网络空间安全系列丛书

密 码 学

——密码算法与协议（第3版）

郑 东 李祥学 黄 征 郁 昱 编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书共 10 章，主要介绍密码学的基本原理与设计方法，包括对称密码算法与非对称密码算法、数字签名算法及哈希函数的设计原理、密钥管理体制的设计方法，以及主流密码库的使用说明等。本次修订的内容体现在第 2 章至第 10 章，特别新增了中国流密码、国产分组密码、认证加密、基于属性的加密、国产公钥加密、国产哈希算法、基于属性的数字签名、国产数字签名、后量子签名、国产密钥交换协议、聚合签名、旁路攻击和掩码防护技术，以及全同态运算密码库和双线性对运算密码库等内容。本书涵盖了传统密码体制、基于属性的密码体制、后量子密码、抗泄露对称密码、主要的国产密码算法和主流密码库，体现了经典与前沿热点融合、理论与应用结合的特色。

本书可作为高等院校计算机、信息安全和网络空间安全等专业本科生的教材，也可作为电子信息与通信和信息管理等专业研究生的选读教材，还可供信息安全、计算机及通信等领域的工程技术人员和管理人员参考。

图书在版编目（CIP）数据

密码学：密码算法与协议 / 郑东等编著. —3 版. —北京：电子工业出版社，2022.6
ISBN 978-7-121-43417-4

Ⅰ. ①密… Ⅱ. ①郑… Ⅲ. ①密码学－高等学校－教材 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字（2022）第 077264 号

责任编辑：戴晨辰　　文字编辑：张　京　李　然
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1 092　1/16　印张：19　字数：486 千字
版　　次：2009 年 6 月第 1 版
　　2022 年 6 月第 3 版
印　　次：2022 年 6 月第 1 次印刷
定　　价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

FOREWORD

丛书序

进入 21 世纪以来，信息技术的快速发展和深度应用使得虚拟世界与物理世界加速融合，网络资源与数据资源进一步集中，人与设备通过各种无线或有线手段接入整个网络，各种网络应用、设备与人逐渐融为一体，网络空间的概念逐渐形成。人们认为，网络空间是继海、陆、空、天之后的第五维空间，也可以理解为物理世界之外的虚拟世界，是人类生存的“第二类空间”。信息网络不仅渗透到人们日常生活的方方面面，同时也控制了国家的交通、能源、金融等各类基础设施，还是军事指挥的重要基础平台，承载了巨大的社会价值和国家利益。因此，无论是技术实力雄厚的黑客组织，还是技术发达的国家机构，都在试图通过对信息网络的渗透、控制和破坏，获取相应的价值。网络空间安全问题已经成为关乎百姓生命财产安全、关系战争输赢和国家安全的重大战略问题。

要解决网络空间安全问题，必须掌握其科学发展规律。但科学发展规律的掌握非一朝一夕之功，治水、训火、利用核能都曾经历了漫长的岁月。无数事实证明，人类是有能力发现规律和认识真理的。国内外学者已出版了大量网络空间安全方面的著作，当然，相关著作还在像雨后春笋一样不断涌现。我相信有了这些基础和积累，一定能够推出更高质量、更高水平的网络空间安全著作，以进一步推动网络空间安全创新发展和进步，促进网络空间安全高水平创新人才培养，展现网络空间安全最新创新研究成果。

“网络空间安全系列丛书”出版的目标是推出体系化的、独具特色的网络空间安全系列著作。丛书主要包括五大类：基础类、密码类、系统类、网络类、应用类。在其部署上可动态调整，坚持“宁缺毋滥，成熟一本，出版一本”的原则，希望每本书都能提升读者的认识水平，也希望每本书都能成为经典范本。

非常感谢电子工业出版社为我们搭建了这样一个高端平台，能够使英雄有用武之地，也特别感谢编委会和作者们的大力支持和鼎力相助。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

中国科学院　院士

2022 年 5 月于北京

PREFACE

前言

随着人工智能、大数据、云计算和区块链等新兴前沿技术的迅猛发展，网络和数据安全及其隐私保护问题也愈加成为人们关注的焦点。为了增强我国行业信息系统的安全可控，近年来，国家有关机关和监管机构从国家安全和长远战略的角度，大力推进相关法律法规的颁布与实施。2016 年 11 月，中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》，并于 2017 年 6 月 1 日起施行。2019 年 10 月，中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议通过《中华人民共和国密码法》，并于 2020 年 1 月 1 日起实施。2021 年 6 月，中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，并于 2021 年 9 月 1 日起施行。

在此背景下，亟待加快网络空间安全领域人才的培养，提高公民的信息安全保护意识，因此出版网络空间安全领域教材的意义不言而喻。本书第 2 版出版已达 7 年之久，期间密码学各个研究分支的设计理论、分析方法和工作模式均有很大发展，新的研究方法和研究方向不断涌现。本次修订定位于面向国家战略需求而推出的网络空间安全领域（密码类）精品教材。在第 3 版中，作者依据这几年的研究实践对第 2 版的内容和组织结构都做了较大的调整和更新，主要特色是经典与前沿热点融合、理论与应用结合。

全书共 10 章，涵盖密码算法、密码协议和密码应用。第 1 章主要介绍密码学在信息安全中的作用及其相关概念。第 2 章介绍流密码的基础知识和典型流密码算法，包括中国流密码算法，使读者了解现实中使用的流密码算法及其研究现状。第 3 章介绍分组密码算法的设计，并对其进行分析，特别是分组密码的工作模式、轻量级分组密码及 SM4 算法，使读者了解各种分析方法的基本思想，并能够从中吸取经验和教训。第 4 章介绍公钥密码，包括经典的大整数因子分解密码、离散对数密码、椭圆曲线密码、基于身份的加密、基于属性的加密及近年的研究热点，如后量子公钥加密、SM2 公钥加密及 SM9 公钥加密等新型密码算法。第 5 章介绍认证和哈希函数，重点介绍 SHA 系列算法和 SM3 算法等，同时介绍对哈希函数攻击的现状。第 6 章和第 8 章介绍数字签名，包括经典的 RSA 签名、离散对数签名等，以及近年的研究热点，如聚合签名、后量子签名、SM2 数字签名和 SM9 数字签名等。第 7 章介绍密钥管理，包括基本概念、密钥建立模型、公钥传输机制、密钥传输机制、密钥导出机制及密钥协商机制等，特别介绍了 SM2 密钥交换协议和 SM9 密钥交换协议。第 9 章介绍抗泄露对称密码，包括基本概念、定义和算法设计，特别介绍了旁路攻击和掩码防护技术，并对未来抗泄露密码算法的发展方向做出展望。第 10 章介绍 OpenSSL 与其他相关密码库的使用，特别介绍了全同态运算密码库。

本书作者多年来在西安邮电大学、华东师范大学和上海交通大学等高校从事密码学的研

究和教学工作，为本科生和研究生主讲“密码学基础”“密码理论与实践”“密码协议”等专业课程。本书在写作过程中参考了大量的密码学专著、论文和技术报告。本书正是基于作者的研究、教学经验并参阅相关文献编写而成的。

本书是计算机、信息安全和网络空间安全专业高年级本科生的教材，可作为电子信息与通信和信息管理等专业研究生的选读教材，也可供信息安全、计算机、通信及电子工程等领域的科技人员参考。教学中也可根据需要，对密码协议和密码应用部分的内容进行调整。

本书包含配套教学资源，读者可登录华信教育资源网（www.hxedu.com.cn）注册后免费下载。

本书第 1、4、6、10 章主要由郑东编写，第 2、8 章主要由李祥学编写，第 3、5、7 章由黄征编写，第 9 章由郁昱编写。其中，张应辉参与了第 4 章的编写工作，王剑涛和肖畅分别参与了第 2 章和第 10 章的编写工作，在此表示感谢。在本书的选题策划和撰写过程中得到了电子工业出版社编辑的鼓励、支持，在此对为本书的出版而付出辛勤工作的相关人员表示诚挚的感谢。本书的完成得到了国家自然科学基金（62072371、61971192、61772418、62072369）资助。

鉴于作者的水平有限，书中的错误和缺憾在所难免，对一些问题的理解和叙述或有肤浅之处，诚恳地希望读者及时指出发现的错误和问题。我们欢迎任何关于本书的批评和建设性意见，以便我们以后对本书修改时参考。

编著者

于西安

CONTENTS

目录

第 1 章　密码学引论

内容提要

信息安全技术是保障受攻击的通信网络能够按照预期目标进行通信的重要技术，是包含计算机、数学及信息论等多门学科的综合学科。密码学是信息安全中的关键技术。本章主要介绍信息安全技术的应用背景及密码学在信息安全中的作用，并简要介绍相关的基本概念。

本章重点

- 密码学在信息安全中的作用
- 信息的机密性、完整性与不可否认性
- 对称密码算法与非对称密码算法
- 完善保密体制
- 算法复杂度

1.1 密码学在信息安全中的作用

信息安全涉及的范围很广，无论在军事方面，还是日常生活方面，都会涉及信息安全的问题。就计算机通信而言，其处理的信息可以归纳成两类：一类是仅在计算机内部处理和存储的信息；另一类是在计算机之间相互传递的信息。对于仅在计算机内部处理和存储的信息，希望不被非法人员访问，即禁止非法用户读取计算机内的信息；对于后一类，发送者希望能够控制在公开信道上传输的信息具有完整性和不可伪造性等。

1.1.1 信息安全面临的威胁

信息安全面临多方面的威胁，如意外事故、自然灾害及人为恶意攻击等。人为恶意攻击是有目的的破坏，可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息（如修改、删除、伪造、添加、重传、乱序、冒充及传播病毒等）。被动攻击是指在不干扰信息系统正常工作的情况下，进行截获、窃取、破译和业务流量分析等。

人为恶意攻击主要有下列 8 种手段。

（1）窃听：攻击者通过监视网络数据获得敏感信息。

（2）重传：攻击者事先截获部分或全部信息，再将此信息发送给接收者。

（3）伪造：攻击者伪造一个信息，将伪造的信息以他人身份发送给接收者。

（4）篡改：攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者。

（5）行为否认：通信实体否认已经发生的行为。

（6）拒绝服务攻击：攻击者通过某种方法使系统响应变慢甚至瘫痪，阻止合法用户获得服务。

（7）非授权访问：不按照设定的安全策略要求使用网络或计算机资源的行为都可以看作非授权访问。非授权访问主要有假冒、身份攻击、非法用户进入网络系统进行违法操作，以及合法用户以未授权方式进行操作等形式。

（8）传播病毒：通过网络传播计算机病毒，其破坏性非常大，而且难以防范。例如众所周知的 CIH 病毒、“爱虫”病毒，都具有极大的破坏性。

人为恶意攻击具有智能性、严重性、隐蔽性和多样性等特性。

（1）智能性：指恶意攻击者大都具有相当高的专业技术和熟练的操作技能，对攻击的环境经过了周密的预谋和精心策划。

（2）严重性：指涉及金融资产的网络信息系统受到恶意攻击，往往由于资金损失巨大而使金融机构和企业蒙受重大损失，甚至破产，同时也给社会稳定带来负面影响。

（3）隐蔽性：指人为恶意攻击的隐蔽性很强，不易引起怀疑，破案的技术难度大。在一般情况下，其犯罪的证据存在于软件的数据和信息资料之中，若无专业知识很难获取侦破证据。相反，犯罪行为人却可以很容易地毁灭证据。计算机犯罪现场也不像传统犯罪现场那样明显。

（4）多样性：指随着互联网的迅速发展，网络信息系统中的恶意攻击也随之发展变化。出于经济利益的巨大诱惑，近年来，各种恶意攻击主要集中于电子商务和电子金融领域。攻

击手段日新月异，目的包括偷税漏税、利用自动结算系统洗钱，以及在网络上进行营利性的商业间谍活动等。

信息安全面临的威胁也可能来自人为的无意失误。例如，操作员安全配置不当、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。事实上，人为恶意攻击虽然会造成重大后果，但更多的安全事件其实是由于人们缺乏安全意识或管理不善造成的。

1.1.2 信息安全需要的基本安全服务

要想使通信系统尽可能地正常工作，需要提供几个基本安全服务：保密性、完整性、不可否认性及可用性服务。

（1）保密性：保密性指信息不被非指定对象获得。信息的保密性需求来自消息使用的环境要求，如军队、民事机构等部门对访问人员的限制。特别是军队，通信或军事指挥部门的信息不能被敌方获得。为了达到对信息获取人员的限制，需要对信息的存储和传输提供保密性服务，使没有权限的人员不能获得这些保密信息。

密码技术是提供保密性的有效机制。密码技术通过变换，把数据内容变换成不易读懂的数据，同时又能够让授权的用户恢复出原来的数据。

（2）完整性：完整性指数据来源的完整性和数据内容的完整性。数据来源的完整性包含数据来源的准确性和可信性。数据内容的完整性指接收到的数据与正确来源生成的数据的一致性。

（3）不可否认性：不可否认性指数据的生成者或发送者不能对自己做过的事进行抵赖。当发送者对发送过的消息进行否认时，第三方能够对发送者的行为进行判断、裁决。

密码技术能够为上述服务提供基本保障，还能够提供其他更多的安全服务，如访问控制、身份认证等。

1.2 密码学导引

1.2.1 密码学历史

密码学是一门古老的学科，它通过把人们能够读懂的消息变换成不易读懂的消息来隐藏消息内容，使窃听者无法理解消息的内容，同时又能让合法用户把变换的结果还原成能够读懂的消息。

密码学的发展大致可以分为以下 4 个阶段。

（1）手工阶段：这个阶段是密码技术的初级阶段，可以追溯到几千年前，可以说自从有了人类战争，就有了密码技术。早期的密码技术是非常简单的，主要以简单的“替换”或“换位”实施密码变换，比较著名的密码是古罗马的 Caesar 密码、法国的 Vigenere 密码等。

（2）机械阶段：密码技术是不断发展的，随着破译技术的不断提升，对密码算法的安全性要求越来越高，相应的算法复杂度也越来越大，这使得人们有必要改进加密手段，使用机械的方法实现相对复杂的密码算法。从 20 世纪初到第二次世界大战后期，出现了一些专用

的加密机器，如英国 A. Turing 设计的加密机 Colossus。

（3）现代密码阶段：随着电子通信与计算机技术的发展，密码学得到了系统的发展。1949 年，香农（C. Shannon）发表了《保密系统的通信理论》，给出了密码学的数学基础，证明了一次一密密码系统的完善保密性。

（4）密码学的新方向：20 世纪 70 年代末，美国政府为了满足政府及民间对信息安全的需求，确定了数据加密标准算法 DES，首次公开加密算法细节，这使得加密的安全性仅建立在密钥的保密性之上。在 1976 年，W. Diffie 和 M. Hellman 提出了“密码学新方向”，开辟了公钥密码技术理论，使密钥协商、数字签名等密码问题有了新的解决方法。

手工阶段和机械阶段使用的密码技术可以称为古典密码技术，主要采用简单的替换或置换技术。

1.2.2 密码学基本概念

（1）密码学：研究把来自信息源的可理解的原始消息变换成不可理解的消息，同时又可恢复到原消息的方法和原理的一门科学。

（2）明文和密文：利用密码技术变换前的消息称作明文，用密码技术变换后的消息称作密文。

（3）加密算法：用于把原始消息变换成密文的算法称作加密算法。

（4）解密算法：用于恢复明文消息的算法称作解密算法。

（5）密钥：用于加密或解密的秘密信息。

（6）明文空间：一个加密算法能够加密的所有可能明文的集合。

（7）密文空间：一个加密算法输出的所有可能密文的集合。

（8）密钥空间：能够用于一个算法加密或解密的所有可能密钥的集合。

（9）密码分析：对密码体制的攻击，一般可以分为以下 4 种，即① 唯密文攻击——攻击者只知道一个要攻击的密文（通常包含消息的上文和下文）；② 已知明文攻击——攻击者知道一些明文/密文对，若一个密码系统能够抵抗这种攻击，合法的接收者就不需要销毁已解密的明文；③ 选择明文攻击——攻击者可以选择一些明文并得到对应的密文（公钥密码体制必须能够抵抗这种攻击）；④ 选择密文攻击——攻击者可以选择一些密文并得到相应的明文。

1.2.3 密码体制的分类

密码体制可以分为对称密码体制和非对称密码体制。对称密码体制（见图 1.1）是指加密/解密共用同一个密钥或很容易从一个密钥推导出另一个密钥。非对称密码体制是指加密/解密使用不同的密钥，且难以由公开密钥推出私有密钥。

对称密码体制首先假设通信双方能够通过一个安全信道协商一个会话密钥（加密/解密密钥），双方通信时，发送者 A 利用加密密钥 k 及加密算法将原消息 m 加密成密文 c；合法接收者 B 收到密文 c 后，利用解密算法及密钥 k 对密文解密得到原始消息 m。对称密码体制在公开算法的前提下，其安全性依赖于密钥的安全性。

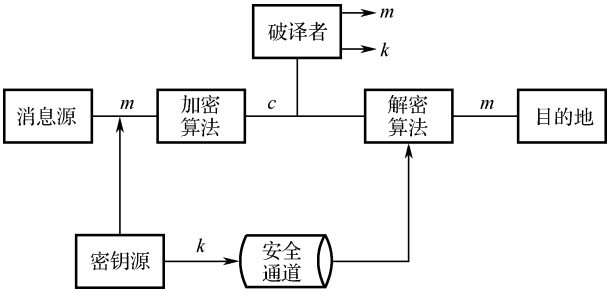

图 1.1　对称密码体制

非对称密码体制（见图 1.2）又称公钥加密体制，其主要思想如下所述。

（1）消息的接收者拥有一对公钥（PK_B）和私钥（SK_B），公钥用于加密数据，私钥用于解密数据。在使用公钥加密算法前，需要一个初始化过程安全地生成用户的公钥和私钥，并利用可靠的方法发布公钥。

（2）公钥是公开的数据，可以通过一些方法让其他任何用户得到，即公钥不对任何实体保密，但由公钥计算对应的私钥是一个难题（由私钥计算公钥是容易的）。

（3）利用公钥及密文，在不知私钥的情况下，计算对应的明文是困难的。

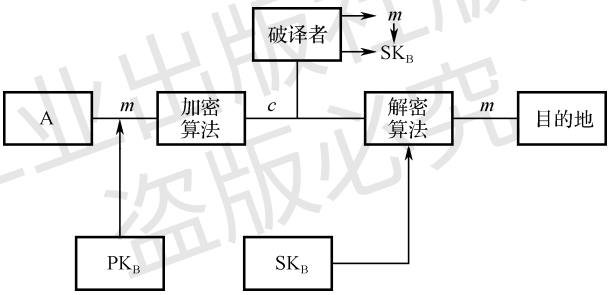

图 1.2　非对称密码体制

1.3　信息论基本概念

Shannon 于 1949 年发表了《保密系统的通信理论》，奠定了现代密码学基础。他在此文中用信息论的观点深刻阐述了信息系统的保密性问题，阐明了完善保密性、理论保密性和计算保密性等重要概念。

1．信息量和熵

定义 1.1：给定一个离散事件的集合 $X=\{x_i, i=1,\cdots,n\}$，记 $p(x_i)$是事件 x_i 出现的概率，$p(x_i)\geqslant 0$，$\sum_{i=1}^{n} p(x_i)=1$，称

$$I(x_i)=-\log_a p(x_i)$$

为事件 x_i 包含的信息量，通常令 a =2，此时相应的信息量单位是 bit。

称 $H(X)=-\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)\geqslant 0$ 为随机事件集合 X 的熵。可以看出，熵表示了集合 X

中事件包含的平均信息量或 X 中事件的平均不确定性。可以证明，对于含有 n 个事件的集合 X，有

$$0 \leqslant H(X) \leqslant \log_a n$$

当集合 X 中的所有事件等概率出现时，X 的熵达到最大值。

2．条件熵

设有两个事件集合：$X=\{x_i, i=1,\cdots,n\}$，$Y=\{y_i, i=1,\cdots,n\}$，定义联合事件集合为 $XY=\{x_i y_j, i=1,\cdots,n, j=1,\cdots,m\}$。记联合事件 x_iy_j 出现的概率为 $p(x_i,y_j)$，则

$$\sum_{i,j} p(x_i,y_j)=\sum_{i=1}^{n} p(x_i)\sum_{j=1}^{m} p(y_j \mid x_i)=1$$

由此可得集合 XY 的联合熵为

$$H(XY)=-\sum_{i,j} p(x_i,y_j)\log_2 p(x_i,y_j)$$

定义条件熵 $H(X \mid Y), H(Y \mid X)$ 分别为

$$H(X \mid Y)=-\sum_{i,j} p(x_i,y_j)\log_2 p(x_i \mid y_j)$$

$$H(Y \mid X)=-\sum_{i,j} p(x_i,y_j)\log_2 p(y_j \mid x_i)$$

综上可得

$$H(XY)=H(X)+H(Y \mid X)=H(Y)+H(X \mid Y)$$

容易证明

$$H(Y \mid X) \leqslant H(X)$$

$$H(Y \mid X) \leqslant H(Y)$$

3．互信息

设 X 和 Y 分别表示输入离散事件集合和输出离散事件集合，当输入 $x_i \in X$ 时，输出为 $y_j \in Y$，则 y_j 出现时给出 x_i 的信息量 $I(x_i;y_j)$ 可定义为

$$I(x_i;y_j)=\log_2 \frac{p(x_i \mid y_j)}{p(x_i)}$$

由 $p(x_i,y_j)=p(x_i)p(y_j \mid x_i)=p(y_j)p(x_i \mid y_j)$ 容易得到

$$I(x_i;y_j)=I(y_j;x_i)$$

即两个事件集合中一对事件相互提供相等的信息量。$I(x_i;y_j)$ 也称为 x_i 与 y_j 之间的互信息。

事件 y_j 出现时给出 X 中事件的平均信息量为

$$I(X;y_j)=\sum_i p(x_i \mid y_j)\log_2 \frac{p(x_i \mid y_j)}{p(x_i)}$$

上式经统计平均后 X 和 Y 的平均互信息为

$$I(X;Y)=\sum_i \sum_j p(x_i,y_j)\log_2 \frac{p(x_i \mid y_j)}{p(x_i)}$$

容易证明，平均互信息有以下性质：

（1）$I(X;Y)\geqslant 0$；

（2）$I(X;Y)=I(Y;X)$；

（3）$I(X;Y)=H(X)-H(X|Y)=H(Y)-H(Y|X)=H(X)+H(Y)-H(X,Y)$；

（4）当 X 与 Y 独立时，$I(X;Y)=0$。

4．信道容量

对于一个通信系统，设 X 是其所有可能输入的集合，Y 是其所有可能输出的集合，定义其信道容量为

$$C=\max_{\{p(x_i)\}} I(X;Y)$$

5．完善保密性

在一个保密系统中，设 M 为明文空间，明文长度为 l，m 为 M 中的明文，K 为密钥空间，密钥长度为 r，k 为 K 中的密钥，C 为密文空间，密文长度为 v，c 为 C 中的密文。有下列关系式成立：

$$I(m;c)=H(m)-H(m|c)$$
$$I(k;c)=H(k)-H(k|c)$$

即密文与明文的互信息等于明文熵与明文对密文的条件熵之差，密文与密钥的互信息等于密钥熵与密钥对密文的条件熵之差。同时还有

$$H(m|(c,k))=0,\quad I(m;(c,k))=H(m)$$

在一个保密系统中，若密文与明文之间的互信息 $I(m;c)=0$，则称该保密系统为完善保密系统或无条件保密系统，此时在唯密文攻击下，系统是安全的（在已知明文或选择明文攻击下不一定安全）。

关于完善保密体制更多的内容见参考文献[1]。

1.4　计算复杂性

问题是指给定一些描述参数，要求给出满足一些条件的解答的一个提问；也可以理解为给定一些参数的输入，要求给出满足一些性质的输出。

算法是指求解某个问题的一系列具体步骤或求解某个问题的通用计算机程序。算法必须是正确的、长度有限的且对于任意输入都能终止的。

一个算法的复杂度可用两个变量度量：时间复杂性 $T(n)$和空间复杂性 $S(n)$，n 是输入的规模。时间复杂性 $T(n)$指的是以某特定的基本步骤为单元，完成计算过程所需要的总单元数。空间复杂性 $S(n)$是指以某特定的基本存储空间为单元，完成计算过程所需要的总存储单元数。

算法的复杂性通常用 $O(\cdot)$ 表示数量级，其含义为：对于任意的实值函数 f 和 g，$f(n)=O(g(n)),n\to\infty$ 表示存在一个值 $a>0$，当 n 充分大时，使 $|f(n)|\leqslant a|g(n)|$。计算复杂性的数量级是指当 n 较大时，使得算法增长最快的函数，其所有常数和较低阶形式的函数忽略不计。例如一个算法的复杂性是 $5n^3+3n^2+34$，则其计算复杂性是 n^3 阶的，表示为

$O(n^3)$；若算法复杂性是 $3n^2+34$，则其计算复杂性是 n^2 阶的，表示为 $O(n^2)$。

计算复杂性理论中的另一个符号是“o”：若 $\lim_{n\to\infty} f(n)/g(n)=0$，则记作 $f(n)=o(g(n))$，$n\to\infty$，其含义是：当 $n\to\infty$ 时，与 $g(n)$相比，$f(n)$可以忽略不计。

若一个算法的复杂性不依赖于 n，则它是常数级的，用 $O(1)$表示。$O(n)$表示算法的复杂性随 n 线性增长，该算法称为线性算法。若一个算法的复杂性是 n 的多项式函数 $f(n)$，则称此算法为多项式时间算法或有效算法，其复杂度为 $T(n)=O(n^t)$，t 是一个常数。

复杂性是 $O(c^{f(n)})$ 的算法称为指数型算法，其中 c 是常数，$f(n)$是多项式。

复杂性不能用多项式函数去界定的算法称为指数时间算法，其复杂性称为指数复杂性。常见的指数复杂性有 $2^n, n!, n^n, 2^{n^2}, n^{\mathrm{lb}(n)}, n^{n^n}$ 等。其中，$n^{\mathrm{lb}(n)}, n^{n^n}$ 不是通常说的指数函数，如 $n^{\mathrm{lb}(n)}$ 比任何多项式增长速度都快，但比 $2^{n\varepsilon}(\varepsilon>0)$ 增长速度慢，n^{n^n} 比指数增长还要快。在复杂性理论中，这类函数统称为指数函数，而不做进一步细分。

问题的种类有很多，比较重要的有两种形式：一种是从一些可行解的组合中求出最优解的问题；另一种是判定问题或判别问题，它只有两种可能的解，即“yes”或“no”。

图灵机是一种配有无限读/写纸带的有限状态机，它是一种实际计算模型。图灵机可分为确定型图灵机（DTM）和非确定型图灵机（NTM）。确定型图灵机是指每执行一步计算，都有下一步确定的动作。非确定型图灵机是指每执行一步计算，其下一步动作都有几种可能的选择（即下一步动作不唯一确定）。关于图灵机更多的知识可以见参考文献[2]。

在图灵机计算模型下，复杂性理论根据对解决最难问题特例的算法、所需要的最低时间和空间进行分类。在确定型图灵机上，多项式时间内可解的问题属于 P 类，即这类问题有多项式时间 DTM 程序。在非确定型图灵机上，多项式时间内可解的问题属于 NP 类，即这类问题有多项式时间 NTM 程序。P 类包含在 NP 类中，即 $\mathrm{P}\subseteq\mathrm{NP}$，但 P 是否等于 NP，是个未知的问题。

本 章 小 结

本章主要介绍了计算机安全面临的问题及安全服务的需求，并概述了密码技术的分类，同时介绍了与密码技术相关的基础知识、信息论的相关概念及计算复杂性理论。

参 考 文 献

[1] 杨义先, 林须端. 编码密码学[M]. 北京: 人民邮电出版社, 1992.

[2] 陈志平, 徐宗本. 计算机数学——计算复杂性理论与 NPC, NP 难问题的求解[M]. 北京: 科学出版社, 2001.

[3] 王新梅, 马文平, 武传坤. 纠错密码理论[M]. 北京: 人民邮电出版社, 2001.

问 题 讨 论

1．举出了解的两个使用对称加密算法的实例。

2．设一个系统传送 0,1,…,9，偶数在传送时以 0.1 的概率错成另外的偶数，其他数字能够正确接收，求收到一个数字平均得到的信息量。

3．对于任意概率事件集 X，Y，Z，证明下述三角不等式成立：

$$H(X|Y)+H(Y|Z)\geqslant H(X|Z)$$