的安全威胁主要表现在对电能表或采集终端等设备进行恶意攻击，使电能表或采集终端等设备不能正常工作或修改设备中的参数，破坏计量准确性等。

（3）拒绝服务攻击。攻击者利用协议、操作系统或网络设备的网络协议栈存在的缺陷，通过对主站系统或售电系统发送一些非法数据包使系统响应减慢

甚至瘫痪，从而导致用户对主站系统或售电系统的合法访问不畅或访问被无条件地阻止。

（4）非法使用。没有预先经过同意，就使用用电信息采集系统网络或计算机资源，如有意避开系统访问控制机制，对设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等几种形式。

（5）逻辑炸弹、蠕虫、恶意代码、木马等病毒的威胁。利用用电信息采集系统存在的漏洞，植入逻辑炸弹、蠕虫、恶意代码、木马等病毒，破坏用电信息采集系统的正常工作。

（6）备份数据和存储媒体损坏或丢失。磁盘阵列、磁带、磁带库、光盘塔、光盘库、加密U盘等专用硬件，加上适当的备份软件组成数据备份与恢复系统，然而有了完善的数据备份与恢复系统，仍可能存在备份数据和备份媒体损坏或丢失的危险。如存储媒介中的数据读不出来，存储媒介丢失、损坏等。

（7）管理漏洞带来的信息安全威胁。信息安全问题的解决，三分靠技术，七分靠管理，信息安全威胁60%来自网络内部。人为的违规、无意失误、渎职等行为是造成信息不安全的重要原因，因此，加强信息内网管理及员工的安全意识是信息安全十分重要的一环。

二、攻击手段

威胁电能计量信息安全的主要方法有篡改、截获/侦听、拒绝服务攻击、非授权访问/非法使用、假冒与伪造、重放攻击等。攻击者可以通过改变信息流的时序、次序、内容、形式、流向，删除全部或部分信息，在消息中插入无意义信息或有害信息等方法来破坏信息的机密性和完整性。攻击者通过使用电磁辐射探测设备或搭线等方式截获/侦听信息。攻击者可使主站或售电系统响应减慢甚至瘫痪，阻止合法用户获得服务。攻击者可假冒管理员调阅机密内容或发布命令；假冒合法主站或用户，进行非法连接盗取信息资源；假冒网络控制程序，套取和修改使用权限、口令、密钥等信息，越权使用用电信息采集系统中的设备和资源。攻击者可对截获的某次合法数据进行复制，而后出于非法的目的重新发送。通信的某一方出于某种目的，事后否认曾发送或接收某些信息。信息安全典型攻击及相互关系如图1-1所示。

从信息安全属性的角度看，每一种攻击都对应于某些信息安全的外部特征。其中，截获/侦听攻击主要针对信息的完整性；中断攻击主要针对信息的可用性；伪造与假冒攻击主要针对信息的不可否认性/可靠性；非授权访问/非

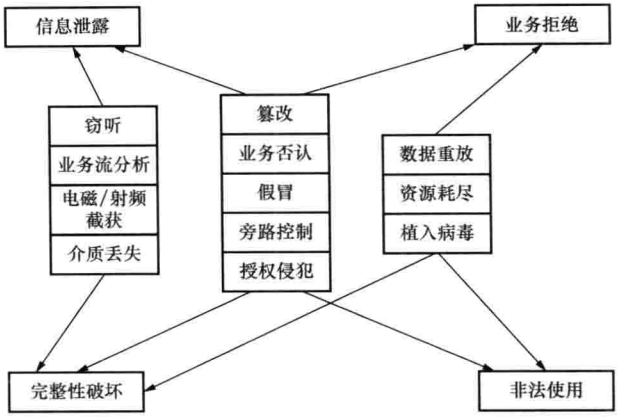


图 1-1　典型攻击及相互关系

法使用主要针对信息的可控性。

第三节　防　护　策　略

针对用电信息系统可能面临的各种攻击，构建电能计量信息安全体系，采取的安全防护策略体现在物理安全、链路安全、网络安全、系统安全、数据安全等五个方面。

一、数据的物理安全

数据的物理安全包括介质安全和设备安全。介质安全是指数据的传输及存储介质的防盗、防毁及防信息泄露等。在用电信息采集系统中，数据传输和存储介质主要包括 USB KEY、CPU 卡和密码机等。为保证介质的使用安全和存放安全，介质的存放和管理应有相应的措施和制度，例如，系统中的重要数据，或对系统运行和应用起关键作用的数据，应采用加密等方法进行保护；存放重要数据和关键数据的各类介质，应采取有效措施，如异地存放或建立介质库等，防止被盗、被毁和变质；应该销毁和删除的重要数据，应由专人负责集中销毁，防止被非法复制。

设备安全指用电信息采集系统中的计算机、智能电能表、采集终端等设备的防毁、防盗、防电磁泄漏发射、抗电磁干扰及电源保护等。我们应该保护系统中的相关设施免受自然灾害、人为破坏和搭线攻击，采取的防范措施有：

（1）采用符合规范的机房或计算机场地。

（2）采用光电接口和光缆，减少线路被窃取概率。

（3）主要网络设备要置于专门的屏蔽室中，防止线路被窃取。

二、链路安全

为保障电能计量信息资源不被非法访问和使用，可采用身份认证技术和会话密钥协商技术，即在智能电能表或采集终端与主站系统之间建立安全通信链路。身份认证是整个电能计量信息安全体系的基础，它能确认用户的权限和责任。身份认证是在信息通信网络中确认操作者身份的过程，分为智能电能表或采集终端与主站间的身份认证以及主站与主站之间的身份认证。最常用的认证方式就是“用户＋密码”，这种认证方法存在认证过程不加密，密码容易被破解和监听的缺陷。因此，又产生了多种认证方法，如智能卡（IC 卡）认证、短信密码验证、动态口令牌验证、USB KEY 验证、生物识别技术（如指纹识别、语音识别）等。会话密钥协商是建立安全通信链路的有效方法，通过安全通信协议为用电信息采集系统网络应用层提供一条全透明的网络安全传输通道，它一般分为握手和数据传输两个阶段。在握手阶段，智能电能表或采集终端与主站相互进行认证，并确立用于保护数据传输的加密密钥，一般采用公钥密码体制实现。握手完成后，数据被分成经过保护的记录进行传输。

三、网络安全

在用电信息采集系统中，采集终端和主站之间需要利用 Intenert 网络进行通信，采集终端与电能表之间一般采用电力载波或小无线进行通信，需要采用一些安全保障技术减少用电信息采集系统面临的来自公共网络的安全威胁。

利用 VPN 技术建立采集终端和主站之间进行通信的加密隧道，可保障计量信息在公共网络上传输的安全性。同时利用防火墙，限制非授权用户对内部网络的访问和控制内部网络用户的外部访问行为。为了降低网络攻击对防火墙的压力，通过过滤进入信息内网的数据包或使用网络隔离技术，防御利用操作系统或协议漏洞进行的攻击。

在恶意代码、蠕虫、木马等病毒威胁日益严重的情况下，需要在用电信息采集系统关键的节点部署漏洞扫描系统、防病毒软件和入侵检测系统。避免攻击者利用系统漏洞植入攻击，使用入侵检测系统监控网络数据流，及时发现来自外部的攻击。

除了应用必要的技术手段保障电能计量信息安全外，内网网络的运维和管理同样重要。防止用电信息采集系统内部信息外泄最重要的手段就是布置内网监控系统。内网监控系统必须具备以下功能：一是采取有效措施防止内部网络信息泄露；二是对系统用户账号进行管理，能够将用户登录系统时的信息记录下来；三是能够监视和控制整个系统及内部人员的使用情况；四是对系统资源

安全管理，能够控制和限制某些特殊程序的运行。

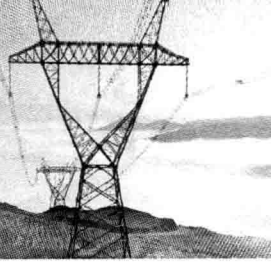
四、系统安全

信息系统可通过备份的方式确保其安全。电能计量信息系统备份是指对电能计量系统核心设备和数据信息进行备份，以便在系统出现意外时能快速、全面地恢复。核心设备的备份主要包括核心交换机、核心路由器、主站服务器、售电服务器等的备份。数据信息备份包括对设备的配置信息、服务器数据等的备份。电能计量信息系统数据备份是信息系统日常维护工作的重要环节之一，做好相关备份工作，才能在系统出现故障时及时、迅速、有效地恢复系统，确保系统的正常运行操作系统是连接硬件与其他应用软件之间的桥梁，在网络环境下，网络的安全可信性依赖于各主机系统的安全可信性，没有操作系统的安全性，就不会有主机系统和网络系统的安全性。

五、数据安全

数据加密技术是保障电能计量信息安全的最基本、最核心的技术。数据加密就是通过一种方式使信息变得混乱，从而使未被授权的人看不懂。数据加密过程由形形色色的加密算法来具体实现，它可以以较小的代价获得较大的安全保障。

目前采用的数据加密方法可分为软加密、硬加密和网络加密三种。软加密比较常见的有密码表加密、软件子校验方式、许可证管理方式等。硬加密主要有加密锁和加密卡等。网络加密不同于软件加密方法和硬件加密方法，而由基于网络的其他计算机或密码设备来完成加解密或验证工作，网络设备和客户端之间通过安全通道进行通信。在用电信息采集系统中，主站与采集终端之间以及主站与智能电能表之间进行关键数据传输时，主要采用网络数据加密方式，加密算法主要为国密 SM1 对称密码算法，加密设备为电能计量密码机。



第二章

信息安全技术

信息安全技术是研究对信息进行保密处理，以防止攻击者对信息进行窃取、破坏其机密性的技术。一般来说，信息安全技术主要分为基于信息密码学的数据加密技术和认证识别技术。数据加密技术是目前应用最广泛的信息安全技术，是实现信息安全的核心技术，是保护数据最重要的技术之一。通过加密变换，将可读的文件变换成不可理解的乱码，使未被授权者看不懂，从而起到保护信息和数据的作用。它分为对称数据加密技术和非对称数据加密技术，直接支持机密性、完整性和抗否认性等功能。认证识别技术也是信息安全技术的重要组成部分之一，它对于开放环境中的各种信息系统的安全性有重要作用，它支持识别用户身份的合法性和消息的真实性、完整性及正确性等功能。

通用信息安全技术同样适用于用电信息采集系统，因此，本章主要介绍信息安全的一般概念和原理，即首先在数据加密模型的基础上阐述了对称加密技术和非对称加密技术的一般概念、工作原理、主要算法及分类，然后介绍了认证识别系统的一般模型，数字证书和数字签名的基本概念及实现方法，接着介绍哈希函数基本概念和消息认证含义，最后介绍身份识别的常用技术。

第一节　数据加密技术

数据加密技术是当今信息安全的主流技术，同时也是信息安全的核心技术。它主要用来保护关键信息的安全传输与存储。信息发送者可以使用加密密钥对关键数据进行加密，将所得到的密文传送给接收方，信息接收者则使用解密密钥对传输的密文数据解密后得到关键数据原文。下面介绍数据加密技术中常用的基本术语。

（1）消息（明文）指未被加密的数据信息，它是加密输入的原始信息，通常用 m 或 p 表示。所有明文的集合称为明文空间，通常用 M 或 P 来表示。

（2）密文是明文经过加密变换后的数据，即消息经过加密运算处理后的数据，通常用 c 表示。所有密文的集合称为密文空间，通常用 C 来表示。

（3）密钥是控制密码变换操作的关键数据或参数，通常用 k 表示，它由加密密钥 k_e 和解密密钥 k_d 组成。所有密钥的集合称为密钥空间，通常用 K 来表示。

（4）加密算法是将明文变换成密文的函数，相应的变换过程称为加密过程，即编码的过程，通常用 E 表示，即 $c=E_k(m)$。信息加密的基本原理如图 2-1 所示。

（5）解密算法是将密文恢复为明文的函数，相应的变换过程称为解密过程，即解码的过程，通常用 D 表示，即 $m=D_k(c)$，它与加密过程互逆。信息解密的基本原理如图 2-2 所示。

图 2-1　信息加密基本原理

图 2-2　信息解密基本原理

在数据加密技术中，将上述明文、密文、密钥、加密算法和解密算法五部分进行组合，就构成了密码信息系统典型模型，如图 2-3 所示。

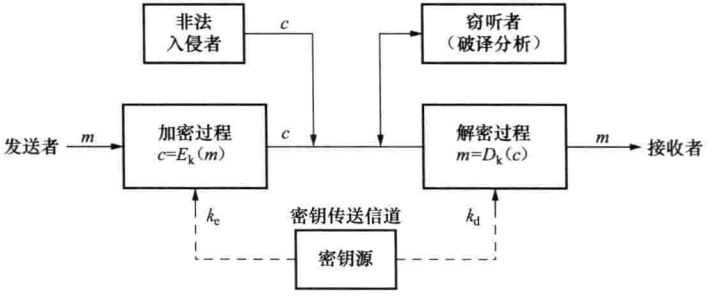


图 2-3　密码通信系统模型

（6）消息鉴别。用密钥和公开函数产生一个固定长度的值作为认证标识，消息的接收者用这个标识确认消息的完整性和真实性。

（7）完整性。消息的接收者应该能够验证消息在传输过程中是否被修改过，入侵者不可能用假消息代替合法的消息。

（8）抗抵赖。消息发送者不能否认他发送过的消息。

（9）密码体制。完成加密和解密功能的密码方案，它分为对称密码体制和非对称密码体制，包括密码算法以及所有可能的明文、密文和密钥。

数据加密技术应用领域不断拓展，它不仅服务于信息的加密和解密，为信

息提供机密性和完整性保护，还用于访问控制、身份认证、数字证书和数字签名等多种安全技术领域，为通信业务信息提供机密性保护。在数据加解密系统中，密钥 k_e 和密钥 k_d 是比被保护的信息数据总量短得多的随机数或伪随机数，根据 k_e 和 k_d 的关系，数据加密技术可分为对称加密技术和非对称加密技术。下面将分别介绍这两种数据加密技术。

一、对称加密技术

对称加密技术是一种采用对称加密算法，原发方的变换和接收方的变换均采用同一秘密密钥或两个秘密密钥可相互推导的加密技术，其加、解密过程如图 2-4 所示。常用的对称加、解密算法在计算上是简单的，如 DES 算法、AES 算法、SM1 算法、SM4 算法和 RC4 算法等。

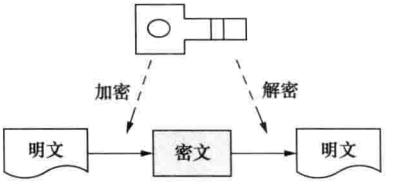


图 2-4　对称密钥加解密过程

在对称加密体制中，收发双方均使用相同的密钥，整个加密体制的安全性完全取决于密钥，因此，保证密钥的安全至关重要，并且信息的发送方和接收方都必须是相互信任的，任何一方将密钥泄露出去，都使得另一方对密钥的保密完全失去意义。在每次通信前，信息接收方使用的密钥必须通过保密信道传递到信息发出方。因此，对称加密体制密钥的产生、传输、存储是一个异常复杂的问题，特别是在公共的通信网络中，用户数目多，每对用户之间分配的密钥不同，多个用户通信时密钥分发异常复杂等问题日益凸显，这也使得密钥管理的任务变得更复杂。此外，在对称加密密码体制中，由于收发双方使用相同的密钥，无法实现数据签名和不可否认等功能。

根据一次处理信息数据量的大小，对称密码算法又分为序列密码算法和分组密码算法两类，其中，序列密码算法也称为流密码算法，它是一次仅处理明文中的一个比特或几个比特的一种加密算法；分组密码算法是一次处理明文的一组比特的数据加密算法。根据两者每次处理的数据量不同，序列密码算法和分组密码算法一般采用不同的分析方法和设计思路。

由于序列密码算法每次只处理一个比特的数据，便于硬件实现，而不便于软件实现，因此，它一般应用于专用密码机。

随着分组密码算法的不断发展，一些分组密码算法的安全强度已经超越了序列密码算法的安全强度。分组密码算法具有简捷、快速等特点，容易标准化，并可以内嵌到软件模块中，因此，分组密码算法广泛应用于用电信息采集系统的各类软硬件中。分组密码算法是一种用小数据量的秘密数据保护大数据