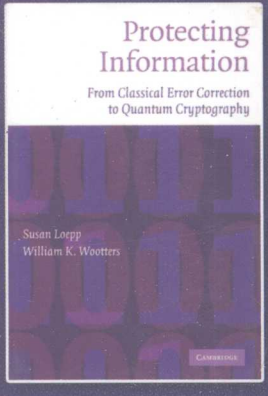
CAMBRIDGE

信息保护：从经典纠错到量子密码

Protecting Information

From Classical Error Correction to Quantum Cryptography



[美] Susan Loepp
William K. Wootters 著

吕欣 马智 许亚杰 译

冯登国 审校

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息保护：从经典纠错到量子密码

Protecting Information: From Classical Error Correction to Quantum Cryptography

[美] Susan Loepp
William K.Wootters [著]
吕 欣 马 智 许亚杰 译
冯登国 审校

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

内 容 简 介

本书以密码学和量子物理为切入点，深入介绍了量子密码和量子纠错码的主要思想和方法。针对密码学和编码学，分别从经典信息学和量子信息学两个角度进行了讨论和比较分析，重点介绍了量子密码和量子纠错码的基础理论和研究进展。主要内容包括：密码学绪论；量子力学；量子密码；纠错码介绍；量子密码的深入探讨；推广的 RS 码；量子计算等。本书可以作为计算机、通信、信息安全、密码学、数学、物理学等专业研究生和本科生的教材，也可供从事相关专业的教学、科研人员参考使用。

Protecting Information:From Classical Error Correction to Quantum Cryptography first edition (ISBN: 0521534763) by Susan Loepp, William K.Wootters first published by Cambridge University Press 2006

All rights reserved.
This simplified Chinese edition for the People's Republic of China is published by arrangement with the Press Syndicate of the University of Cambridge, Cambridge, United Kingdom.
©Publishing House of Electronics Industry & Cambridge University Press 2008

This book is in copyright. No reproduction of any part may take place without the written permission of Cambridge University Press.
This edition is for sale in the mainland of China only, excluding Hong Kong SAR, Macao SAR and Taiwan, and may not be bought for export therefrom.
此版本仅限在中国大陆销售（不包括中国香港、澳门特别行政区及台湾）。不得出口。
版权贸易合同登记号　图字：01-2007-6080

图书在版编目（CIP）数据

信息保护：从经典纠错到量子密码/（美）楼坡（Loepp,S.），（美）伍特斯（Wootters,W.）著. 吕欣，马智，许亚杰译. —北京：电子工业出版社，2008.9
ISBN 978-7-121-06856-0

Ⅰ. 信…　Ⅱ.①楼…②伍…③吕…④马…⑤许…　Ⅲ. ①信息系统—安全技术—研究 ②量子—密码—研究　Ⅳ. TP309　TN918.1

中国版本图书馆 CIP 数据核字（2008）第 081702 号

责任编辑：董亚峰
印　　刷：北京机工印刷厂
装　　订：三河市鹏成印业有限公司
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：720×1 000　1/16　印张：15.5　字数：384 千字
印　　次：2008 年 9 月第 1 次印刷
印　　数：4 000 册　　定价：36.00 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。

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。

服务热线：（010）88258888。

序

对于许多日常传输任务来说，保护数字信息免受噪声干扰和窃听是非常重要的。这本介绍纠错编码和密码学的书，用几个重要章节介绍量子密码和量子计算的基础理论，为数学和物理思想的交融提供了一个良好的平台。本书通过对 Shor 量子因子分解算法等内容的阐述，将当前量子信息理论的基本观点传递给读者，并启发式地展现了数学与科学间的奇妙关系。

特别有趣的问题是量子物理对密码学带来的潜在影响：①如果能成功制造出一台量子计算机，就能破解我们当前使用的公钥密码系统；②量子密码在未来有望替代这种不能抵抗量子算法攻击的密码体系，这是建立在自然法则基础之上，而非基于计算复杂性理论。

读者即使不懂量子力学，只要具备基本的复数、向量空间和矩阵的知识，都可以读懂本书，并从中受益。

Susan Loepp 是威廉姆斯（Williams）大学数学和统计系的一位数学专业副教授。她的主要研究兴趣是交换代数，特别是基于环上的交换代数。

William K.Wootters 是美国物理学会的会员，威廉姆斯大学物理系的自然哲学教授。他主要研究量子纠缠及量子信息的有关理论。

作者将密码学和编码学这两个热门学科融合在一起，并利用经典与量子等计算和通信模型分别对其进行观察和讨论。这些引人入胜的内容通过代数结构和相关技巧的逐步展开而有机地结合在一起。通过学习，学生将会在群、有限域和向量空间的理论及它们的具体应用上，有更为开阔的思路。

Ben Lotto，瓦萨尔 Vassar 学院

译 者 序

21 世纪，信息空间的开发、利用和对抗无疑成为各国科技发展的战略高点。近年来，量子信息技术的快速发展拓宽了信息理论的研究内容，也给信息科学研究带来了新的机遇与挑战。

纠错编码和密码学是信息科学中两个重要的研究分支。纠错编码的主要任务是通过增加信息冗余度的方法，排除在噪声信道下传输消息时受到的干扰。而密码学是研究在通信中，通过人为地置乱消息或添加噪声，使得非法窃听者无法获取消息。

本书从数学和物理两个角度介绍了量子密码、量子纠错码和量子计算，并与经典密码学和经典纠错方法进行了比较分析。在量子密码方面，主要介绍了量子密钥分配协议及其安全性证明的方法，接着从纠错码基础理论、广义 Reed-Solomon 码，逐层深入到量子纠错和量子计算。本书知识由浅入深，是信息安全相关专业的科研人员和学生学习量子密码及量子信息的好教材。阅读本书并不要求具备物理专业的背景知识，但要求具备线性代数、向量空间等基础知识。

我们在自然科学基金项目“量子密码协议与量子纠错码研究”的研究过程中发现了本书，并愈加认识到本书对学习和掌握量子密码及量子编码的重要意义，也深感翻译本书十分必要。因此，在电子工业出版社的大力支持下完成了本书的翻译。尽管翻译组的同志们付出了大量努力，反复讨论、认真校正，但基于水平限制，一定还存在一些不当之处，欢迎广大读者批评指正！

感谢何德全院士和国家信息中心有关领导对本书翻译工作给予的支持。

感谢冯登国研究员百忙之中审阅了全书译稿，并提出了宝贵的建议。

中国科学院高能物理研究所刘蕾博士，信息工程大学杨新元硕士参加了本书部分章节的翻译工作，中国科学院信息安全国家重点实验室的张雅哲博士参加了本书的校对工作。没有他们的鼎力相助，本书的翻译和审校工作不可能进行得如此顺利，对他们的工作表示衷心的感谢。

本书的翻译工作得到了电子工业出版社董亚峰编辑的大力帮助，在此表示诚挚的谢意。

本书所涉及的字母、公式和人名等，均沿用原著表示方法。

译者

2008 年 6 月

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

在进入信息时代的近几十年里，信息通信在我们的日常生活中变得越来越重要，因此，保护信息传输不被窃听（例如，人们在互联网上发送信用卡信息时）和噪声干扰（可能发生在蜂窝电话通话中或当磁盘偶尔被刮伤时）变得十分重要。虽然我们中的大多数人都在用各种手段来保护我们的信息，但是却很少有人知道这些保护方式是如何运作的。本书目的之一是向广大读者介绍关于信息保护方面的基础知识。

除在现实生活中的重要意义之外，信息保护本身就与数学、计算机科学，甚至还有物理学等很多学科密切相关。再加上它对社会所具有的重要意义，这门学科可以说是上述所有学科思想的完美融合。介绍这门学科的多学科性是我们编写这本书的动机之一，我们希望对读者而言，它也具有同样的吸引力。

在关于编码学或密码学方面的章节中，本书的特色在于与量子物理学以及正在兴起的量子信息技术的有机结合。在量子密码体制中，窃听者的存在不可避免地会导致量子信号的扰动，从而可以被通信双方发现。这个发现20世纪80年代被提出之后，在世界上许多实验室得到了不断的研究和发展。虽然它看上去仍是在未来才可能被广泛应用的一种技术，但其实已经离我们不远了。事实上，一些公司已经在出售针对特定应用范围的量子密码系统了。量子信息技术的另一个潜在应用是量子计算，它离现实要更加遥远，大多数专家认为制造出完全意义上的量子计算机至少还需要几十年的时间，但是由于量子计算机拥有巨大的潜力，研究者们正在夜以继日地研究。我们关心的是，量子计算机的出现将会导致现在被广泛应用于互联网通信标准等领域的所有公钥密码系统的失效。实际上，量子计算机对传统密码学的这种威胁正是促进量子密码学不断发展的原动力之一。

因此，本书将重点围绕两方面内容来展开讨论。首先，促使我们实施信息保护的两个原因：防止窃听和防止噪声干扰。其次，我们可以展开研究的两个领域：经典领域和量子领域。本书的大多数章节将主要就其中某一方面的某一个问题展开讨论，但就整体而言，还是旨在将这些不同方面的知识互相补充和加强。因此，本书中数学和物理学的知识在某种程度上是交织在一起的，虽然不是完全融合，却是以一种比较理想的方式联系在一起。

本书是在给几届数学、物理学和计算机科学专业的大学生讲课的基础上形成的。读者需要具有一定程度的数学知识，线性代数的知识尤其重要，但对物理学的知识不做特别要求。基于对本书读者群的定位，作者更

注重于介绍量子力学的数学结构，而不是它与物理学其他理论的联系，尽管书中会涉及一些物理学味道非常浓的术语，如“电场”（Electric field）和“夸克”（quark）等。本书中每节末尾的大多数习题难度适中，都已在课堂中使用过，但还是有一些没有测试过的习题，需要使用本书的老师和学生重点关注。

本书第 1 章对密码学的思想进行了选择性的概述，由浅入深逐步介绍了模运算的知识，最后介绍了关于群论和椭圆曲线理论的知识。量子密码学需要一些量子物理学的概念，因此在介绍量子密码学之前，在第 2 章中介绍了关于量子物理学的知识。从设想一些简单的实验入手，包括光量子的极化等，而不是完整地介绍整个量子力学体系。第 2 章所介绍的知识将使读者有足够的基础进行后续的关于量子密码学、量子计算以及量子纠错码基础理论的学习（如果想略过量子纠错码部分，本章最后一节可以不看）。

有了量子物理学的基础知识，第 3 章中介绍量子密码学，重点将放在已经被广泛研究的量子密钥分配上。量子密钥分配促进了量子力学的其他应用发展：不可克隆定理和量子远程传态，这些内容也将在第 3 章中涉及。但是到此为止，读者还不能够完全理解量子密钥分配协议，这需要对经典领域有进一步的了解，这就引出了第 4 章的经典纠错码理论。在第 2 章中主要的数学思想围绕在复数域的向量空间上，而在第 4 章中主要的数学思想将围绕在 $\mathbb{Z}_p$ 的向量空间上，这里 p 是一个素数。在具备了生成矩阵、校验矩阵和校验子译码（Syndrome Decoding）的知识后，在第 5 章中完成对量子密钥分配协议的讨论，然后在第 6 章中运用 $\mathbb{Z}_p$ 和其他有限域的知识来研究 Reed-Solomon 码理论。

本书最后一章属于量子世界。首先用足够的量子计算理论来描述量子因子分解算法，正是它威胁到了第 1 章中所提到的公钥密码体制；最后指出在原理上如何才能保护量子信息免受噪声干扰。

本书没有涉及的知识也有很多，比较重要的有信息论和熵理论的全部知识，包括像关于纠错的基本限制等。有很多关于这方面的好书籍，同本书结合起来学习，将会起到非常好的效果（就经验来看，本书中所介绍的内容已经足够学生使用了）。然而本书并不打算像其他一样给出一个完整的书目，而是会尝试通过脚注等方式来提供足够的资源，帮助有志于更进一步深入学习的读者，为此，本书还提供了获得这些资源所必需的背景知识。

希望这本书能够促进数学和物理学之间的联系，使它们在当前以及未来的信息技术领域里扮演更加重要的角色。

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888
传　　真：（010）88254397
E-mail：　dbqq@phei.com.cn
通信地址：北京市万寿路 173 信箱
　　电子工业出版社总编办公室
邮　　编：100036

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章　密码学：绪论

1.1　初等密码

密码编码（Cryptography）是设计和使用通信方案对除目标接收者之外的所有人员隐藏消息含义的学科。密码分析（Cryptanalysis）则是用来破译加密系统和破解加密代码的学科。对密码编码和密码分析的研究统称为密码学（Cryptology），这是本章讨论的重点[1]。后面将学习一些相当高深且复杂的密码系统，但是先从一些基本的例子谈起。

1.1.1　替换密码

替换密码（Substitution Ciphers）是一类为大家所熟知的加密方案，读者可能会从周末报纸（Sunday Newspaper）的猜字游戏中找到类似的方法，它是用字母表中的一个字母替代另外一个字母。一个特殊例子就是恺撒密码（Caesar Cipher），它将字母表中的每一个字母推移若干位。在朱利斯·恺撒（Julius Caesar）使用的版本中，字母表向前推移三个位置。例如，如果原始消息的一个字母或明文（Plaintext）是 A，则相应的加密消息字母或者密文（Cyphertext）就是 D，以此类推可将明、密文间的对应关系表示如下。

明文：$A\quad B\quad C\ldots X\quad Y\quad Z$

密文：$D\quad E\quad F\ldots A\quad B\quad C$

我们用数学语言来表述这个密码，给每个字母赋一个数：$A\rightarrow 0$，$B\rightarrow 1$，…，$Z\rightarrow 25$。如果 x 代表一个明文字母，y 代表相应的密文字母，朱利斯·恺撒密文可以表示为

$$y = x + 3 \ (\mathrm{mod}\ 26),$$

这里“(mod 26)”表示被 26 除的余数（在本章的后面几节中很多地方用

[1] 对密码编码和密码分析的简洁概括，包括一些实践问题，见 Piper 和 Murphy（2002）。更多数学化的信息理论方案在 Welsh（1988）中给出。历史上流行的说法见 Singh（1999）。更彻底的历史回顾见 Kahn（1967）。

到模运算）。如果理解了破解周末报纸上的替换密码的原理，将会发现恺撒能够用这种简单的策略保护任何秘密信息，事实证明的确如此。

恺撒密码的一般形式可以简单地表示为等式 $y = ax + b \pmod{26}$，这里 a 和 b 都是整数[2]。讨论 a 和 b 取什么值更好是一个很有趣的问题，这将留作本节后的一个练习。更一般化的加密方式是使用字母表的任意置换。

怎样才能破解替换密码呢？一般是利用今天大家所熟知的频率分析方法，这种技术在罗马统治时期是没有的。假定密码分析者知道明文使用什么语言，假设明文就是英语，在典型的英语文章里，每个字母出现的频率是一定的。在英语里最常见的字母是 E，如果你闭着眼睛在一本小说里的一页上随意指定一个字母，字母是 E 的概率是 12.7%左右。表 1.1 给出了所有英文字母出现的频率，这是对从报纸和小说中随机选取的 300 000 个字符进行统计所得到的结果[3]。

表 1.1　英文字母出现的概率表

E	12.7%	D	4.2%	P	1.9%
T	9.0%	L	4.0%	B	1.5%
A	8.2%	U	2.8 %	V	1.0%
O	7.5%	C	2.8%	K	0.8%
I	7.0%	M	2.4%	Q	0.1%
N	6.7%	W	2.4%	X	0.1%
S	6.3%	F	2.2%	J	0.1%
H	6.1%	G	2.0%	Z	0.1%
R	6.0%	Y	2.0%		

利用表 1.1 可以使用如下方法来破解替换密码。给定密文后，计算每个字母出现的频率。如果消息足够长，字母出现的频率将帮助我们猜出每个密文字母所代表的明文字母。例如，如果字母 v 出现的频率是 13%左右，我们猜测字母 v 代表字母 e。一旦猜出几个正确的字母，就继续找熟悉的单词，这样下去就可以得到所有明文。相关的技术可以用在经常一起出现的成对字母上。本节后的一些题目将让读者练习频率分析方法。

[2] 对于 a=1 和 b=3 的特殊情况，我们称为 “ROT13”，当前被用于在线隐藏一些妙语和猜字游戏的答案等信息。

[3] Piper 和 Murphy（2002）。作者这里引用的这张表格最初是由 H.J.Beker 和 F.C.Piper 编辑的。

1.1.2　维吉尼亚密码

现在介绍一种比简单替换复杂的密码。该密码是 Giovan Batista Belaso 在 16 世纪发明的，但是后来被人们错误地归功于维吉尼亚（Blaise de Vigenère），并以他的名字命名（维吉尼亚在这种密码里发明了一种很有效的变换，即用消息本身来产生密钥）[4]。在这种情况下秘密密钥就是一个单词或者一个短语。很容易通过一个例子来解释这种密码，例如，要发送的消息是“Meet me at midnight”，密钥是“quantum”（该密钥是 Belaso 或者 Vigenère 当时不可能使用过的密钥）。

明文：　M E E T M E A T M I D N I G H T
密钥：　Q U A N T U M Q U A N T U M Q U
密文：　C Y E G F Y M J G I Q G C S X N

为生成密文，与前面讲到的方法类似，将每一个字母赋予一个整数值：$A \rightarrow 0$，$B \rightarrow 1$，…，并把上面的每一列明文字母和密钥字母对应的整数执行模 26 加运算。例如，第一个密文字母可以按如下方法得到：

$$M + Q \rightarrow 12 + 16 \ (\mathrm{mod}\ 26) = 2 \rightarrow C$$

换句话说，这种方式是用恺撒密码加密每一个字母，加密方法采用字母表的循环平移，但是不同的字母要被平移不同的位数。在上面的例子里，六种不同的恺撒密码通过间隔七个字母的方式被重复使用。接收者应该知道密钥，并且用每一个密文字母减去相应的密钥字母来恢复出明文。

注意这种密码与简单的替换密码方案相比，有以下改进。字母“M”在明文中出现了三次，每一次也加密的结果都是不同的；另一方面，字母“G”在密文中出现了三次，但是每一次代表了不同的明文字母。因此如果直接使用频率分析方法，它不会像破解简单的替换密码那样有效。

然而，如果消息足够长，则仍然能够使用频率分析来破解这种密码。假设密码分析者总能正确地猜出重复密钥的长度，与上面的例子一样，不妨设密钥长度为 7，那么每隔七个字母用相同的恺撒密码加密，而每一种恺撒密码又可以通过分析密文出现的频率来破解它。因此一旦知道了密钥的长度，破解密文就变得简单了。但是密码分析者怎样才能猜出密钥的长度呢？一种方法是寻找重复的字符串。例如，一段较长的消息中单词

[4] Belaso 的密码与前人设计的密码密切相关。详细说明见 Kahn（1967）。

“the”将极有可能以同样的方式被加密若干次，因而将产生几次同样的三字母序列。所以，假如密码分析者看到了三个“rqv”，第二个“rqv”距第一个21步，第三个距第二个56步，密码分析者就有理由猜测重复密钥是7个字母长，因为7是唯一可以整除21和56的正整数因子（除了1）。当然，因为密文中的字符串偶尔重复的可能性是很大的，如果能发现更多这样的重复，这样的假设会更可信。这种破解维吉尼亚密码的方法是在19世纪被Friedrich Kasiski发现。

另外一类维吉尼亚密码使用变化的密钥（Running Key）而不是重复的密钥。这种变化的密钥通常是容易获得的文本，其长度至少与消息长度一样。比如可以使用从导言开始的美国宪法作为密钥。那么可以这样加密“Meet me at midnight”：

明文：　M E E T M E A T M I D N I G H T

密钥：　W E T H E P E O P L E O F T H E

密文：　I I X A Q T E H B T H B N Z O X

解密也很简单，知道密钥的话，用密文字母逐个减去密钥字母就能恢复原始消息。

很显然，之前所描述的密码分析方法并不能破解这种加密方案，因为密钥不再是周期性的。但是即使采用这种变化的密钥，其密钥自身也同样具有某种结构性，密码分析者可以利用其结构性在恢复明文过程中有所突破。例如，如果密码分析者怀疑密钥是一篇英文文章，并且能猜出单词“the”出现的频率，那么就能用“the”作为密钥的一部分，在密文的各个位置试验，观察试验的结果作为消息的一部分是否有意义。在上面的例子中试用这种方法，把THE铺在密文的各个位置上，如表1.2所示。

表1.2　假设“the”作为密钥的一部分

密文中的三字符串	三字符串减THE
IIX	PBT
IXA	PQW
XAQ	ETM
AQT	HJP
⋮	⋮
ZQX	GHT

表1.2中右侧的多数三字符串不可能作为英文消息的一部分，事实上只有“ETM”和“GHT”可以作为候选对象。如果是后者，可能会对解

密极有帮助，因为在英语里仅有少数字母组合可能出现在“GHT”之前。密码分析者经过多次猜测，分析密钥可能会含有哪些词，表 1.3 列出了可能的发现。

表 1.3　可能的字母组合

猜测的明文	密文减明文=密钥
OUGHT	NTTHE
NIGHT	OFTHE
FIGHT	WFTHE
RIGHT	KFTHE
LIGHT	QFTHE
EIGHT	XFTHE

在所有猜测的密钥中，只有前两个作为消息的一部分在英语里是有意义的，第二个可能性更大。因此密码分析者会暂时猜测“NIGHT”是明文的一部分，“OFTHE”是密钥的一部分。继续这样做下去，不断地对未破解的明密文进行分析，就有可能破解这种密码。

1.1.3　一次一密

即使在前面例子中使用了变化的密钥，维吉尼亚密码仍有不安全的本质，因为密钥所具有的某种结构性能够被密码分析者所利用，如果密钥是一篇英文文章，但英文有其本身的结构。自然地，避免这个问题的方法是使用变化的、纯粹由随机字母组成的密钥。下面的例子用到的密钥是通过投币逐个生成的。

明文：　M E E T M E A T M I D N I G H T
密钥：　P O V N H U J B K R C J D C O F
密文：　B S Z G T Y J U W Z F W L I V Y

当然，要破解密文，接收者必须也有一份相同的随机密钥。

在这个例子里，即使明文中存在很多结构，密钥的随机性（如果密钥是真正随机的）也能保证密文不会存在任何结构。因此这种密码编码方案是不可破解的[5]（虽然窃听者可能采用其他攻击方法，如在密钥传送给接收者的途中截取密钥）。假设随机密钥的长度至少和消息一样长，这样的

[5] 这种说法的准确表述已被香农 Shannon(1949)证明。

密钥就是不重复的。另外值得注意的是，为了保证绝对安全，密钥只能使用一次。如果同一密钥被使用了两次，攻击者就可以通过分析比较这两次的密文来寻求攻击的方法。只使用一次的随机密钥被称做一次一密（One-time Pad），是指密钥被复制在便笺薄上交给接收者，使用一次后将其销毁。

今天，许多信息以数字的形式从一个地方传送到另一个地方，而信息可以表示为 0 和 1 的序列。一次一密在这方面有很好的应用，因为在这种情况下，密钥是随机的二进制序列。例如，下面是对一条二进制消息的一次一密加密（同样，这里所用的密钥也是一个均匀的投币序列）。

明文：　0　1　0　1　0　1　0　1　0　1　0　1　0　1　0　1

密钥：　1　0　0　1　0　0　1　0　0　1　0　0　0　0　1　1

密文：　1　1　0　0　0　1　1　1　0　0　0　1　0　1　1　0

在每一列有两个输入，一个是明文，一个是密钥，两者进行模 2 加运算，也就是说，普通加法的结果除以 2 所得的余数即为密文，如 $1+1 \pmod 2 = 0$。

虽然一次一密对于密码分析来说是绝对安全的，但是它不可能广泛地应用于密码编码，因为对于此种加密方案而言，生成并且安全传输随机密钥的费用不会小于，甚至会大于传输消息本身所需要的费用。如果消息传输量很大，那么消息发送者将不得不雇用一群可靠的送信人专门传递密钥。

本书的后面部分会详细地论述最近出现的一种新方案，即量子密钥分配，它有能力通过自然规律而不是数学定理解决这个问题。对量子密钥分配的研究将在第 2 章引入相关的定理后再做介绍。

练习

1．替换密码中每一个明文字母可以用一个整数 x 代表，密文字母可以用相应的整数 $y = ax + b \pmod{26}$ 代表，这里 a 和 b 是整数。如果使用含有 n 个字母的字母表，这里 n 不一定是 26，定义 $y = ax + b \pmod n$，这里“mod n”意思是取被 n 除的余数。请回答下列问题，假定整数 a 和 b 取 0，…，$n-1$ 中的某个值。

（a）假定 n 取 26，如果明文是英文，并且不对空格或标点符号加密。是否有理由说明常量 a 或者常量 b 不能取某个特定值？如果是，哪些值不好？原因何在？

此为试读，需要完整PDF请访问：www.ertongbook.com