普通高等教育“十一五”国家级规划教材

重点大学计算机专业系列教材

应用密码学

刘嘉勇 主编
任德斌 胡勇 方勇 编著

清华大学出版社

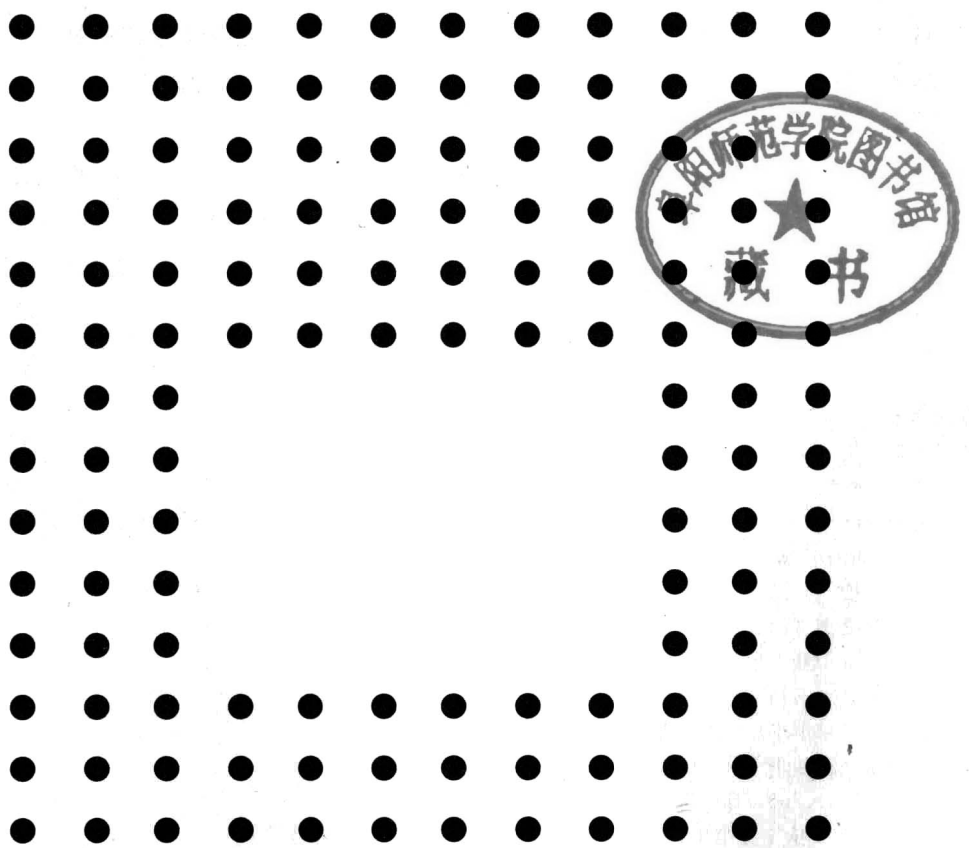
普通高等教育“十一五”国家级规划教材

重点大学计算机专业系列教材

应用密码学

刘嘉勇　主编

任德斌　胡　勇　方　勇　编著



清华大学出版社

北京

内 容 简 介

应用密码学是信息安全学科体系和信息系统安全工程的重要组成部分。本书旨在从应用的角度系统介绍密码学的体系结构、基本原理和技术。全书共分为10章，主要内容包括密码学概述、古典密码技术、分组密码体制、公钥密码体制、散列函数与报文鉴别、数字签名技术、密钥管理技术、身份鉴别技术、序列密码技术基础及密码技术应用等，并将与密码学密切相关的一些数学知识作为附录，以供需要的读者学习阅读。每章最后均配有思考题和习题，以帮助读者掌握本章重要知识点并加以巩固。

本书可作为信息安全、计算机科学与技术、信息与计算科学、通信工程、信息管理以及电子商务等信息技术类本/专科专业密码学课程的教材，也可供初学密码学的研究生及从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

图书在版编目(CIP)数据

应用密码学/刘嘉勇主编；任德斌，胡勇，方勇编著. —北京：清华大学出版社，2008.9
(重点大学计算机专业系列教材)
ISBN 978-7-302-17715-9

Ⅰ. 应… Ⅱ. ①刘… ②任… ③胡… ④方… Ⅲ. 密码－理论－高等学校－教材
Ⅳ. TN918.1

中国版本图书馆CIP数据核字(2008)第075210号

责任编辑：付弘宇　李玮琪
责任校对：焦丽丽
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京国马印刷厂
装 订 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：16.5　**字　数**：408千字
版　　次：2008年9月第1版　　**印　　次**：2008年9月第1次印刷
印　　数：1～3000
定　　价：25.00元

出版说明

随着国家信息化步伐的加快和高等教育规模的扩大，社会对计算机专业人才的需求不仅体现在数量的增加上，而且体现在质量要求的提高上，培养具有研究和实践能力的高层次的计算机专业人才已成为许多重点大学计算机专业教育的主要目标。目前，我国共有16个国家重点学科、20个博士点一级学科、28个博士点二级学科集中在教育部部属重点大学，这些高校在计算机教学和科研方面具有一定优势，并且大多以国际著名大学计算机教育为参照系，具有系统完善的教学课程体系、教学实验体系、教学质量保证体系和人才培养评估体系等综合体系，形成了培养一流人才的教学和科研环境。

重点大学计算机学科的教学与科研氛围是培养一流计算机人才的基础，其中专业教材的使用和建设则是这种氛围的重要组成部分，一批具有学科方向特色优势的计算机专业教材作为各重点大学的重点建设项目成果得到肯定。为了展示和发扬各重点大学在计算机专业教育上的优势，特别是专业教材建设上的优势，同时配合各重点大学的计算机学科建设和专业课程教学需要，在教育部相关教学指导委员会专家的建议和各重点大学的大力支持下，清华大学出版社规划并出版本系列教材。本系列教材的建设旨在“汇聚学科精英、引领学科建设、培育专业英才”，同时以教材示范各重点大学的优秀教学理念、教学方法、教学手段和教学内容等。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

1. 面向学科发展的前沿，适应当前社会对计算机专业高级人才的培养需求。教材内容以基本理论为基础，反映基本理论和原理的综合应用，重视实践和应用环节。

2. 反映教学需要，促进教学发展。教材要能适应多样化的教学需要，正确把握教学内容和课程体系的改革方向。在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

3. 实施精品战略，突出重点，保证质量。规划教材建设的重点依然是专业基础课和专业主干课；特别注意选择并安排了一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现重点大学计算机专业教学内容和课程体系改革成果的教材。

4. 主张一纲多本，合理配套。专业基础课和专业主干课教材要配套，同一门课程可以有多本具有不同内容特点的教材。处理好教材统一性与多样化的关系；基本教材

与辅助教材以及教学参考书的关系；文字教材与软件教材的关系，实现教材系列资源配套。

5. 依靠专家，择优落实。在制订教材规划时要依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后要认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

教材编委会

前言

现代密码技术已被广泛地应用到了信息技术的许多领域，是实现信息系统安全的关键技术之一，在保障网络信息安全的应用中具有重要地位。现代密码技术的研究内容除传统的信息机密性保护技术外，还包括数字签名、报文与身份鉴别、密钥管理、安全协议等与信息安全密切相关的重要内容。应用密码学已成为许多高等院校信息安全、通信工程、计算机科学、信息管理、电子商务等本科专业一门重要的专业基础课程及重要的教学内容。

针对高等院校信息技术类相关专业本科生所开设的课程特点，编者结合近几年在应用密码学方面的教学实践情况，广泛汲取了各类成功教材的有益经验，博采众家之长而精心编著了本教材。在教材的体系构架和内容编排上以培养学生的密码技术应用能力为目标，突出教材的体系性和密码技术的实用性，尽量避免传统密码教材或专著注重密码学的数学原理和理论分析，而应用性偏弱的局限，并对一些需要数学知识可能过于深奥的知识点，如密码学的信息论基础、序列密码以及密码分析等内容进行了简化或忽略，重点选择一些具有典型意义和常用的密码体制和算法进行介绍，并在每章最后均配有思考题和习题以帮助学生对本章重要知识点的掌握和巩固。使其更加易于课堂教学的实施和学生阅读，激发学生潜在的学习积极性。

本教材的主要特色：可读性强、结构合理、强调基础、注重应用，不求面面俱到，力求使学生能够较快掌握密码技术的核心内容。在教材内容取舍、结构编排、密码算法选择及习题设计上尽量体现出广泛的代表性和典型性，做到教材内容主次分明、结构清晰、重点突出、逻辑性强，对知识点的阐述强调由浅入深、循序渐进，使教材具有显著的可读性和实用性。可使读者能够在充分掌握密码学基础知识的同时，掌握应用密码技术，并将其尽快运用到实际工作中，是一本较为系统全面介绍密码学基本原理和典型应用的教材。全书共分为 10 章，其具体章节内容安排如下。

第 1 章主要介绍密码学与信息安全、密码技术发展概况以及密码学的基本概念，包括密码学的任务、密码系统、密码系统攻击以及密码体制的分类等内容。

第 2 章介绍古典密码体制中的基本加密运算、几种典型的古典密码体制以及关于古典密码体制的基本破译方法。

第 3 章通过对典型的分组密码算法，如数据加密标准（DES）、高级加密标准（AES）、国际数据加密算法（IDEA）、RC5 等，介绍分组密码算法的特点、设计原理、实

现方法与安全强度，以及分组密码算法在实际应用中的基本工作模式及相关问题。

第 4 章介绍公钥密码体制的原理和基本概念、RSA 与 ElGamal 算法原理、计算问题与安全性、椭圆曲线密码体制(ECC)基本原理与应用等内容。

第 5 章介绍散列函数的需求、特点、一般结构以及相关的安全性问题等。通过 SHA、HMAC 等密码算法，介绍散列算法和报文鉴别的原理以及实现报文完整性保护和鉴别的应用。

第 6 章介绍数字签名的基本概念和典型数字签名方案，如 RSA 数字签名方案、ElGamal 数字签名方案和数字签名标准(DSS)的原理与实现，并对典型特殊数字签名方案的原理与应用进行了介绍。

第 7 章介绍密钥的种类与层次结构、密钥管理的生命周期、密钥的生成与安全存储、密钥的协商与分发问题、典型密钥分配与协商协议及算法、PKI 技术基础等。

第 8 章则对身份鉴别的基本原理与典型协议进行了介绍。

第 9 章包括序列密码的基本原理及模型、线性反馈移位寄存器 LFSR、基于 LFSR 的序列密码以及典型序列密码算法。

第 10 章介绍密码技术在数字通信安全、电子商务中的典型应用技术和协议。

考虑密码学涉及的数学知识较多，特别是概率论、近代代数和数论方面的基础知识。希望学习本书的读者需要具备一定的概率论基础知识。为方便读者学习，本书的附录对书中涉及的有关初等数论和近代代数的基础知识进行了介绍。学习和了解这方面的数学知识对研究和学习应用密码学是大有帮助的，但即使没有学过这些数学知识也不会影响对本书的阅读和学习。

本书语言通俗易懂，内容丰富翔实，可作为信息安全、计算机科学与技术、信息与计算科学、通信工程、网络工程以及电子商务等信息技术类本/专科专业密码学课程的教材，也适合初学密码学的研究生及从事信息安全、计算机、通信、电子工程等领域的科技人员阅读参考。

本书由四川大学信息安全研究所组织编写，全书由刘嘉勇教授负责组织与统稿工作。第 1、5、6、10 章由刘嘉勇负责编写；第 3、4、7、9 章由任德斌负责编写；第 2 章由方勇编写；第 8 章及附录由胡勇编写。戴宗坤教授、周安民教授对全书的结构设计和统筹提出了宝贵意见和建议，刘晓东、戴进锋、叶云霞、吴荣军等研究生参与了部分资料的收集和整理工作。四川大学信息安全研究所全体同志为本书的编写给予了大力支持和多方面的帮助。本书的编写还从其他老师和同行的有关著作和教材(包括网站)中得到了帮助，作者在此一并表示由衷的感谢。

尽管作者已尽了最大努力，但由于作者的学识和水平，书中难免有需要商榷之处，诚望读者不吝赐教斧正。作者的电子邮箱：ljy@scu.edu.cn。

本书编者制作了配套的电子课件，以方便使用本书作教材的老师教学。课件可从清华大学出版社网站 http://www.tup.tsinghua.edu.cn 下载。在本书及课件的使用中遇到任何问题，可联系：fuhy@tup.tsinghua.edu.cn。

编　者

2008 年 5 月于四川大学

目 录

第 1 章　密码学概述 …… 1

1.1　信息安全与密码技术 …… 1
1.2　密码技术发展简介 …… 1
1.2.1　古典密码时期 …… 2
1.2.2　近代密码时期 …… 3
1.2.3　现代密码时期 …… 4
1.3　密码学基本概念 …… 6
1.3.1　密码学的主要任务 …… 6
1.3.2　密码系统的概念 …… 7
1.3.3　对密码系统的攻击 …… 8
1.3.4　密码系统的安全性 …… 10
1.3.5　密码体制的分类 …… 12
1.3.6　对称与非对称密码体制的主要特点 …… 13
思考题与习题 …… 15

第 2 章　古典密码技术 …… 16

2.1　替代密码 …… 16
2.1.1　单表替代密码 …… 16
2.1.2　多表替代密码 …… 19
2.2　置换密码 …… 23
2.2.1　周期置换密码 …… 24
2.2.2　列置换密码 …… 25
2.3　转轮机密码 …… 25
2.4　古典密码的统计分析 …… 27
2.4.1　单表替代密码分析 …… 27
2.4.2　多表替代密码分析 …… 33
2.4.3　对 Hill 密码的已知明文分析 …… 38

思考题与习题 …… 39

第 3 章 分组密码 …… 41

3.1 概述 …… 41
3.2 分组密码的设计原则与评估 …… 41
3.2.1 分组密码的设计原则 …… 41
3.2.2 分组密码的评估 …… 42
3.3 分组密码常见的设计方法 …… 43
3.3.1 Feistel 结构 …… 43
3.3.2 SPN 结构 …… 43
3.4 数据加密标准(DES) …… 44
3.4.1 算法描述 …… 45
3.4.2 DES 的安全性分析 …… 50
3.4.3 三重 DES …… 51
3.5 高级加密标准(AES) …… 52
3.5.1 AES 算法的数学基础 …… 53
3.5.2 算法的总体描述 …… 55
3.5.3 算法的基本变换 …… 56
3.5.4 密钥扩展算法 …… 58
3.5.5 解密算法 …… 59
3.6 分组密码的工作模式 …… 61
3.6.1 电子本模式(ECB) …… 61
3.6.2 密码分组链接模式(CBC) …… 62
3.6.3 密码反馈模式(CFB) …… 63
3.6.4 输出反馈模式(OFB) …… 64
3.6.5 计数器模式(CTR) …… 65
3.7 其他分组密码 …… 66
3.7.1 IDEA 加密算法 …… 66
3.7.2 RC6 加密算法 …… 68
思考题与习题 …… 70

第 4 章 公钥密码体制 …… 71

4.1 概述 …… 71
4.1.1 公钥密码体制提出的背景 …… 71
4.1.2 公钥密码的基本思想 …… 72
4.1.3 公钥密码的应用 …… 73
4.2 RSA 公钥密码体制 …… 73
4.2.1 RSA 的算法描述 …… 74
4.2.2 RSA 的实现 …… 75

4.2.3 RSA 的安全性 …… 76
4.2.4 RSA 在应用中的问题 …… 77
4.3 ElGamal 公钥密码体制 …… 78
4.4 椭圆曲线密码体制 …… 79
4.4.1 概述 …… 79
4.4.2 椭圆曲线的概念与运算 …… 80
4.4.3 椭圆曲线密码体制 …… 82
思考题与习题 …… 85

第 5 章 散列函数与消息鉴别 …… 86

5.1 散列函数的概念 …… 86
5.1.1 散列函数的性质 …… 86
5.1.2 散列函数的应用 …… 87
5.2 散列函数的构造与设计 …… 88
5.2.1 迭代型散列函数的一般结构 …… 88
5.2.2 散列函数的设计方法 …… 89
5.3 安全散列算法 SHA …… 91
5.3.1 SHA-1 …… 91
5.3.2 其他 SHA 算法 …… 96
5.4 对散列函数的攻击 …… 100
5.4.1 生日悖论 …… 100
5.4.2 生日攻击 …… 101
5.5 消息鉴别 …… 102
5.5.1 基于加密技术的消息鉴别 …… 103
5.5.2 基于散列函数的消息鉴别 …… 104
5.5.3 HMAC 算法 …… 108
思考题与习题 …… 110

第 6 章 数字签名技术 …… 112

6.1 数字签名概述 …… 112
6.1.1 数字签名的特性 …… 112
6.1.2 数字签名的执行方式 …… 115
6.2 基于公钥密码体制的典型数字签名方案 …… 117
6.2.1 RSA 数字签名方案 …… 117
6.2.2 ElGamal 数字签名方案 …… 118
6.2.3 数字签名标准 DSS …… 120
6.2.4 基于椭圆曲线密码的数字签名算法 ECDSA …… 123
6.3 特殊数字签名方案 …… 125
6.3.1 不可否认签名 …… 125

6.3.2 盲数字签名 …… 127
6.3.3 群签名 …… 128
思考题与习题 …… 130

第7章 密钥管理技术 …… 131

7.1 密钥管理的原则 …… 131
7.2 密钥的层次结构 …… 133
7.3 密钥的生命周期 …… 134
7.3.1 密钥的产生 …… 134
7.3.2 密钥的存储和备份 …… 135
7.3.3 密钥的终止和销毁 …… 136
7.4 密钥分发和密钥协商 …… 136
7.4.1 密钥分发 …… 136
7.4.2 密钥协商 …… 138
7.5 公开密钥的分发 …… 140
7.5.1 公开密钥的分发方式 …… 140
7.5.2 X.509 公钥证书 …… 142
7.6 秘密分割 …… 144
7.6.1 Shamir 秘密分割门限方案 …… 145
7.6.2 Asmuth-Bloom 门限方案 …… 147
7.7 会议密钥 …… 149
思考题与习题 …… 149

第8章 身份鉴别技术 …… 151

8.1 身份鉴别的基本原理 …… 151
8.2 基于口令的身份鉴别技术 …… 152
8.2.1 基本口令鉴别协议 …… 152
8.2.2 口令鉴别协议的改进 …… 152
8.2.3 基于质询—响应的身份鉴别技术 …… 153
8.2.4 S/Key 一次性口令身份鉴别协议 …… 154
8.3 基于生物特征的身份鉴别技术 …… 155
8.4 零知识证明与身份鉴别 …… 157
8.4.1 Fiege-Fiat-Shamir 身份鉴别方案 …… 158
8.4.2 F-F-S 增强方案 …… 160
8.4.3 Guillon-Quisquater 身份鉴别方案 …… 162
8.4.4 Schnorr 身份鉴别方案 …… 163
思考题与习题 …… 164

第 9 章 序列密码 …… 165

9.1 概述 …… 165
9.2 线性反馈移位寄存器(LFSR) …… 167
9.3 基于 LFSR 的序列密码 …… 168
9.4 序列密码 RC4 …… 170
思考题与习题 …… 171

第 10 章 密码技术应用 …… 172

10.1 网络通信的数据加密方式 …… 172
10.1.1 链路加密 …… 172
10.1.2 端—端加密 …… 173
10.2 PGP 技术及应用 …… 175
10.2.1 概述 …… 175
10.2.2 运行方式和服务 …… 176
10.2.3 密钥和密钥环 …… 180
10.2.4 公钥管理和信任关系 …… 185
10.2.5 基于 PGP 的电子邮件通信安全 …… 189
10.3 Kerberos 身份鉴别系统 …… 193
10.3.1 Kerberos 系统概述 …… 193
10.3.2 Kerberos 鉴别模型 …… 194
10.3.3 Kerberos 协议鉴别过程 …… 195
10.3.4 Kerberos 的局限性 …… 199
10.4 安全电子交易 SET …… 200
10.4.1 概述 …… 200
10.4.2 SET 系统的商务模型 …… 201
10.4.3 基于 SET 的交易过程 …… 202
10.4.4 SET 的双重数字签名机制 …… 206
10.4.5 SET 的支付流程 …… 207
10.5 公钥基础设施 PKI …… 209
10.5.1 PKI 的定义 …… 209
10.5.2 PKI 提供的服务和应用 …… 211
10.5.3 PKI 的构成 …… 213
10.5.4 PKI 标准 …… 216
10.5.5 PKI 的信任模型 …… 218
10.5.6 PKI 的运行模型 …… 223
10.5.7 PKI 产品简介 …… 224
思考题与习题 …… 227

附录A 密码学数学基础 …… 228

A.1 数论基础 …… 228
A.1.1 素数与互素 …… 228
A.1.2 模运算与同余式 …… 230
A.1.3 费马定理与欧拉定理 …… 233
A.1.4 中国剩余定理 …… 234
A.1.5 离散对数 …… 236
A.1.6 平方剩余 …… 237
A.2 群论 …… 240
A.2.1 群的概念 …… 240
A.2.2 群的性质 …… 241
A.3 有限域 …… 241
A.3.1 域和有限域的概念 …… 241
A.3.2 域上的多项式 …… 242
A.3.3 有限域元素的多项式表示 …… 243

附录B 计算复杂性 …… 245

B.1 算法的复杂性 …… 245
B.2 问题的复杂性 …… 246
思考题与习题 …… 247

参考文献 …… 248

第1章

密码学概述

1.1 信息安全与密码技术

密码技术是一门古老的技术，大概自人类社会出现战争便产生了密码(cipher)。由于密码技术长期仅用于军事、政治、外交等要害部门的保密通信，使得密码技术的研究工作本身也是秘密进行的，因此密码学知识和相关技术主要掌握在军事、政治、外交等保密机关，难以公开发表。然而，随着计算机科学技术、通信技术、微电子技术的发展，使得计算机和通信网络的应用进入了人们的日常生活和工作中，出现了电子政务、电子商务、电子金融等必须确保信息安全的网络信息系统，密码技术在信息安全中的应用不断得到发展，密码学也因此而脱去神秘的面纱从军事科学逐步走向商用，成为受到广泛关注的学科。

随着信息技术的发展和信息社会的来临，网络信息交换逐步已成为人们获取和交换信息的主要形式，信息安全变得越来越重要。密码技术在解决网络信息安全中发挥着重要作用，信息安全服务要依赖各种安全机制来实现，而许多安全机制则需要依赖于密码技术。使用密码技术不仅可以有效保障信息的机密性，而且可以保护信息的完整性和真实性，防止信息被篡改、伪造和假冒等。因此，密码技术是信息安全的基础技术，而密码算法又是密码技术的核心，其重要性不言而喻。可以说密码学贯穿于网络信息安全的整个过程，在解决信息的机密性保护、可鉴别性、完整性保护和信息抗抵赖性等方面发挥着极其重要的作用。因此，密码学是信息安全学科建设和信息系统安全工程实践的基础理论之一。密码技术已渗透到信息系统安全工程的多个领域和大部分安全技术或机制中。可以毫不夸张地说，对密码学或密码技术一无所知的人不可能从技术层面上完全理解信息安全。

1.2 密码技术发展简介

密码技术源远流长，其起源可以追溯到几千年前的埃及、巴比伦、古罗马和古希腊。早在4000多年以前，古埃及人就在墓志铭中使用过类似于象形文字那样奇妙的符号，这是史载的最早的密码形式。古代密码虽然不是起源于战争，但其发展成果却首先被用于战争。可以说，人类社会自从有了战争，有了保密通信的需求，就有了密码技术的研究和应用。交战双方都为了保护自己的通信安全、窃取对方的情报而研究各种信息加密技术和密码分析技术。

根据不同时期密码技术采用的加密和解密实现手段的不同特点，密码技术的发展历史大致可以划分为三个时期，即古典密码、近代密码和现代密码时期。

1.2.1 古典密码时期

这一时期从古代到19世纪末，长达数千年。由于这个时期社会生产力低下，产生的许多密码体制都是以“手工作业”的方式进行，用纸笔或简单的器械来实现加密/解密的，一般称这个阶段产生的密码体制为“古典密码体制”，这是密码学发展的手工阶段。

中国历史的密码轶事虽不多，但在我国古代却早有以藏头诗、藏尾诗、漏格诗及绘画等形式，将要表达的真正意思或秘密信息隐藏在诗文或画卷中特定位置的记载。

早期的古希腊人在战争中使用一种“秘密书写”的方法来安全传送军事情报，奴隶主先将奴隶的头剃光，然后将情报刺在奴隶的头上，等奴隶的头发长长以后，将他派往另一个部落，然后再剃光头发使原来信息显现出来，从而实现了两个部落间的秘密通信。

古希腊著名作家艾奈阿斯在其著作《城市防卫论》中曾提到一种被称为“艾奈阿斯绳结”的密码。它的作法是从绳子的一端开始，每隔一段距离打一个绳结，而绳结之间距离不等，不同的距离表达不同的字母。按此规定把绳子上所有绳结的距离按顺序记录下来，并换成字母，就可理解它所传递的信息。

公元前440多年的斯巴达克人发明了一种称为“天书”(skytale)的加密器械来秘密传送军事情报。这是人类历史上有文献记载的最早使用的密码器械。“天书”是通过一个带状物，如纸带、羊皮带或是皮革类的东西，呈螺旋形紧紧地缠在一根权杖或木棍上，之后再沿着棍子的纵轴书写文字，在这条带状物解开后，上面的文字将杂乱无章，无法理解，但收信人只需用一根同样直径的棍子，重复这个过程，就可以看到明文。这是最早的移位密码(也称换位密码或置换密码)。

大约在公元前1世纪，罗马帝国恺撒(Caesar)大帝就设计出一种较简单的替换式密码，并在高卢战争中使用。这种密码把信中每个文字的字母都用字母顺序表中相隔两位后的一个字母取代。

公元16世纪中期，意大利的数学家卡尔达诺发明了卡尔达诺漏格板，他利用硬纸上留出的空格，经过数次移位后，把需要传递的秘密信息写到信纸一些位置上，然后在其他地方填上一些文字，组成通信的公开信文。收信人只要在信纸上铺上同样的漏格板，即可读出秘密信文。1917年，法国的密码分析专家就曾成功地破译了德国间谍利用旋转漏格移位法加密的密码。

17世纪，英国著名的哲学家弗朗西斯·培根在他所著的《学问的发展》一书中最早给密码下了定义，他说，“所谓密码应具备三个必要的条件，即易于翻译、第三者无法理解、在一定场合下不易引人注意。”

古典密码的形式是多种多样的，其基本加密方法包括各种隐写术、文字替换或移位，大多使用手工或简单机械变换的方式实现。现代英语中的cryptography(密码编码学)一词就是由古希腊语的kryptos(隐藏)和graphcin(写)这两个单词组合而成的。

这一时期的密码技术仅是一门文字变换艺术，其研究与应用远没有形成一门科学，最多只能称其为密码术。

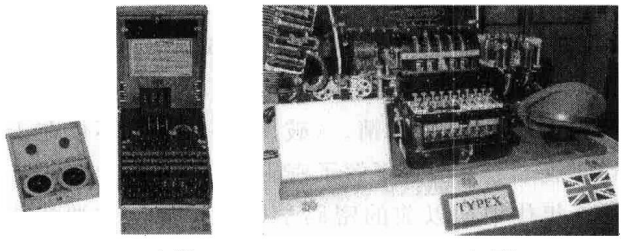
1.2.2　近代密码时期

近代密码时期是指20世纪初到20世纪50年代左右。1895年无线电诞生后，各国在通信、特别是军事通信中普遍采用无线电技术。由于通过无线电波送出的每条信息不仅传给了己方，也传送给了敌方。为了实现保密通信，各国随即开始研究无线电密码的编制和破译。因此人类历史上早就伴随战争出现的密码也就立即与无线电结合，出现了无线电密码。直到第一次世界大战结束，所有无线电密码都是使用手工编码，毫无疑问，手工编码效率极其低下，同时由于受到手工编码与解码效率的限制，使得许多复杂的保密性强的加密方法无法在实际中应用，而简单的加密方法又很容易被破译，因此在军事通信领域，急需一种安全可靠而又简便有效的方法。

为了适应无线电密码通信的需要，从1919年以后的几十年中，密码研究人员设计出了各种各样采用机电技术的密码机来取代手工编码加密方法，实现保密通信的自动编解码。随着转轮机的出现，使得几千年以来主要通过手工作业实现加密/解密的密码技术有了很大进展。

1918年，美国加州奥克兰的Edward H. Hebern申请了第一个转轮机专利，这种装置在差不多五十年里被指定为美军的主要密码设备。毫无疑问，这项工作奠定了第二次世界大战中美国在密码学方面的重要地位。

1919年，德国人亚瑟·谢尔比乌斯(Arthur Scherbius)利用机械电气技术发明了一种能够自动编码的转轮密码机(简称转轮机，rotor)。这就是历史上最著名的德国“埃尼格玛”(ENIGMA，意为哑谜)密码机，如图1.1(a)所示。在第二次世界大战期间，ENIGMA机曾作为德国陆、海、空三军最高级密码机，并使得英军从1942年2月到12月一直都不能解读德国潜艇发出的信号。



(a) ENIGMA密码　　(b) TYPEX密码机

图1.1　密码机

英国在第二次世界大战期间发明并使用的TYPEX密码机，如图1.1(b)所示，这种密码机是德国三轮ENIGMA的改进型密码机，它增加了两个转轮使得破译更加困难，在英国密码通信中广泛使用，并帮助英军破译了德军信号。

1944年5月31日，美国海军的一个反潜特遣大队在巡逻中发现了一艘德国的“U-505”型潜艇。6月4日对潜艇发起攻击，深水炸弹很快就将潜艇的外壳炸开了一个大洞，潜艇被迫浮上水面。美军派出海军陆战队员从破洞中钻进潜艇，缴获了德军的现用密码本、加密机及密钥表。和击沉一艘潜艇相比，所缴获的东西重要多了。美军迅速将战利品送到了密码

破译机构那里。由于德国潜艇指挥机构认为“U-505”已被击沉，所以没有更换密码。从此，德国的密码对美军就毫无秘密可言了。据统计，在欧战结束前的11个月里，依靠破译的密码，美军和同盟国军队共击沉德国潜艇三百多艘，平均每天一艘，同时大大减少了自己舰船的损失，对战争的胜利产生了重大影响。

转轮密码机的使用大大提高了密码加密的速度，但由于密钥量有限，二战期间，波兰人和英国人破译了ENIGMA密码，美国密码分析者攻破了日本的RED、ORANGE和PURPLE密码，这对盟军在第二次世界大战中获胜起到了重要作用。

第二次世界大战后，随着电子技术的发展，电子学开始引入到密码机中。第一个电子密码机仅仅是一个转轮机，只是转轮被电子器件所代替。这些电子转轮机的唯一优势在于它们的操作速度，但它们仍然受到机械式转轮机密码周期有限、制造费用高等固有弱点的影响。

近代密码时期可以看作是科学密码学的前夜，这阶段的密码技术可以说是一种艺术，是一种技巧和经验的综合体，但还不是一种科学，密码专家常常是凭直觉和信念来进行密码设计和分析，而不是推理和证明。因此，也有很多学者将古典、近代密码时期划分为一个阶段，即古典密码阶段。

1.2.3 现代密码时期

1949年香农(Claude Shannon)的奠基性论文“保密系统的通信理论”(*Communication Theory of Secrecy System*)在《贝尔系统技术杂志》上发表，首次将信息论引入密码技术的研究，用统计的观点对信源、密码源、密文进行数学描述和定量分析，引入了不确定性、多余度、唯一解距离等安全性测度概念和计算方法，为现代密码学研究与发展奠定了坚实的理论基础，把已有数千年历史的密码技术推向了科学的轨道，使密码学(cryptology)成为一门真正的科学。

从1949年到1967年，密码学文献近乎空白。1967年，戴维·卡恩(David Kahn)出版了一本专著《破译者》(*The CodeBreaker*)，该书对以往的密码学历史作了相当完整的记述，甚至包括政府认为仍然是秘密的一些事情。《破译者》的意义不仅在于记述了1967年之前密码学发展的历史，它使成千上万的人了解了密码学。

实际上，20世纪70年代中期以前的密码学研究和应用主要集中在军事、外交领域，研究工作也大多是秘密进行的，密码学的真正蓬勃发展和广泛应用是从70年代中期开始的。

1977年，美国国家标准局(NBS，即现在的国家标准与技术研究所NIST)正式公布实施了美国的数据加密标准(Data Encryption Standard，DES)，DES被批准用于美国政府非机密单位及商业上的保密通信，并被多个部门和标准化机构采纳为标准，甚至成为事实上的国际标准。更具有重要意义的是DES密码开创了公开全部密码算法的先例，从而揭开了密码学的神秘面纱，大大推动了分组密码理论的发展和技术的应用。

1976年11月，美国斯坦福大学的著名密码学家迪菲(W. Diffie)和赫尔曼(M. Hellman)发表了“密码学新方向”(*New Direction in Cryptography*)一文，首次提出了公钥密码体制的概念和设计思想，开辟了公开密钥密码学的新领域，掀起了公钥密码研究的