国家经济信息系统设计与应用

标准化规范

（七）

信息安全与保密系统建设必备文件

国家信息中心　　编著

航空工业出版社

国家经济信息系统设计与应用

标准化规范

(七)

信息安全与保密系统建设必备文件

国家信息中心 编著

航空工业出版社

1993

（京）新登字161号

国家经济信息系统设计与应用
标 准 化 规 范
（七）
信息安全与保密·系统建设必备文件
国家信息中心 编著

航空工业出版社出版发行
（北京市安定门外小关东里14号）
—邮政编码：100029—
全国各地新华书店经售
北京通县向阳印刷厂印刷

1993年6月第1版 1993月6月第1次印刷
开本：787×1092 1/16 印张： 4
印数：1—3000 字数： 94千字
ISBN 7-80046-542-X/Z·093
定价：4.00元

序

早在1986年初国家经济信息系统建设初期，国家信息中心就注意到及早制定出符合我国信息系统实际情况的一整套标准与规范的重要意义，十分重视系统标准规范的制定工作。为此，国家信息中心和原国家标准局共同组织编制了《国家经济信息系统设计与应用标准化规范》(下称红皮书)并于1986年7月由国家计委、原国家标准局联合批准，在系统内试行，成为我国经济信息系统建设的一个重要的指导性文件。

3年来，红皮书在指导我国各级信息系统建设中发挥了十分重要的作用，成为各级信息中心及其他信息机构从事系统设计与应用开发工作必不可少的依据。现已发行近1万册，需求还在增加。

与此同时，我们广泛征求了系统内外各级用户的意见，得到了大家的热情支持，收集到各使用单位的许多宝贵意见，感到书中确有一些不足之处；同时这几年系统建设和标准化理论发展很快，红皮书的内容也需要进一步修改完善。为此，国家信息中心在1988年初决定对红皮书进行重新修订。经过了近四年的努力，现在终于定稿出版。

这次公开发行的规范文本，是国家信息中心根据几年来信息系统建设实践中总结的经验，组织了国内著名的专家学者在该书原有基础上进行修改、充实、细化而成的。修订后的规范文本覆盖了信息系统建设可行性研究、系统设计、应用开发、使用维护的全过程，具有技术先进、实用性强等特点，是各级信息系统建设的必备文件。

新的规范文本由八个分册组成。它们是：《概述》、《信息分类编码·通用文件格式》、《信息记录格式》、《数据库开发工程实施细则》、《软件工程规范》、《数据通信、计算机网络及系统互连》、《中文信息处理》、《信息安全与保密·系统建设必备文件》。

国家经济信息系统的建设是一项庞大而复杂的系统工程，标准化工作在这一工程的建设中占有十分重要的地位。这次红皮书的修订是对这一面向未来的课题的又一次积极尝试，同时也是系统标准化建设的一个新的开端。目前国内信息系统的标准化工作仍然处在初创阶段，要做的事还很多。但只要我们积极进取，勇于开拓，就能够引导这一工作向预期的目标发展。

编　者

1990年3月

出 版 说 明

《国家经济信息系统设计与应用标准化规范》经国家计划委员会和原国家标准局批准作为指导国家信息系统建设与开发的纲领性文件，并于1986年7月正式颁布试行。3年来本规范在指导全国范围内的国家信息系统建设，保证各种信息系统在设计与应用开发中，按系统工程规律健康开发等方面发挥了巨大的作用。

此次公开发行的规范文本是国家信息中心根据几年来国家信息系统各级设计与开发部门对《规范》提出的意见和要求，组织国内著名专家、学者，经过一年多的努力在原有基础上进行修改、充实、细化而成的。修改后的《规范》覆盖了信息系统设计、开发、应用的全过程，具有技术上的先进性，使用上的实用性和权威性等突出特点，将成为各级政府经济信息系统建设的必备文件，对其他信息系统的建设开发、使用和管理也具有一定的指导意义。

全《规范》由8个分册组成。本次出版发行包括《概述》、《信息分类编码·通用文件格式》、《信息记录格式》、《数据库开发工程实施细则》、《软件工程规范》、《数据通信、计算机网络及系统互连》、《中文信息处理》、《信息安全与保密·系统建设必备文件》。

本分册为第八分册。主要叙述了国家经济信息系统的安全与保密，包括数据传输的安全与保密、数据存储的安全与保密、存取控制、数据完整性鉴别、数字签名、密钥、系统处理安全与物理安全、安全保密管理；系统建设的必备文件包括：必备文件种类及内容等。

本分册由国家信息中心姜开富同志编写。

在全套书完成之际，我们谨向航空工业出版社为该书的出版做出辛勤劳动的冯士斌、杨步云等同志表示谢意。

目　录

第一部分　信息系统的安全与保密

1.　概述……（1）
2.　数据传输的安全与保密……（4）
2.1　数据传输的内容……（4）
2.2　保密目标……（4）
2.3　传输数据加密方法……（5）
2.4　系统的保密等级……（6）
2.5　系统保密设备的要求……（6）
2.6　加密算法……（6）
3.　数据存贮的安全保密……（15）
3.1　文件加密保护……（15）
3.2　数据库加密保护……（18）
4.　存取控制……（18）
4.1　存取资格检查……（19）
4.2　存取保护……（19）
4.3　数据库的存取保护……（20）
4.4　防止存取信息破坏……（21）
5.　数据完整性鉴别……（21）
5.1　口令鉴别……（21）
5.2　密钥鉴别……（21）
5.3　通信双方身份鉴别……（21）
5.4　报文鉴别……（22）
6.　数字鉴名……（22）
6.1　非保密的数字鉴名……（22）
6.2　保密的数字鉴名……（23）
7.　密钥……（23）
7.1　范围……（23）
7.2　密钥的产生……（24）
7.3　密钥的存贮……（24）
7.4　密钥的分配……（24）
7.5　密钥的注入……（25）
7.6　密钥的销毁……（26）
8.　系统处理安全……（26）
8.1　系统恢复处理……（26）

8.2 向前恢复……（26）
8.3 退回恢复……（27）
8.4 向回恢复……（27）
8.5 系统超负荷处理……（27）
9. 系统的物理安全……（28）
9.1 概述……（28）
9.2 计算机系统设备的场地环境……（28）
9.3 计算机系统设备场地技术要求……（28）
9.4 电磁干扰和辐射的防护……（29）
9.5 记录媒体保护……（30）
9.6 计算机网络安全……（31）
9.7 人身和设备安全……（32）
9.8 灾难性事件应急计划……（32）
9.9 计算机病毒的预防和清除……（33）
9.10 安全责任与监督……（33）
10. 安全与保密的管理……（34）
10.1 安全机构……（34）
10.2 安全机构的任务……（34）
10.3 安全等级……（34）
10.4 密钥管理……（34）
10.5 环境管理……（35）
10.6 机房门卫与出入管理……（35）
10.7 设备管理……（36）
10.8 技术文档资料管理……（36）
10.9 操作管理……（36）
10.10安全规章制度……（36）
参考资料……（36）

第二部分 系统建设必备文件

1. 系统建设必备文件的含义……（38）
2. 系统建设阶段划分及必备文件种类……（38）
2.1 系统建设阶段划分……（38）
2.2 系统建设必备文件种类……（41）
3. 系统建设必备文件内容……（41）
3.1 项目建议书……（41）
3.2 可行性研究报告……（42）
3.3 系统设计任务书……（43）
3.4 系统功能说明书……（44）

3.5 系统技术设计说明书……（45）
3.6 实施进度报告……（48）
3.7 系统测试报告……（49）
3.8 新旧系统转轨报告……（50）
3.9 系统评价验收报告……（51）
3.10 系统建设总结报告……（51）
参考资料……（52）

第一部分　信息系统的安全与保密

1．概述

国家经济信息系统*是对经济和有关社会信息进行收集、加工、存贮、分析和交换的人—机结合的系统，也是国家级的大型计算机通信网。它将迅速、准确地为中央和地方各级领导机关和经济管理部门提供各种经济信息服务和辅助决策手段，因此会有大量涉及国家秘密的数据在各类计算机上处理，在磁盘和磁带等媒体上存贮，在有线和无线等各种通信信道上传输。如果不采取有效措施，这些秘密数据的安全，以至整个系统的安全将会受到损害，给国家造成不可弥补的巨大损失和危害。

危及系统安全的因素，有硬件或软件的工作不可靠、用户无意的误操作或各种自然灾害；更重要的是敌对者故意地采取种种手段窃取秘密或破坏系统的正常运行。对于前者，一方面要求各种硬件和软件符合规定的可靠性要求，一方面系统也要设计成能防止因误动作或自然灾害而可能产生的对系统安全性的危害；对于后者，则要针对敌对者的可能行动，采取相应的措施。

敌对者可能采用打进来、拉出去的办法，利用系统用户、操作员、管理人员盗窃秘密数据或破坏系统资源，也可利用制度不健全或管理不严盗窃存有秘密数据的媒体，还可能直接用暴力抢劫或破坏。敌对者还会用各种技术手段对系统安全进行攻击，攻击的方法有被动攻击和主动攻击。被动攻击只是窃取秘密数据；主动攻击是采用修改、删除、添加等手段来破坏数据的完整性。无论是处理过程中的数据，存贮在媒体上的数据，还是传输中的数据都可能受到攻击。例如：由于一切电子设备在工作过程中都有电磁辐射，即使用不很先进的设备，在一二百米处就可将这些数据，包括在终端屏幕上显示的数据接收下来；敌对者冒充合法用户，非法存取或修改系统内的秘密数据；盗窃或复制在传送中和存放着记录秘密数据的媒体；对信道上传输的数据用搭线方法监听截收秘密数据或用相应的无线设备接收；也可插入一个假终端，篡改截收后的数据再发送出去。在具有支付现金能力的自动出纳机系统中，敌对者可结合使用这两种攻击方法，先通过搭线窃听获取某合法用户的识别符和通行字等数据信息，然后冒充该用户，插入伪造的数据，以非法手段获取现金。据有关资料报导，近几年来，美国等西方国家，利用计算机进行犯罪而窃走的资金高达数十亿美元。

为了保护系统的安全，要在法律、行政、技术三方面采取综合措施，三者不能偏废，不能互相代替，而是互为补充：要制定相应法律，依法惩处罪犯；要加强管理，严格组织纪律，教育各类人员忠于职守；要在技术上采用物理保护和数据加密两种方法。系统的物理保护包括诸如对计算机及通信设备采取必要的屏蔽；在系统的重要部位应划定安全区域，设立门卫，严格出入手续，直至配备专职安全人员；将存有秘密数据的媒体存放在能防盗、防火、防水、防外界电磁干扰的专用房间并加锁；制定系统遭到各种不测事件后的应急计划和措施

---

*本书所使用的"系统"一词除特别说明外，其含义是指国家经济信息系统或其子系统。

等。数据加密保护提供的第一种服务是数据传输过程中的加密保护。系统密钥分配过程也属于这一范围。同时，对存贮的数据施以加密保护也是数据存贮保护的一种行之有效的方法。加密的方法是保护秘密数据的最后一道防线，是保护传输数据秘密的唯一实用的方法，在物理安全措施不足的地方，也是保护存贮数据秘密的最有效、最经济的方法。

对秘密数据进行加密是指通过密码算法，在密钥的控制下，将明文数据变换成不可懂的密文数据，在相应的密钥控制下，再将密文数据还原成原来的明文数据。密码算法是一组事先确定的运算法则，它受一个可变的密钥变量的控制。密码算法的设计，必须遵循"秘密全寓于密钥"的原则，即假定敌对者完全掌握密码算法细节，只是不知道当时所用的密钥。这是条公认的比较保险的原则。对于国家经济信息系统这样大型的信息系统，也应遵循这一原则。当然，敌对者若不知道算法，解读密文数据会极其困难，但从算法的设计开始，经做成硬件或软件，安装在分布面很广的终端和计算机系统上，供使用到最后被替换，这是一个相当长的时间，几年，十几年甚至更长，所有法律的、行政的、物理的保护措施都难以担保算法不落入敌手，因此密码算法应当设计成除了逐个密钥的穷举试验外，就不能将密文数据还原成明文数据。这样，敌对者即使窃到密文数据，由于没有密钥，也很难获取明文数据。

一个密码算法是否满足上述要求，要经过有关审查部门的严格的分析验证。现在的情况是，可变密钥的数量可以很大，达到10^{40}、10^{60}甚至还高得多，想穷举这样的密钥量来破译分析，在当前可以预见的今后若干年内技术的进步，即使不是不可能，至少也是极其困难的。但是事实上，不少算法存在着各种各样的弱点，不需要采用穷举所有密钥的方法就能达到破译。能否发现这些弱点，采用什么样的破译方法，则要看破译分析者的水平。一个明智的密码算法设计者应当随时将自己置于破译分析者的地位，挑剔自己设计的算法，自觉地避免算法出现弱点，因此不懂得破译分析的密码算法设计者设计出的算法往往带有不同程度的弱点，即使有破译分析知识和经验的算法设计者，也应小心谨慎。一个保密性能不好的算法，常常会给人一种虚假的安全感，这比不使用加密还要危险，因为后者还可能提醒人们注意用其他方法来保护秘密数据的安全。因此不经有关主管部门审定的密码算法是不能使用的。

有了好的密码算法，秘密数据的安全就依赖于密钥的安全了。密钥的安全取决于包括密钥的产生、存贮、分配、注入、使用、更换和销毁等所有环节，它们组成了密钥管理的全过程。一个大型的计算机通信网的密钥管理是十分复杂的问题，任何一个环节保护不严，都可能造成密钥的失密。因此，除了系统应配备专门人员负责掌管记录密钥的各种媒体和注入器外，密钥一旦由注入器注入密码设备后，任何人都不能将密钥从密码设备内读出来；密钥还要定期更换；不允许在两对密码设备内使用相同的密钥；由于系统内有很多密码设备，每个密码设备要存放其他所有密码设备的密钥，在具体实现时是难以解决的，因此必须在系统内通过通信网动态地自动分配密钥，目前较为成熟的是采用人工和自动分配相结合的体制。每个密码设备的主密钥采用人工分配，由专职人员更换，确定一定的使用期限，而每次通信则要由密钥分配中心给有关通信双方配一个随机的会话密钥，由于这个密钥要在通信线路上传输，因此必须用通信双方的主密钥分别对这个会话密钥加密后再传送。加密传输数据的会话密钥使用期限很短，一次通信结束就应清除，加密存贮数据的密钥使用期限较长，需和这些数据的保存期相适应。因此除了对这类密钥也要用另一个密钥加密保护外，还要采用物理保护的方法，切实防止密钥的丢失，以免加了密的文件变成无法读懂的死文件。

为了解决复杂的密钥分配问题，1976年，国际上提出了公开密钥的思想。这种思想一经提出，便受到广泛的重视，国内外陆续提出了若干种实现公开密钥的密码算法。这类密码算法和传统的密码算法的主要区别在于将原来加密、解密使用同一个密钥变成两个不同的密钥，加密密钥公开，只保密解密密钥。尽管公开密钥算法目前尚未达到实用阶段，从长远的观点看，它是有发展前途的，它不仅可用于分配密钥，也可用于各种鉴别技术，特别是获得数字签名的比较理想的密码技术，和对待传统的密码算法一样，任何公开密钥密码算法也必须经有关部门审定后方可在此系统上运用。

为了抗住敌对者的主动攻击，可通过对数据进行分组链接式的加密来检测出敌对者对数据的任何窜改。

还需指出，系统中各种设备和人身的安全问题也应十分重视，这不仅是为了保护国家财产不受损失，而且也是整个系统能正常运行，发挥其最大效益的前提。

对系统的一切安全措施，都需要很大的投资，投资的大小应和保护对象的价值相匹配。

总之，系统的安全保护将贯穿于从信息收集、处理、存贮和传送的全过程。整个系统的安全和系统中的各个课题均有密切关系，而加密技术又和整个网络结构特别是通信网的结构密切相关，因此系统的安全与保密是整个系统的重要组成部分，系统的安全与保密设计应与系统的其他课题的设计同步进行，各课题也应重视自己课题中的安全与保密问题。

本部份由三个内容组成：

第一，数据加密保护，包括：

- 传输数据的加密保护；
- 存贮数据的加密保护；
- 存取控制；
- 数据完整性鉴别；
- 数字签名；
- 密钥。

第二，系统的物理安全，包括：

- 计算机系统设备的场地环境要求；
- 计算机系统设备的场地技术要求；
- 电磁干扰和辐射的防护；
- 记录媒体的保护；
- 计算机网络的安全要求；
- 人身和设备的安全要求；
- 灾难性事件应急计划的制度；
- 安全责任和监督的实施。

第三，安全与保密的管理，包括：

- 密钥管理；
- 门卫和出入管理；
- 设备管理；
- 文档资料管理；
- 操作管理；

· 规章制度的建立。

本书对上述内容分别作了详细的描述和规定，各主系统和分系统在建设和运行过程中，对于信息系统的安全与保密的有关技术要求和规定必须严格遵照执行。

2. 数据传输的安全与保密

2.1 数据传输的内容

信息系统的传输数据加密保护是指系统在数据通信过程中的加密保护。通信网的加密是一种十分复杂的技术，它涉及到系统所要达到的保密目标；系统采用的加密方法；系统采用的加密算法；加密工作方式；数据通信采用加密时的互操作性和安全性要求；系统的保密等级；系统保密设备，机构的要求和配置等一系列问题。

2.2 保密目标

2.2.1 系统所面临的威胁

随着信息社会的不断发展，提供对计算机设备的远程访问的网络不断被开发和广泛应用。由于目前计算机本身的物理安全措施已得到了极大的改善，因而使得入侵者转而对网络的攻击产生了极大的兴趣。在无加密保护的条件下截取到网络传输过程中数据的数量不断增加，而这些数据中许多是极为敏感的数据，因此网络已成为入侵者攻击的主要目标。网络新技术的发展使得有些类型的攻击变得极为容易，如入侵者可轻而易举地监视卫星和无线网络的传输。在这种情况下，潜在的犯法行为可分为三种类型：

(1) 数据非授权的公布；

(2) 数据非授权的修改；

(3) 数据来源的非法否认。

2.2.2 入侵者对系统的攻击

入侵者对系统的攻击可分为两种形式：

(1) 被动攻击

在被动攻击中，入侵者不干扰信息流量，只是观察通过"结合"的PDU(协议数据单元)或凭证。这是被动攻击的最基本形式——数据内容的透露。若对入侵者来说数据是不可懂的，他还可以观察数据的控制信息部分从而获悉通信协议实体的位置和身份。入侵者还可以研究PDU的长度和传送的频繁程度以获得正在交换的数据的性质。这两种形式的攻击称为信息量分析攻击。被动攻击不易被发现，但可采用加密方法有效地避免。

(2) 主动攻击

入侵者可以实施主动攻击。这种攻击是把通过"结合"的PDU进行各种各样处理实现的。这些PDU可有选择地被改变、删除、延迟、重新排序、复制并及时地插入到"结合"中不受影响地通过。

由于防止的措施不同，主动攻击又可细分为：

①数据流的修改；

②数据服务的否认；

③假的“结合”初始化。

数据流的修改包括对通过“结合”的PDU的真实性、完整性和顺序性攻击。真实性意味着PDU的源点能被可靠地确定；完整性意味着PDU在途中没有被修改；顺序性则意味着PDU被正确地放置于传送的数据中。

数据服务的否认是入侵者全部报废通过“结合”的PDU。

假的“结合”初始化是入侵者重放以前录制的合法的“结合”初终序列或者试图确立假身份的“结合”。

2.2.3 保密要求

已描述过的对系统的威胁和攻击的类型在某种意义上讲主动攻击和被动攻击是双重的。也就是说，尽管数据流的修改、数据服务的否认、假的“结合”初始化等攻击是不可避免的，但它们都能被可靠地检测出来。相反，数据内容的透露和信息量分析等攻击通常无法被检测出来，但它们可被有效地避免。当我们注意到这些限制后，制定的保密要求应是：

(1) 避免数据内容的透露；

(2) 避免信息量分析；

(3) 检测出数据流的修改；

(4) 检测出数据服务的否认；

(5) 检测出假的“结合”初始化。

2.3 传输数据加密方法

存在三种传输数据加密方法：面向线路的链路加密、节点加密和端—端加密方法。链路加密方法是通过单独保护每条通信线路通过的数据流来提供安全保护的；节点加密是链路加密的改进型；端—端方法则是始终保护从信源到目的地的每个数据。这三种方法不仅它们的内部实现方法(执行过程)不同，而且提供的保密性能也不相同。

2.3.1 链路加密

链路加密方法是对通过二个节点之间的单独的通信线路的数据进行加密保护的，此时不考虑信源和目的地，

一个“结合”上的信息可以跨越大量的通信线路。每个这样的线路都对应OSI参考模式的一个数据线路层的“结合”。这些线路可以是电话线、微波线路和卫星信道，而这些线路是不受保护的，因而它们是入侵者攻击的目标。在采用链路加密方式的系统中，加密是在每个通信线路上独立实现的，而每个线路都用不同的加密密钥。因此，瓦解了一条线路并不泄漏在另一条线路上传送的数据。数据的加密通常采用序列密码。由于所通过的数据并没有进行处理，所以PDU的控制信息和数据都被加密，这就掩盖了源点和目的地的格式内容。如果在两点保持连续的密文序列，PDU的长度和频率也能被很好地掩盖。因此，在链路加密条件下所有形式的信息量分析攻击都能被避免。由于数据只在线路上被加密，在节点内不加密，所以节点必须有物质环境保密，否则破坏一个节点就要暴露通过那个节点的所有数据。

链路加密的另一个问题是安装保密设备的费用问题。除了为节点提供加密设备和安全的物质环境的一次性费用外，还包括物质环境保密所需的雇员费用、密钥管理费用、保密人员所需费用、频繁检查保密效果和保密手段是否正确执行的事务费用。这些费用要比一次性费用多得多。另一方面，平均地把链路加密保护的费用摊给每个用户也是困难的，因为系统内有些

用户并不需要加密保护。

2.3.2 节点加密

节点加密是链路加密的改进，它与链路加密的主要区别是通过节点的数据是密文而不是明文。在每个节点处，收到的加密数据被送入该节点的保密组件中，用一个密钥脱密后再用另一个密钥加密，然后向另一个节点传输。

2.3.3 端一端加密

端一端加密方法是为网络提供从源点到目的地传送的数据的加密保护。在此条件下任何一条线路被破坏都不妨碍数据的保密。确定端一端加密在哪点实现是很灵活的：可以从主机到主机；从终端到终端；从终端到服务主机或到处理过程；从处理过程到处理过程。

端一端加密方法通常超出通信子网之外，因此要求用户所用的协议有更高的标准化程度。

端一端加密方法的优点在于：每个用户或主机都可单独采用这种方法而不影响其它用户或主机；采用此法的费用可严格地摊派；这种方法不仅适用于分组交换网而且也能用于分组广播网；这种方法更适合用户对他的保密要求的了解。

2.4 系统的保密等级

通信传输系统的保密等级需根据所处理业务的保密等级适当地划分，以免不适当地增加经济负担和技术难度或带来不安全因素。

2.5 系统保密设备的要求

(1) 保密设备所用的密码算法应符合规定的密级要求，并应通过相应机关的审查，审查通过后方可在系统中使用。

(2) 保密设备应符合系统中各设备之间的接口要求。

(3) 保密设备应防止由于疏忽而发出明文。

(4) 保密设备的安装要防止盗窃和非法使用。

(5) 只要密钥变量存入设备内，就要防止对密钥的非法存取和改变。

(6) 保密设备应有在紧急情况下清除密钥的功能。

(7) 保密设备出现故障应禁止加密并警告。

(8) 保密设备有好的防电磁辐射特性，避免明文数据的辐射并应符合国家标准(待定)。

2.6 加密算法

2.6.1 类型

加密算法被定义为由明文到密文的一种变换。加密算法分为两种：常规加密算法，又称对称加密算法。公开密钥加密算法，又称非对称加密算法。常规加密算法分为序列加密算法和分组加密算法。

2.6.2 加密算法的要求

对加密算法有如下的一般要求：

(1) 加密算法所提供的保护仅取决于密钥的保密，即完全知道算法的细节(或设备的硬件)，也不能降低所期望的保密度。

(2) 加密算法能抗已知明文攻击，即知道一段明文以及与其它对应的密文也不能解密数

据的其余部分，更不能破开密钥；即或被破译，破译所需的时间也超过了掩蔽时间。

(3) 密钥量应足够大，以满足所要求的保密等级。

(4) 算法的复杂性要排除递归分类的可能性。

(5) 算法不用某些非线性攻击方法加速分析的捷径。密钥和数据相结合应采用仙农的混乱和扩散原理。

(6) 算法不存在"弱密钥"，所有选用的密钥都有同样的保密度。

本系统使用的加密算法将根据有关的审定标准划分保密的强度等级。

2.6.3 序列密码算法

(1) 序列密码算法的定义

序列密码算法是在一个密钥序列的控制下逐位地变换明文数据的一种算法。这种算法可实时地加密明文数据。明文序列和密钥序列相结合产生密文序列。密钥序列由密钥序列产生器产生，通常它是非线性序列产生器。一种典型的序列密码体制如图1所示。

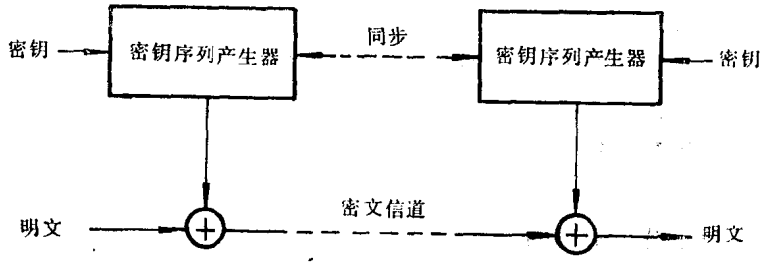

图1 序列密码体制

(2) 序列密码算法

序列密码算法是在一个密钥序列的控制下逐位变换明文数据的一种算法。明文序列和密钥序列相结合产生密文序列。密钥序列由密钥序列产生器产生。序列密码算法是以密钥和起始向量作为参量把明文和密文相关联起来的。只要起始向量满足随机的、伪随机的和不可重演的特性，密码流就是不可预计的，因而敌手就不可能解出截获的密码。

(3) 序列密码算法的要求

除满足2.6.2所述的一般要求外，序列密码算法的密钥序列产生器有以下几个重要参数：

① 可选择的密钥空间(即密钥量)的大小。

② 密钥序列的周期(即密钥序列本身重复的周期)。

③ 算法的复杂性。例如，非线性序列产生器的线性等价量等。

④ 序列产生器所产生的序列的局部随机性能。

在设计系统用的序列密码算法时，上述各参数应能满足系统的要求。

2.6.4 分组密码算法

(1) 分组密码的定义

分组密码算法是在密钥的控制下一次变换一个明文分组的密码算法。它把明文分组空间映照到一密文分组空间。如果分组长度为N比特，那么明文空间大小和密文空间大小为2^N。最基本的分组密码如图2所示。

(2) 分组密码算法

分组密码算法是把明文分成固定长度二进制数据串组，在密钥控制下逐组进行变换的密码算法。输出串组的每一位综合地依赖于输入串的每一位和密钥的每一位。密码串组的长度

必须足够大，以提高密码强度。

(3) 分组密码的适用范围

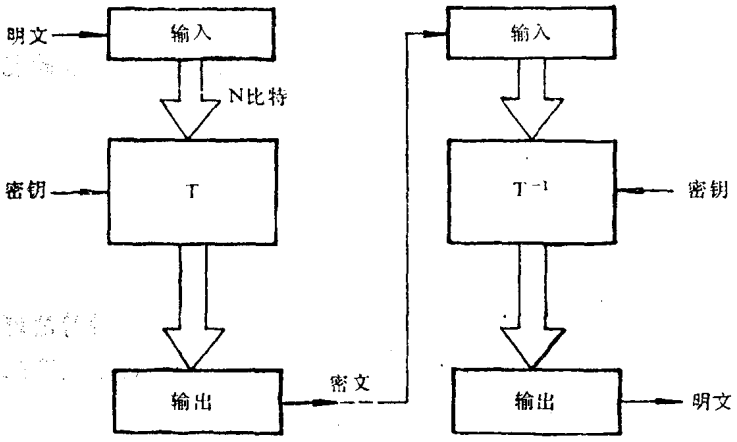

图2 分组密码体制

分组密码算法一次加密一个分组的明文，在相同的密钥条件下，相同的明文输入将产生相同的密文，这在许多场合下是不利的。由于明文是按组加密的，因此一旦分组边界丢失就会使加密产生错误，直到分组边界重新确立才能恢复。分组密码对传输错误很敏感，一旦传输过程中某一分组中的一个比特发生错误，就会使整个分组的解密发生错误。在某些应用场合下这是一个严重的缺点。但是，为了御止对数据的修改，这种错误扩散特性就变成了很重要的优点。因此，在系统中使用分组密码时必须考虑上述因素。

2.6.5 公开密钥密码算法

(1) 公开密钥密码算法定义

公开密钥密码属于分组密码的一种。它和常规的分组密码的主要区别是：公开密钥密码，把加密和解密的能力分开(即所谓的不对称性)，加密和解密是用一对密钥(E_K, D_K)实现的。这两个密钥规定了一对变换，其中的每一个是另一个的逆，但难以由其中的一个推导出另一个。每个用户都具有一对这样的密钥。其中的一个是公开的(E_K)，另一个则是保密的(D_K)。E_K用于加密明文，D_K用于解密由E_K加密的密文。公开密钥密码的一种体制如图3所示。

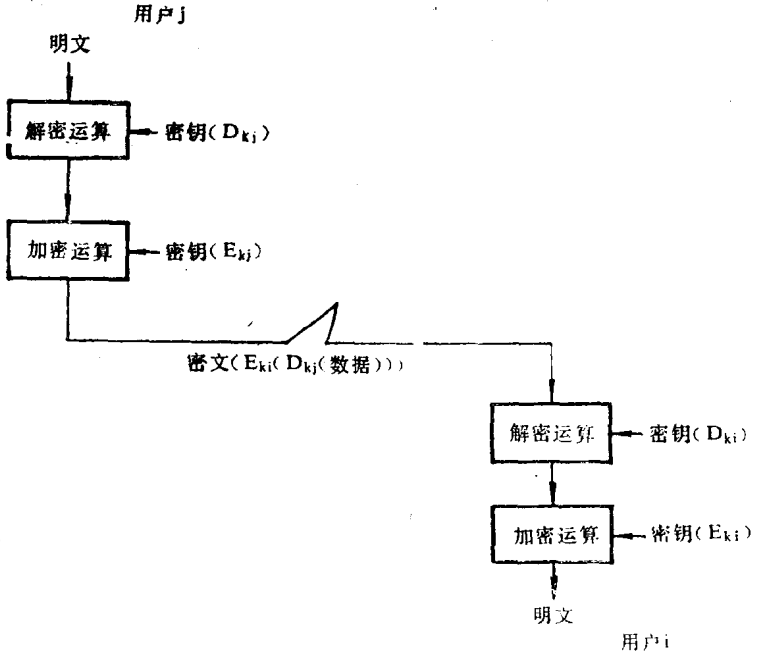

图3 公开密钥密码体制

(2) 公开密钥密码的应用

由于公开密钥密码算法的保密强度以及运行速度等因素的影响，公开密钥密码算法的应用受到了一定的限制。但是，随着技术的发展将会扩大其应用范围。目前，在密钥的分配、鉴别和数字签名领域将得到应用。

2.6.6 系统采用的加密算法

信息网络系统目前通常采用DES加密算法。美国商业部国家标准局NBS于1973年5月和1974年8月两次发布通告，向社会征求密码算法，IBM公司提出的Lucifer算法中选。1975年3月，NBS公布了此算法，以求得公众的评论。1977年1月，以"联邦信息处理标准公告(46)"的名称正式公布。

DES是一种分组加密算法。DES算法用一个64位明文数据进行初始变换、乘积交换、逆初始置换等复杂的计算和变换，得到64位密文。在DES算法中，可以由一块电路或一个程序同时完成加密和解密功能，所以受到用户的欢迎。

DES算法的保密强度是经过鉴定的，它已被普遍用于民用计算机系统中。DES使用至今，虽然有众多批评，但还未发现任何数学上可行的破译分析方法。详见"联邦信息处理标准公告(46)"，1977年1月15日公布。

有关数据加密算法也可参照国际标准化组织制定的国际标准草案DIS8227。

(1) 数据加密算法一号(DEA1)

国际标准化组织（ISO）已制定了数据加密算法的国际标准草案（DIS8227），该标准规定了一种数据加密标准——DEA1。该算法由美国提出。目前，国际上对这种分组长度为64比特的分组密码的认识仍然存在较大的分歧，许多国家的一些学者认为该算法的强度是不够的，有人则认为它只能使用到1988年。这种算法即便在美国国内也存在两种不同的意见。同时，美国只把这种算法用于非机密的政府部门的保密通信。ISO/TC97/SC20的成员国已提出要研究保密度更高的加密算法。

(2) DEA1算法规范

DEA1算法规范见ISO DIS8227。

(3) 系统密码算法

系统的密码算法包括序列密码算法、分组密码算法，公开密钥密码算法将由有关单位开展专题研究并报国家保密主管部门审查批准。

2.6.7 加密方式

加密方式因加密算法不同而分为：序列加密工作方式和分组加密工作方式。

(1) 序列加密工作方式

序列加密的工作方式基本上可划分为两种，它是以密钥序列产生的方式划分的。密钥序列可以是明文的函数，也可以是密文的函数或者是密钥序列本身的函数。

密钥序列是密钥的自身函数的工作方式，是密钥自身的密钥密码(KAK)，密钥序列也是明文和密文函数的工作方式，称为密文自身密钥(CTAK)密码。

①密钥自身密钥密码(KAK)

KAK是序列密码的基本工作方式。在这种工作方式中，密钥序列与明文以及密文序列完全无关。传输过程中某些数据比特被改变并不影响对其它数据比特的解密。从某种意义上讲这是一大优点。但是，对检测信息序列的修改并无好处。因此，这种方式不适合作为开放