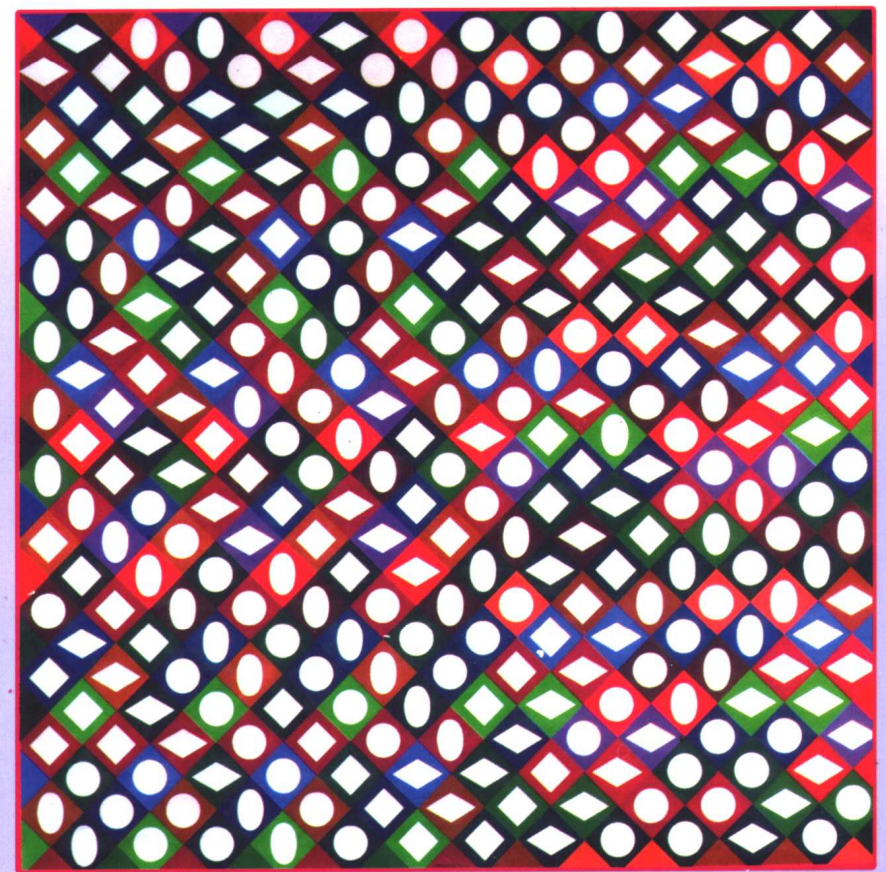
国外著名高等院校
信息科学与技术优秀教材

PEARSON Prentice Hall

密码学概论

Introduction to CRYPTOGRAPHY *with* CODING THEORY



〔美〕Wade Trappe
Lawrence C.Washington 著

邹红霞 许鹏文 李勇奇 译

中文版

人民邮电出版社
POSTS & TELECOM PRESS

国外著名高等院校信息科学与技术优秀教材

密码学概论

[美] Wade Trappe
Lawrence C.Washington 著

邹红霞 许鹏文 李勇奇 译

人民邮电出版社

图书在版编目（CIP）数据

密码学概论/（美）特拉普（Trappe，W.），（美）华盛顿（Washington，L.C.）著；许鹏文，邹红霞，李勇奇译. —北京：人民邮电出版社，2004.6
国外著名高等院校信息科学与技术优秀教材
ISBN 7-115-12184-2

Ⅰ. 密… Ⅱ. ①特… ②华… ③许… ④邹… ⑤李… 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（2004）第 021915 号

版 权 声 明

国外著名高等院校信息科学与技术优秀教材

密码学概论

◆ 著 [美] Wade Trappe Lawrence C.Washington
译 邹红霞 许鹏文 李勇奇
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：21.75
字数：526 千字 2004 年 6 月第 1 版
印数：1-4 000 册 2004 年 6 月北京第 1 次印刷

著作权合同登记 图字：01 - 2002 - 5927 号
ISBN 7-115-12184-2/TP • 3914

定价：38.00 元

本书如有印装质量问题，请与本社联系 电话：（010）67129223

内容提要

本书全面讲解了密码学的基本知识以及相关的基础数论，并对椭圆曲线、量子密码体制等密码学前沿知识进行了介绍。在此基础上，本书对数字签名、数字现金等应用问题作了较为详细的阐述。另外，本书每章都给出了相应的习题，而且在附录中给出了用 Mathematica、Maple 和 MATLAB 实现的相关示例。

本书可供高等院校应用数学、通信和计算机等专业用作密码学、通信安全和网络安全等课程的教材或参考书，也可供信息安全系统设计开发人员、密码学和信息安全爱好者参考。

出版说明

2001年，教育部印发了《关于“十五”期间普通高等教育教材建设与改革的意见》。该文件明确指出，“九五”期间原国家教委在“抓好重点教材，全面提高质量”方针指导下，调动了各方面的积极性，产生了一大批具有改革特色的新教材。然而随着科学技术的飞速发展，目前高校教材建设工作仍滞后于教学改革的实践，一些教材内容陈旧，不能满足按新的专业目录修订的教学计划和课程设置的需要。为此该文件明确强调，要加强国外教材的引进工作。当前，引进的重点是信息科学与技术和生物科学与技术两大学科的教材。要根据专业（课程）建设的需要，通过深入调查、专家论证，引进国外优秀教材。要注意引进教材的系统配套，加强对引进教材的宣传，促进引进教材的使用和推广。

邓小平同志早在1977年就明确指出：“要引进外国教材，吸收外国教材中有益的东西。”随着我国加入WTO，信息产业的国际竞争将日趋激烈，我们必须尽快培养出大批具有国际竞争能力的高水平信息技术人才。教材是一个很关键的问题，国外的一些优秀教材不但内容新，而且还提供了很多新的研究方法和思考方式。引进国外原版教材，可以促进我国教学水平的提高，提高学生的英语水平和学习能力，保证我们培养出的学生具有国际水准。

为了贯彻中央“科教兴国”的方针，配合国内高等教育教材建设的需要，人民邮电出版社约请有关专家反复论证，与国外知名的教材出版公司合作，陆续引进一些信息科学与技术优秀教材。第一批教材针对计算机专业的主干核心课程，是国外著名高等院校所采用的教材，教材的作者都是在相关领域享有盛名的专家教授。这些教材内容新，反映了计算机科学技术的最新发展，对全面提高我国信息科学与技术的教学水平必将起到巨大的推动作用。

出版国外著名高等院校信息科学与技术优秀教材的工作将是一个长期的、坚持不懈的过程，我社网站（www.ptpress.com.cn）上介绍了我们陆续推出的图书的详细情况，敬请关注。希望广大教师和学生将使用中的意见和建议及时反馈给我们，我们将根据您的反馈不断改进我们的工作，推出更多更好的引进版信息科学与技术教材。

人民邮电出版社

前 言

自 1997 年以来，本书一直作为马里兰大学高年级（大三和大四年级）本科生密码学课程的教材。该教材具有如下特点：

- 书中涉及到了最新的技术和广泛的数学基础。
- 未学过数论及计算机程序设计的学生可直接阅读本教材。
- 书中列举了大量的例子来验证算法的实际工作。

本书避免孤立讲述 RSA 算法及大量涉及到数论知识的离散对数等内容，也未提及具体的协议及怎样攻击别人的计算机。本书以描述性为主，涉及少量的数学证明。

该教材全面讲述了密码学的大量基础知识。本书中的许多章节内容超出了一学期的教学内容。前 8 章是课程的基础和核心部分，剩余章节可根据学生的层次选择讲解。

由于教材内容较多，按章节排出了序号，但除了第 3 章讲述的是该课程的基础数论知识以外，其余各章基本上都是独立的，可根据需要自由组织顺序，虽然我们不主张这样。有基础的读者可跳过前 3 章，直接阅读第 4～17 章。

信息论、椭圆曲线、量子密码体制及纠错码这几章比之前几章更趋于数学讨论。纠错码这章列在本教材中是有原因的，因为该章包括了密码术和广泛使用的编码理论。

计算机实例。考虑给出一个 RSA 实例，你可以选择两个 1 位素数，而伪装成用 50 位的素数，或者选择你熟悉的软件包用大的素数来实现实例。也可以考虑采用移位密码，尝试所有 26 个英文字母的各种移位情况，去解密一段消息，显然这需要借助于计算机。本书的最后附上了用 Mathematica、Maple 和 MATLAB 语言写出的程序实例，之所以选择这 3 种语言，是因为它们比较容易且不要求编程人员有很多的编程经验。即使没有计算机上机操作也可以学习该课程，但这些实例作为书中完整的一部分被列出，应该尽可能地学习它们。这些实例不仅包括怎样去实现某个数学示例和计算，而且证明了书中所提出的重要观点和问题。为了保持本书的逻辑性和连续性，我们还在每章的最后给出了用这 3 种语言所

写的计算机实例。

程序源代码可到如下网站下载：

www.prenhall.com/washington

上课讲解时，需将源程序安装至计算机（其中至少要安装一种语言），为保证效果，需要利用投影仪投影程序执行的结果。课后作业（每章后的上机习题）可基于一种软件让学生自己练习。当然，学生也可以选择他们熟悉的程序语言来替代。

致谢。在本书的编写过程中许多人提供了大量的帮助。首先，要感谢我的学生，他们无私地、热情地为本书提出了许多宝贵的意见。我要特别感谢 David Bindel，Jason Ernst，Christine Planchak，Haw-ren Fang，Marwan Oweis，Bob Grafton，他们收集了大量的资料并进行了录入。我的同事 Bill Gasarch 帮助校正了修订版，他的许多建议使我受益匪浅。Jonathan Rosenberg 和 Tim Strobell 提出了相当有价值的技术帮助。另外还要特别感谢 David Grant（Boulder 的 Colorado 大学），David M.Pozar（Amherst，Massachusetts 大学），Jugal K.Kalita（Colorado Springs 的 Colorado 大学）……，他们始终如一地在内容的组织与安排上提出了宝贵的建议。我们也很高兴与 Prentice Hall 的同仁们，特别是数学专家 George Lobell 和应用专家 Jeanne Audinor 的合作。

在此第一作者还要感谢 Nisha Gilra 提供的许多鼓励和宝贵意见，以及 Sheilagh O'Hare 和 K.J.Ray Liu 的支持。

第二作者要感谢 Susan Zengerle 和 Patrick Washington 在成书过程中的耐心、帮助和鼓励。

Wade Trappe

wxt@math.umd.edu

Lawrence C.Washington

lcw@math.umd.edu

目 录

第 1 章 密码学及其应用概述 …… 1

1.1 安全通信 …… 2
1.1.1 可能的攻击 …… 2
1.1.2 对称和公开密钥算法 …… 3
1.1.3 密钥长度 …… 5
1.2 密码学应用 …… 6

第 2 章 古典密码体制 …… 8

2.1 移位密码 …… 8
2.2 仿射密码 …… 9
2.3 Vigenère 密码 …… 11
2.3.1 发现密钥长度 …… 12
2.3.2 发现密钥：第一种方法 …… 13
2.3.3 发现密钥：第二种方法 …… 15
2.4 替换密码 …… 16
2.5 福尔摩斯密码 …… 18
2.6 Playfair 和 ADFGX 密码 …… 21
2.7 分组密码 …… 23
2.8 二进制数和 ASCII …… 26
2.9 一次一密 …… 27
2.10 伪随机序列生成 …… 28
2.11 线性反馈移位寄存序列 …… 30
2.12 Enigma …… 34
2.13 习题 …… 37
2.14 上机题 …… 39

第 3 章 基础数论 …… 42

3.1 基本概念 …… 42
3.1.1 整除 …… 42
3.1.2 素数 …… 43
3.1.3 最大公约数(Greatest Common Divisor) …… 44
3.2 求解 $ax+by=d$ …… 46

3.3 同余 …… 47
3.3.1 除法 …… 49
3.3.2 求 a-1(mod n) …… 50
3.3.3 当 gcd(a, n)=1 时，解 $ax \equiv c \pmod{n}$ …… 50
3.3.4 如果 gcd(a, n)>1 怎么办 …… 50
3.3.5 分数的计算 …… 51
3.4 中国剩余定理 …… 51
3.5 模的幂计算 …… 53
3.6 费尔马小定理和欧拉定理 …… 54
3.7 本原根 …… 56
3.8 模 n 逆矩阵 …… 57
3.9 模 n 平方根 …… 58
3.10 有限域 …… 59
3.10.1 除法 …… 62
3.10.2 LFSR 序列 …… 64
3.11 习题 …… 65
3.12 上机题 …… 67

第 4 章 数据加密标准 …… 69

4.1 概述 …… 69
4.2 一个简单的类 DES 算法 …… 70
4.3 微分密码分析法 …… 72
4.3.1 具有三轮循环的微分密码分析法 …… 73
4.3.2 具有四轮循环的微分密码分析法 …… 75
4.4 DES …… 76
4.5 操作模式 …… 82
4.5.1 电子密码本（ECB） …… 82
4.5.2 密码分组链（CBC） …… 82
4.5.3 密码反馈（CFB） …… 83
4.6 破解 DES …… 84
4.7 口令的安全 …… 87
4.8 习题 …… 88

第 5 章 高级加密标准：Rijndael …… 90

5.1 基本算法 …… 90
5.2 层 …… 91
5.2.1 字节转换 …… 91
5.2.2 移动行变换 …… 92
5.2.3 混合列变换 …… 92

5.2.4 加循环密钥 …… 93
5.2.5 密钥计划表 …… 93
5.2.6 S-盒的构成 …… 94
5.3 解密 …… 94
5.4 设计中要考虑的问题 …… 96

第 6 章 RSA 算法 …… 98

6.1 RSA 算法 …… 98
6.2 对 RSA 的攻击 …… 101
6.3 素数判定 …… 103
6.4 因数分解 …… 106
6.5 RSA 挑战 …… 110
6.6 协议验证上的应用 …… 111
6.7 公钥概念 …… 111
6.8 习题 …… 113
6.9 上机题 …… 115

第 7 章 离散对数 …… 117

7.1 离散对数 …… 117
7.2 离散对数的计算 …… 118
7.2.1 Pohlig-Hellman 算法 …… 118
7.2.2 指数微积分 …… 120
7.2.3 模 4 离散对数的计算 …… 121
7.3 比特约定 …… 122
7.4 ElGamal 公钥体制 …… 123
7.5 习题 …… 124
7.6 上机题 …… 125

第 8 章 数字签名 …… 126

8.1 RSA 签名 …… 126
8.2 ElGamal 签名方案 …… 127
8.3 散列函数 …… 129
8.4 生日攻击 …… 132
8.4.1 签名方案中的生日攻击 …… 133
8.4.2 基于离散对数的生日攻击 …… 133
8.4.3 双重加密的中间相遇攻击 …… 134
8.5 数字签名算法 …… 134
8.6 习题 …… 136
8.7 上机题 …… 137

第 9 章 电子商务与数字现金 …… 139

9.1 安全的电子交易 …… 139
9.2 数字现金 …… 141
9.3 习题 …… 145

第 10 章 秘密共享方案 …… 146

10.1 秘密分拆 …… 146
10.2 门限方案 …… 146
10.3 习题 …… 151
10.4 上机题 …… 152

第 11 章 搏弈 …… 153

11.1 电话掷币 …… 153
11.2 电话扑克 …… 155
11.3 习题 …… 158

第 12 章 零知识证明 …… 159

12.1 基本构成 …… 159
12.2 Feige-Fiat-Shamir 识别方案 …… 161
12.3 习题 …… 162

第 13 章 密钥建立协议 …… 165

13.1 密钥协商协议 …… 165
13.2 密钥预分发 …… 167
13.3 密钥分发 …… 168
13.4 公钥基础设施（PKI） …… 171
13.5 习题 …… 173

第 14 章 信息论 …… 175

14.1 概率回顾 …… 175
14.2 熵 …… 177
14.3 哈夫曼编码 …… 180
14.4 完全保密 …… 181
14.5 英文的熵 …… 183
14.6 习题 …… 187

第 15 章 椭圆曲线 …… 189

15.1 加法定律 …… 189
15.2 模 n 椭圆曲线 …… 192

15.2.1 模 p 点的数目 …… 193
15.2.2 基于椭圆曲线的离散对数 …… 193
15.2.3 表示明文 …… 194
15.3 用椭圆曲线因数分解 …… 194
15.4 特征为 2 的椭圆曲线 …… 197
15.5 椭圆曲线密码体制 …… 199
15.5.1 椭圆曲线 ElGamal 密码体制 …… 199
15.5.2 椭圆曲线 Diffie-Hellman 密钥交换 …… 200
15.5.3 ElGamal 数字签名 …… 200
15.6 习题 …… 201
15.7 上机题 …… 203

第 16 章 纠错码 …… 205

16.1 绪论 …… 205
16.2 纠错码 …… 209
16.3 一般编码的边界条件 …… 212
16.3.1 上边界条件 …… 212
16.3.2 下边界条件 …… 213
16.3.3 例子 …… 215
16.4 线性码 …… 216
16.5 汉明码 …… 221
16.6 Golay 码 …… 222
16.7 循环码 …… 228
16.8 BCH 码 …… 232
16.9 Reed-Solomon 码 …… 237
16.10 McEliece 密码体制 …… 238
16.11 其他问题 …… 240
16.12 习题 …… 241
16.13 上机题 …… 243

第 17 章 密码学中的量子技术 …… 244

17.1 一个量子实验 …… 244
17.2 量子密钥的分发 …… 246
17.3 Shor 算法 …… 248
17.3.1 因数分解 …… 249
17.3.2 离散的傅立叶变换 …… 249
17.3.3 Shor 的算法 …… 251
17.3.4 连分数 …… 254
17.3.5 结束语 …… 255

17.4 习题 …… 255

附录 A Mathematica 实例 …… 257

A.1 Mathematica 入门 …… 257
A.2 部分命令 …… 258
A.3 第 2 章实例 …… 259
A.4 第 3 章实例 …… 265
A.5 第 6 章实例 …… 267
A.6 第 8 章实例 …… 273
A.7 第 10 章实例 …… 273
A.8 第 11 章实例 …… 274
A.9 第 15 章实例 …… 275

附录 B Maple 实例 …… 279

B.1 Maple 入门 …… 279
B.2 部分命令 …… 280
B.3 第 2 章实例 …… 281
B.4 第 3 章实例 …… 286
B.5 第 6 章实例 …… 289
B.6 第 8 章实例 …… 294
B.7 第 10 章实例 …… 294
B.8 第 11 章实例 …… 295
B.9 第 15 章实例 …… 296

附录 C MATLAB 实例 …… 300

C.1 MATLAB 入门 …… 300
C.2 第 2 章实例 …… 304
C.3 第 3 章实例 …… 314
C.4 第 6 章实例 …… 317
C.5 第 8 章实例 …… 321
C.6 第 10 章实例 …… 321
C.7 第 11 章实例 …… 322
C.8 第 15 章实例 …… 324

附录 D 进一步阅读的建议 …… 330

参考文献 …… 331

第1章 密码学及其应用概述

人类一直以来就对保护信息以不被他人所知有强烈的兴趣，孩提时代，我们当中的很多人就梦想有一个魔幻解码环，使我们能够和朋友交换编码信息而不让父母、兄弟姐妹和老师知道。随着历史的发展，已有无数个事例使人们做到了确保秘密的信息不让敌人得知。国王或将军与他们的军队使用加密的方法来传递战时机密情报，以防止敌人窃取。事实上，据说朱丽叶斯·凯撒（Julius Caesar）发明了一种简单的密码，后来该密码就以他的名字命名。

随着社会的发展，人们对更成熟和更完善的保护数据的方法的要求越来越高，在如今的信息时代，这种呼声愈发强烈。因为世界已经相互关联在一起，对信息和电子设施的使用不断增加，由此势必带来对电子系统依赖性的增加。目前已经存在涉及一些敏感信息的交换，比如信用卡在因特网上的使用已相当普遍。有效地保护这些数据和电子系统在我们的生活中已经刻不容缓。

保护数据的方法属于密码学范畴。实际上，该学科包括3个名字：**密码学（cryptography）**、**密码术（cryptology）**和**密码分析学（cryptanalysis）**，这3个名字经常交替使用。从技术上严格来说，密码术是研究在不安全通道传递信息及相关问题的总称，设计体制来完成这些功能的过程叫密码学，密码分析学则涉及到如何破坏这样的体制。当然，目前基本上不存在在密码学和密码分析学两个领域中都可以使用的十分完美的方法。

术语**编码理论（coding theory）**常用来描述密码学，但这经常会导致混淆。编码理论所提到的输入信息符号和输出信息符号叫做编码符号（code symbol）。编码理论覆盖三方面的基本应用：压缩（compression）、保密（secrecy）和纠错（error correction），在过去的几十年里，术语编码理论已几乎成为纠错码的代名词，如此一来，编码理论集中研究的是在噪声信道传输信息及如何确保收到的信息是正确的，而对密码学来说，研究的是如何保证在不安全的通道上安全传输信息。

虽然纠错码不是本书关注的重点，但在这里我们还是应该强调一下，在任何实际系统中，纠错码经常是和加密联系在一起的，因为在一个设计周到的密码体制中，哪怕是一丁点的改变也会完全破坏信息的完整性。

现代密码学领域主要依赖于数学、计算机科学和人的聪明才智。本书介绍了确保数据传输和电子系统安全的数学理论和协议以及其他一些相关技术，如数字签名（electronic signature）和秘密共享（secret sharing）等。

1.1 安全通信

基本的通信方案如图 1.1，它包括两个当事人，我们称为艾丽斯（Alice）和鲍勃（Bob），彼此要进行通信，第三方伊芙（Eve）是一个可能的偷听者。

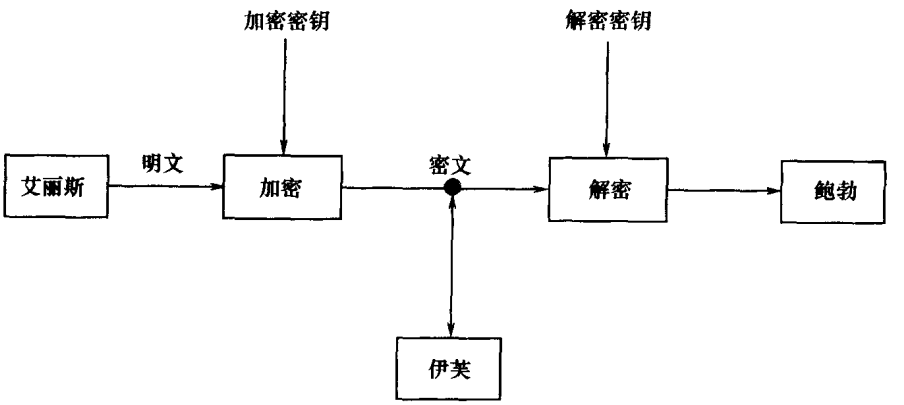


图 1.1 密码学的基本通信方案

当艾丽斯要传递一个消息（称为**明文，plaintext**）给鲍勃时，她使用事先和鲍勃约定好的方法加密要传递的消息，通常，这个加密方法假定伊芙是知道的，保持信息的机密性靠的是**密钥（key）**，当鲍勃收到了这个加过密的消息（称为**密文，ciphertext**）时，他使用解密密钥将消息翻译成明文。

伊芙可能会采取以下某种手段：

1. 读取这个消息。

2. 寻找这个密钥并读取用该密钥解密的所有消息。

3. 中断艾丽斯的消息并用同样的方法改变此消息，使鲍勃认为艾丽斯发送了变换的消息。

4. 伪装成艾丽斯去和鲍勃通信，使鲍勃以为他正和艾丽斯通信。

我们会遇到何种情况取决于伊芙的邪恶程度，步骤（3）和步骤（4）分别涉及的是完整性（integrity）和鉴别（authentication）的问题，这里简单地讨论一下。本书中把更活跃和恶毒的对手称之为马洛里（Mallory），如（3）和（4）所对应的那样，而把被动的观察者称之为奥斯卡（Oscar）如（1）和（2）对应的。我们主要讨论的是伊芙这一方，并假定她尽可能的恶毒。

1.1.1 可能的攻击

伊芙可能采用 4 种主要的攻击手段。它们的主要区别在于，当伊芙想法确定密钥时所能获取的信息数量不同。4 种攻击方式如下：

1. 仅知道密文（ciphertext only）攻击：伊芙仅能得到一份密文的拷贝。

2. 已知明文（known plaintext）攻击：伊芙不仅有一份密文的拷贝还有其对应的明文。

举个例子，假设伊芙中途截获了经加密压缩的密文，第二天又获得了经解密释放过的明文。如果她能推论出密钥，并且假如艾丽斯没有改变这个密钥，那么伊芙就可以阅读以后艾丽斯和鲍勃传递的所有消息。又假如，艾丽斯和鲍勃通信总是以“亲爱的鲍勃”开头，那么伊芙就获得了一小部分密文及其对应的明文，对于大多数较弱的密码体制，这些信息足够用来破译密钥，甚至对功能稍强些的密码体制，如第二次世界大战中德国的“Enigma”机器，这些信息也足以破译密钥了。

3. 选择明文（chosen plaintext）攻击：伊芙临时获取到了加密的机器，她不能打开它去知道密钥；但她可以通过加密大量挑选出的明文，然后试着利用其产生的密文来推测密钥。

4. 选择密文（chosen ciphertext）攻击：伊芙临时获得了用来解密的机器，利用它去“解密”几串符号，并尽可能利用结果推测出密钥。

选择明文攻击可能在如下情况中发生，当要分辨一架飞机是敌还是友时，可以发送一个随机的信息给飞机，然后飞机自动地加密该信息并将它发送回来。友机被认定有正确的密钥，可以用正确的加密信息来比较从飞机传来的信息，如果它们正确，就认为飞机是友机，如果对不上，就认为是敌机。但是，敌机可以利用这一点，发送大量的可选择消息给我方的任意一架飞机，然后查看所得到的密文，假设这样使敌机推测出了密钥，那么敌机就可以伪装成我们的友机。

第二次世界大战时撒哈拉沙漠就出现过已知明文攻击的事例，一个孤独的德国哨兵每天发送同样一条消息说在这儿百无聊赖，当然该消息是用当天的密钥加密过的，这样每天盟军都收到一对明文和密文，这对测定密钥是极为有用的。蒙哥马利将军始终密切关注着这个信息，以确保传递的消息不被遗漏。

现代密码学最重要的假设之一是**克彻霍夫原理（Kerckhoffs's Principle）**：即在评定一个密码体制的安全性时，人们假定攻击方知道所有目前已使用的密码学方法。关于该原理在 1883 年奥古斯特·克彻霍夫（Auguste Kerckhoffs）著名的著作《La Cryptographie Militaire》中有详细论述。攻击方可以通过很多方法获得这些信息。例如，能够捕获和分析加密和解密设备，自己人也可能被发现或逮捕。因此，体制的安全性应该建立在密钥的基础之上，而不是依赖于算法的隐藏。所以我们假定伊芙知道目前已应用的所有加密的运算规则。

1.1.2　对称和公开密钥算法

加密和解密方法分为两类：**对称密钥（symmetric key）**和**公开密钥（public key）**。在对称密钥算法中，艾丽斯和鲍勃双方均知道加密和解密密钥。举一个例子来说，如果双方都知加密密钥，那么很容易从它推出解密密钥。在很多情况下加密密钥和解密密钥是相同的。古典的加密体制（1970 年以前）以及最近的数据加密标准（DES）和 Rijndael（AES）都是基于对称密钥的。

公开密钥是在 20 世纪 70 年代才开始出现，它对传统的密码学提出了根本性的改变。设想艾丽斯希望和鲍勃安全地通信，但是他们相隔上百公里，根本不可能就使用同一个密钥达成一致，看起来似乎也不大可能事先双方约定一个密钥，或委派一个值得信赖的人去传递这

个密钥，当然艾丽斯不能利用公共渠道去传递这个密钥给鲍勃，再利用这个密钥加密消息。令人烦恼的事情终于有了解决办法，即公开密钥加密法。这个密钥是公开的，并且除了鲍勃知道，几乎不可通过计算来发现解密密钥。最流行的算法是 RSA（见第 6 章），它主要基于对大整数因数分解的困难性上，其他的一些算法（见第 7 章和第 16 章）主要有 ElGamal（基于离散对数问题）和 McEliece（基于纠错码）。

这儿用一个非数学的方式来解释公开密钥算法。鲍勃给艾丽斯一个未锁上锁的盒子，艾丽斯将信息放入盒子，用这个锁锁上盒子，然后传给鲍勃，当然只有鲍勃能打开这个盒子并读取信息，先前所提到的公开密钥的方法在数学上就是和该思想联系起来的。很明显，这儿有很多确认的问题需要解决，例如伊芙可能截获第一次的传递，然后换上她自己的锁，这样当艾丽斯传给鲍勃的盒子被伊芙截获后，她就能很轻易地解开锁并读取该信息。这是使用公开密钥体制必然涉及到的一般性问题。

公开密钥加密体制所代表的很可能是密码学有趣的发展历史的最后一步，在早期的密码学中，安全性依赖于加密算法的保密程度，后来假定这些算法已为人所知，加密体制的安全性则依赖于（对称）密钥的保密和不公开。在公开密钥密码学中，算法和加密密钥是公开的，每个人都知道必须做的是寻找解密密钥，这里的安全性依赖（或希望）的是不可能通过计算获取解密密钥。看起来相当荒谬的是，一方面多年来加密算法大量出现，而另一方面对手也获取了更多关于这些算法的信息。

公开密钥方法功能相当强大，似乎它的强大使对称密钥方法成为过时，但是，它所带来的是不自由和计算的代价，在公开密钥算法中所需要的计算量比一般的加密算法如 DES 或 Rijndael 计算量多几个幂的数量级。一个重要的原则是公开密钥不要使用在数据量相当大的加密中，基于此原因，公开密钥一般应用在仅有少量数据需要传输的情况下（如数字签名、传送对称密钥算法中的密钥等）。

在对称密钥密码学中，有两种类型的密码：连续密码（stream cipher）和分组密码（block cipher）。连续密码中，输入到算法中的数据是小的段（比特或字节），而输出结果是其相对应的小段；而分组密码中，输入的是一组比特，相应的输出也是一组比特流。在 2.11 节中我们将讨论关于连续密码的例子，即线性反馈移位寄存器（linear feedback shift register）。我们关注的绝大部分情况是分组密码，为此将介绍两个非常重要的例子，第一个是 DES，第二个是 Rijndael，它在 2000 年被国际标准和技术委员会选中以取代 DES。公开密钥方法如 RSA 也被认为是分组密码。

最后，我们介绍一下两种不同类型的加密即**编码（code）**和**密码（cipher）**在历史上的差别，对于编码，它可用码字（codeword）代替（可以是一串符号），如第一次世界大战中英国海军使用 03680C，36276C 和 50302C 来代表“shipped at”、“shipped by”和“shipped from”。编码有对那些无明确意义的单词无法使用的缺点。反之对于密码来说，不必担心消息语言上的结构，而可以加密每一串字符，不管它代表的是有意义或没意义还是其他什么，因而密码比编码更通用。在早期的密码学中经常使用编码一词，有时相对应地使用密码，直到今天仍然还是这样使用，隐蔽的行动经常用密码，但无论如何，任何秘密要想安全传输都需要用密码加密。在本书中，我们一律使用密码。