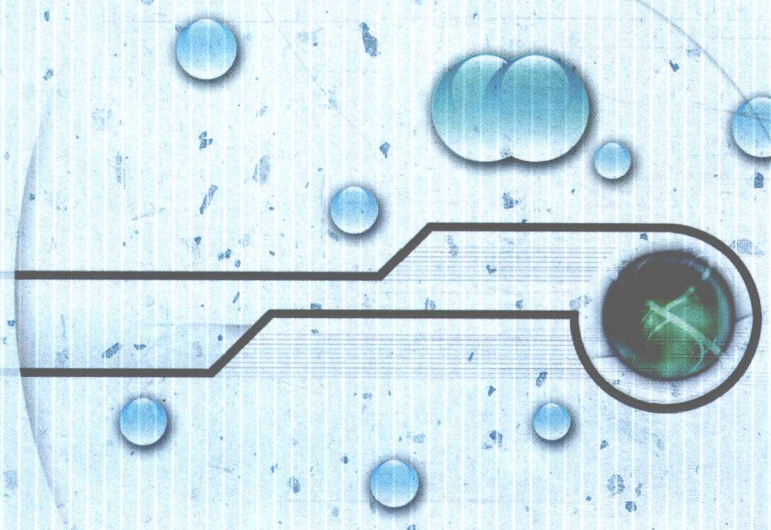
国防特色学术专著·信息与通信技术



量子保密通信引论

LIANGZI BAOMI TONGXIN YINLUN

陈 晖 祝世雄 朱甫臣 著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS
北京航空航天大学出版社 哈尔滨工程大学出版社
哈尔滨工业大学出版社 西北工业大学出版社

国防特色学术专著·信息与通信技术

量子保密通信引论

陈　晖　祝世雄　朱甫臣　著

北京理工大学出版社
北京航空航天大学出版社　哈尔滨工程大学出版社
哈尔滨工业大学出版社　西北工业大学出版社

内容简介

本书从应用的角度出发，使用通俗的表达方式，系统地论述了量子保密通信的基本原理、体系结构、系统实现等，并探讨了量子保密通信技术在国防领域内的重要应用前景。

全书共六章，主要内容包括保密通信概述、量子信息技术基础、量子密钥管理技术、量子保密通信体制、量子保密通信系统工程和量子保密通信与信息安全等。

本书内容深入浅出、层次分明、通俗易懂，可作为信息安全、密码学、通信和光通信、量子光学应用等相关学科的科研和工程技术人员的参考书，也可作为相关专业高等学校师生的参考书。

图书在版编目(CIP)数据

量子保密通信引论/陈晖，祝世雄，朱甫臣著．—北京：北京理工大学出版社，2010.1
(国防特色学术专著．信息与通信技术)
ISBN 978-7-5640-2928-9

Ⅰ．量… Ⅱ．①陈…②祝…③朱… Ⅲ．量子力学-保密通信 Ⅳ．O413.1
TN918

中国版本图书馆 CIP 数据核字(2009)第 217460 号

量子保密通信引论

陈 晖 祝世雄 朱甫臣 著
责任编辑 刘小亦

*

北京理工大学出版社出版发行
北京市海淀区中关村南大街 5 号(100081) 发行部电话：010-68944990 传真：010-68944450
http://www.bitpress.com.cn
北京圣瑞伦印刷厂印刷 全国各地新华书店经销

*

开本：787 毫米×1092 毫米 1/16 印张：11.25 字数：260 千字
2010 年 1 月第 1 版 2010 年 1 月第 1 次印刷 印数：1～3000 册
ISBN 978-7-5640-2928-9 定价：38.00 元

前　言

在信息技术快速发展的今天，信息安全已不再是单纯的通信保密，而是一个涉及数学、物理、生物、化学、信息论、计算机和通信技术等诸多学科知识的综合学科，是一个融合信息的保密性、完整性、可用性、可控性和不可否认性为一体的综合体系，然而，对于长期困扰信息安全的完全保密、身份识别和窃听检测等问题并未得到彻底解决。又因为在经典领域不可能有天然的保密信道，也很难实时发现各种入侵攻击，所有这些问题的彻底解决都需要新的保密通信技术。

近年来，随着人们对量子计算和量子信息的深入研究以及对信息系统安全需求的快速增长，科学家们发现了量子现象在信息科学中的许多新的应用，由于量子信息技术在提高信息处理速度、确保信息安全、增大信息容量和提高检测精度等方面有着经典信息技术无法比拟的潜在技术优势，得到了快速发展并且得到了广泛关注。研究表明，完全保密的、物理安全的保密通信技术——量子密钥分发(QKD)将是最可能首先投入使用的量子信息技术。

为什么要研究量子密钥分发？为什么要研究量子保密通信？量子通信能否突破经典通信的距离和速率极限？假如到2030年左右，量子计算机研究取得重大突破并开始投入使用，256比特密钥的对称密码算法将不安全，RSA等非对称密码算法也将不安全！经典密码体制已经不能为信息系统提供安全性保证的情况下，人们如何保护他们的通信安全，国家又如何保护国防、军事、金融等重要领域内的信息安全？这是本书力求回答的主要问题。

根据经典信息论原理，如果随机密钥的在线安全分发问题能够得到有效解决，那么利用一次一密乱码本就可以解决数据传输的完全保密问题；但是大量随机密钥的高速在线分发面临着一系列技术难题或者技术瓶颈(比如，为了确保密钥的安全，需要采用复杂的加密手段和安全协议，从而限制了密钥分发的速率；另外，密钥的保护措施也得不到完备性证明)。而QKD可以解决随机密钥的高速在线保密分发问题，为一次一密乱码本的广泛应用提供了技术可能性，进而可以解决数据传输的完全保密问题。基于这样一个特点，QKD受到了许多国家的高度关注并得到了快速发展。但是QKD只是解决经典保密通信的在线密钥分发问题，是对经典保密通信技术的某种改进，而并没有从根本上解决保密通信的其他核心问题，比如身份识别、本地数据的保密存储等。不过，毋庸置疑，QKD作为一个物理上安全的保密体制，它的实用化已是一个明显的趋势。2004年，中国的华东师范大学实现了QKD原理样机，同年美国BBN公司建立了世界上第一个量子保密通信网络。2005年，瑞士IDQuantique公司和美国MagiQ公司都推出了第

二代商用 QKD 系统产品。目前这种商用的量子密钥分发系统，使用标准光纤，可以在长达 100 km 的距离上进行点到点的量子密钥分发，密钥比特率可以达到 1000 bit/s。2008 年，欧盟 SECOQC 组建了一个 7 节点的量子保密通信演示网络。2009 年，中国建设了一个 5 节点的“量子政务网”。由此可见，国内外对量子密钥分发技术的研究已经进入了工程实现的关键时期，可以预见在最近几年内量子密钥分发系统将应用于实际的保密通信系统中。

作为一项前沿综合交叉技术学科，量子信息理论所依赖的量子力学和信息理论都具有相当的难度，对一些与量子保密通信息息相关的问题，诸如“量子信道是保密的吗？量子密钥分发能够解决量子信息的完全保密问题吗？量子保密通信的核心问题是什么？量子保密通信需要使用量子信息加密技术吗？”等，要使非相关专业的学者和研究人员对之形成一个比较全面的认识还有大量的工作要做。目前，在量子信道上进行安全的量子密钥分发已经接近实用，但这并不意味着量子通信是绝对安全的，更不能说明可以把量子信道作为天然的保密信道来直接进行明文信息的保密通信。否则，量子密钥分发就没有任何意义！因为如果存在一个天然的保密信道，就没有必要再使用密钥来保护数据。目前所谓的“量子密码”并不是真正地对量子信息进行加、解密处理的技术，而更多情况下是指基于量子密钥分发技术的相关应用（比如，基于量子密钥的一次一密乱码本），因为加密信息并不是通过量子信道传输的。

为了系统地解答量子保密通信的一些基本技术问题，本书避开一些复杂的基础理论论述，从应用的角度出发，使用通俗的表达方式，深入地论述了量子信息与经典信息的内在区别和联系，量子保密通信的基本原理、体系结构、信号处理、信号传输、通信协议、系统实现原理和特色，探讨了量子保密通信技术在国防、军事等重要领域内的应用前景，其中融合了近十年来我们进行量子保密通信技术研究的许多技术成果。

全书共六章，分别介绍了保密通信概述、量子信息技术基础、量子密钥管理技术、量子保密通信体制、量子保密通信系统工程和量子保密通信与信息安全等。本书可作为信息安全、密码学、通信、计算机科学、量子光学应用等学科的科研和工程人员的参考书，也可作为相关专业高校师生的参考书。

感谢国防科工局、中国电子科技集团公司、北京理工大学出版社对本书出版给予的支持；感谢中国电子科技集团公司第三十研究所（下文简称 30 所）领导和专家们的支持和指导，特别感谢祝世雄、朱甫臣、程蝉、张文政、郝平、穆良知、李振邦等几位研究员在量子保密通信研究方面给予的悉心指导和无私帮助；感谢 30 所密码和量子密码项目组成员曹云飞、刘瑶、江卫、申兵、吉庆兵、霍家佳、谯通旭、于飞、赵伟等人的积极参与；特别感谢刘瑶等对本书稿的校定工作；感谢 30 所人力资源处的刘刚和综合计划处的许嘉对本专著申请和写作过程的跟踪管理。

感谢所有默默支持量子保密通信技术发展的前辈和热心人士，他们的勉励不断鞭策我们刻苦钻研、潜心探究量子保密通信技术的奥秘，以期在量子保密通信体制和系统应用等方面做出一点点有益的贡献。

由于量子保密通信技术是一个正在飞速发展的新兴学科，相关技术体制模型还不完善，其中一些论断很可能因不能描述相关技术的全貌而难免偏颇；再加上作者学识、水平有限，书中难免有错误和不妥之处。因此，作者期望本书能够起到抛砖引玉的作用，同时也期望得到来自读者的批评和指正，以达到不断完善量子保密通信技术体制并普及相关知识的目的。

作者

2009 年 6 月于现代通信国家重点实验室

目　录

第1章　保密通信概述

人类的各种社会活动都与通信有着密切联系，社会越进步，对通信的依赖程度就越大，尤其是在信息社会，一个国家乃至整个世界的社会、军事、政治、经济的正常运转和秩序维护都离不开通信。在当今这个纷繁复杂的人类社会，各种邪恶势力、潜在敌人和黑客等为了得到一个国家各个领域内的重要情报，从未间断过针对各种通信的窃听、监控和破译。在这种情况下，每个国家都不得不采用越来越先进的保密通信技术，以确保国家正常的保密通信不受现实威胁。保密通信是维护国家安全的一个必要技术手段，也是一个十分重要的科学研究领域，有着十分悠久并且充满神秘的历史，它随着技术的发展和进步不断得到提高和完善。

本章分别对保密通信的几个重要发展阶段、经典密码在战争中所扮演的传奇作用、经典密码学基本理论、经典密码所面临的技术困难与挑战以及量子保密通信的发展契机等进行了介绍。

1.1　神秘的古代密码术

“天机不可泄露”在当今是一个被泛用的词语，然而它的真正含义却是十分严肃的，一件东西或者一个消息之所以被称为“天机”，说明它是“神圣”的东西，不能主动或被动地对他人泄露其中的任何秘密，必须用忠诚甚至生命去捍卫它的安全。在商业竞争中，一个公司或者单位的“天机”意味着能否在竞争中取得主动地位；在战争中，有关军队战略部署和战术的“天机”关系着前沿阵地将士们的生命安全和战争的结局，甚至整个国家的兴衰。因此，为了确保“天机不可泄露”，从古至今，人们对如何实现这个目标的追求从未间断过，而确保“天机不可泄露”的主要技术手段就是形式多样的密码技术或者保密通信技术。

现实世界里保密的形式随着文明的发展程度、应用群体（士兵、外交官、写日记的人等）和应用目的等因素的不同而变化多样，保密通信的核心技术——密码技术因主要被用于保护一些“不宜”公开的“重要”信息而显得十分神秘，虽然它的起源缺少详细记载，但是密码技术在它几千年发展历程中却始终与人类战争紧密相连[1]。

在公元前5世纪，古希腊的斯巴达人将皮条紧紧缠绕在特定尺寸的木棍子上，再把密信自上而下地写在皮条上；然后再把皮条解开并通过信使或者信鸽等送给目标接收者。皮条的接收者只需要把皮条重新缠绕在相同尺寸的木棍上，就可以读出其中的信息。而在不知道木棍尺寸的情况下，这些皮条上的文字是毫无意义的，由此达到保密通信的目的。这就是有记载的最早使用的保密通信器械，并且称之为“天书”。由于当时文明程度和技术条件限制，“天书”的应用基本上是手工作业，远距离通信依赖信鸽或信使等。

到了公元前2世纪，希腊人波利比乌斯设计了一个可以使用火把进行远距离通信的信号通信体制，人们称之为波利比乌斯方格或棋盘密表。棋盘密表把26个英文字母按顺序排列在一个5行5列的方格内，并把不容易误用的 i 和 j 排在同一个格子里，使用1、2、3、4、5这5个数字分别对行和列进行编号，然后使用每个字母所在行和列的序号表示这个字母（如表1-1所示），比如“23”表示第2行第3列的字母“h”。信号发送者把信息的每个字母转换为相应的

行和列的序号组合，然后通过使用不同数量的火把（确保接收者能够识别）表示相应的数字把这些序号组合发送出去；接收者使用同样的棋盘密表根据行和列的序号恢复相应的字母，由此实现远距离通信功能。

表 1-1 棋盘密表

列序号 / 行序号	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

可以想象，在古代相隔遥远的烽火台之间，在夜晚利用两组火把进行保密通信的场景。每一个烽火台可以使用两组人员，每组 5 个人，每人各持一个火把。这两组人员相隔一定的距离以确保接收方能分辨出来，其中左边一组表示行序号，另一组表示列序号，然后根据发送字母的不同点亮不同个数的火把。比如为了发送字母“e”，也即需要发送序号组合“15”，那么把左边一组的一个火把点亮，而把另一组的 5 个火把全部点亮（如图 1-1 所示）。

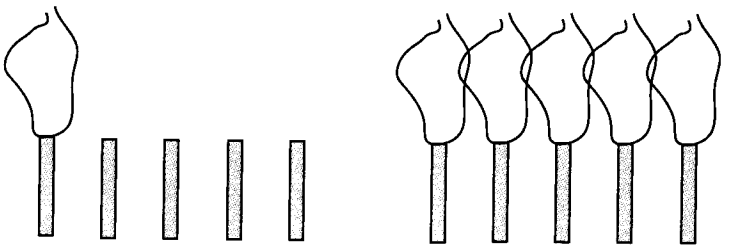


图 1-1 棋盘密表的应用示意图

当然，当他们挥舞着火把进行通信时，也可能被知晓棋盘内容的“敌人”发现并破解他们通信的内容，而对于不知道棋盘内容的人来说，则无法知道他们在传递什么信息。因此，为了保密，他们就不得不经常变换棋盘的排列方式。从技术的角度来分析，棋盘密表把字母转换为数字进行通信，实现了一种简单的编码方式，并可以通过火光等进行远距离通信，简化了在特定环境下的应用条件，因而得到了一定的应用。

棋盘密表是人们尝试使用新方法进行远距离保密通信的一个十分重要的早期成果。当然，棋盘密表只是一个简单的符号代替变换，安全性很弱。

1.2 经典保密通信介绍

随着技术的进步，人们开始尝试把数学变换应用到密码算法的设计与分析中。在 1412 年盖勒盖尚迪所编写的百科全书中，就出现了多种移位密码和代替密码方案，并出现了对语言特征进行分析的论述。实际上，移位密码就是一种简单的数学变换，也即简单的线性代数问题；

而对语言特征的分析主要是利用了概率统计方法。由此不难看出，早在 500 多年前，人们就开始基于一些数学问题进行密码算法设计和分析的探索。下面，我们通过分析一些典型的移位密码和代替密码及其破解方法，来说明数学在密码学中的重要应用（为了上下文的连贯性，我们不对相应的数学理论进行详细说明，其中主要涉及线性代数、概率统计、近世代数、数论等学科中的部分知识点，具体可以参考相应的数学教材）。

为了不影响以后章节内容的阅读，我们对保密通信或者密码通信的一些基本概念进行简单介绍（详细内容见参考文献[2]）。

密码通信过程主要涉及的各方包括发送者、接收者和窃听者，如图 1-2 所示。在本书中，我们把发送者记为 Alice，接收者记为 Bob，窃听者（或称之为分析者、破译者、攻击者等）记为 Eve。

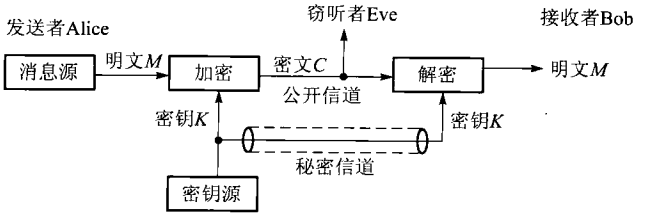


图 1-2　保密通信模型

消息也称为明文，使用某种方法对明文进行掩盖处理的过程称为加密，加密后的数据称为密文；相应地，把密文转变为明文的过程称为解密，加、解密都需要使用相同或者相关的密钥，以确保通信双方能够有效加、解密。一般情况，使用 M 表示消息集，它可以是一般数据、图像、语音等；使用 P 表示明文集；使用 C 表示密文集，使用 K 表示密钥集。

对消息进行掩盖处理以达到对消息进行保密的技术和科学叫做密码编码学，对密码或者密文进行分析和破译以期得到相应消息或者密钥的技术和方法叫做密码分析学。密码编码学和密码分析学共同构成密码学。值得注意的是，根据上下文内容不同，所谓的“密码学”大多数情况下是指二者之一。

1.2.1　基于模运算的移位密码

我们首先对模运算进行简单介绍。如果 $a=b+kn$ 对整数 k 都成立，那么 $a\equiv b(\mathrm{mod}\ n)$；如果 $a>0$，并且 $0\leqslant b<n$，那么可以把 b 看作 a 被 n 整除后的余数。有时，b 被叫做 a 模 n 的余数，或者称 a 与 b 模 n 同余。

从 0 到 $n-1$ 的 n 个整数组成的集合构成了模 n 的“完全剩余集”，对每一个整数 a，它模 n 的余项是这个集合中的某个元素，也即 a 模 n 的运算给出了 a 的余数，这样的余数是从 0 到 $n-1$ 的某个整数。这种运算也称为模运算。

模运算满足交换律、结合律和分配律。简化运算每一个中间结果的模 n 运算，与先进行全部简化运算再模 n 运算得到的结果是一样的。

移位密码的数学语言描述为，设 $P=C=K=Z_{26}$，对于 $0\leqslant k\leqslant 25$，定义 $En_k(x)=(x+k)\ \mathrm{mod}\ 26$，$De_k(y)=(y-k)\mathrm{mod}\ 26$，（其中 $x,y\in Z_{26}$）。可以看出移位密码的加密和解密变换就

是一个简单的代数运算。下面我们基于 26 个英文字母的变换来介绍移位密码的基本原理。

移位密码首先把 26 个英文字母从 0 到 25 依次编上序号，即使用 26 个数字分别表示 26 个英文字母，并参与密码加密和解密变换（如表 1－2 所示）。（以下明文字母使用相应的小写字母，密文字母使用相应的大写字母。）

表 1－2 自然序字母表

0	1	2	3	4	5	6	7	8	9	10	11	12
a	b	c	d	e	f	g	h	i	j	k	l	m
13	14	15	16	17	18	19	20	21	22	23	24	25
n	o	p	q	r	s	t	u	v	w	x	y	z

如果通信双方事先商定使用 8 作为密钥，即把 i 移到 a 的位置，把 j 移位到 b 的位置，依此类推，由此形成一个密表（如表 1－3 所示）。在进行加密时，通信一方根据密表把明文字母一一进行替换，即把明文中的 a 替换为 I，明文中的 b 替换为 J，依此类推；解密时，进行相反的操作。

表 1－3 向左移动 8 位形成的密表

0	1	2	3	4	5	6	7	8	9	10	11	12
I	J	K	L	M	N	O	P	Q	R	S	T	U
13	14	15	16	17	18	19	20	21	22	23	24	25
V	W	X	Y	Z	A	B	C	D	E	F	G	H

例 1.1 假设 Alice 要对“*friend*”进行加密，她首先根据表 1－2 把“*friend*”转换为数字序列“5 17 8 4 13 3”，然后把这些数字分别进行模 26 加 8 运算，即得到“13 25 16 12 21 11”，再根据表 1－2 把它转换为字母得到密文“*NZQMVL*”。同样，解密过程，首先根据表 1－2 把“*NZQMVL*”转换为数字序列“13 25 16 12 21 11”，再进行模 26 减 8 运算，得到“5 17 8 4 13 3”，再根据表 1－2 把它转换为字母得到“*friend*”。从而完成解密过程。当然，她也可以直接根据表 1－3 把“5 17 8 4 13 3”转换为相应的字母“*NZQMVL*”完成加密过程。解密，采用相反的查表顺序，即根据表 1－3 把字母“*NZQMVL*”转换为“5 17 8 4 13 3”；再根据表 1－2 把“5 17 8 4 13 3”转换为相应的字母“*friend*”。

显然，模 26 移位密码是不安全的，因为它只有 26 种可能的情况，也即密钥空间太小，可以通过穷举搜索来进行破译。

根据文献记载朱利叶斯·凯撒最早使用这种移位密码（他当时使用 D 代替 a，E 代替 b，依此类推进行加密），因此，人们习惯把具有自然序的密表称之为凯撒密表，并把相应的密码方案称为凯撒密码。

1.2.2 替换密码

对于 Z_{26} 上的移位密码来说，字母表在移位后所有字母的比邻关系并没有变化，因而操作简单，但是不安全。不过，如果随机把一个字母替换为另外一个字母，那么相应的加、解密变换

就复杂了，安全性也会得到一定的提高。这种随机进行字母替换的密码算法就是替换密码。

替换密码的数学语言描述为：

设 $P=C=K=Z_{26}$，K 是由 26 个数字符号 0，1，…，25 构成的所有可能置换，对每一个置换 $F\in K$，定义 $En_k(x)=F(x)$，$De_k(y)=F^{-1}(y)$，这里 F^{-1} 是 F 的逆置换。

例 1.2　假如我们使用表 1－4 所示的替换密表。

根据替换密表 1－4 把“*friend* ”加密，可以得到“*AKPNUY* ”。解密操作正好相反。

表 1－4　替换密表实例

明文	a	b	c	d	e	f	g	h	i	j	k	l	m
密文	S	L	X	Y	N	A	R	C	P	V	H	M	F
明文	n	o	p	q	r	s	t	u	v	w	x	y	z
密文	U	W	J	D	K	I	G	Q	Z	T	B	E	O

替换密码的密钥空间是由 26 个字母的全部置换所组成，这些置换的总个数是 26!，即 Z_{26} 上的替换密码的密钥空间是 26!，大于 4.1×10^{26}，因此，替换密码对于搜索密钥空间的攻击方法是比较安全的，但是对于统计分析是不安全的。

替换密码对基于英文语言统计特性的攻击是不安全的。人们通过对小说、杂志和报纸等各种英文文章进行统计发现，26 个英文字母及其一些字母组合出现的频率差别很大，并得到了表 1－5 所示的参考概率。

表 1－5　26 个英文字母出现的概率

字 母	概 率	字 母	概 率
A	0.082	N	0.067
B	0.015	O	0.075
C	0.028	P	0.019
D	0.043	Q	0.001
E	0.127	R	0.060
F	0.022	S	0.063
G	0.020	T	0.091
H	0.061	U	0.028
I	0.070	V	0.010
J	0.002	W	0.023
K	0.008	X	0.001
L	0.040	Y	0.020
M	0.024	Z	0.001

可以看出，如果在大量的密文字母统计中发现某个密文字母出现频率和表中某个字母的频率相当，可以初步假定这个密文字母就是那个明文字母，比如假设密文中某个字母出现的频率最大，那么基本上就可以断定它是 e；对于难以确定的字母可以根据英文语法、用词习惯等因素进行猜测，直到得到一个合理的有意义的明文。因为替换密码并没有破坏英文语言的统

计特性，因此替换密码对统计分析来说是不安全的。

1.2.3 维吉尼亚密码

移位密码和替换密码都是一次选择一个密钥，每一个字母都映射成唯一的一个字母，因此这种密码体制被称为单表密码体制。而多表密码体制是使用两个以上的代替表依次对明文消息字母进行代替的加密方法。假设明文字母表为 Z_{26} 上的一个映射，代替序列为 $f=(f_1,f_2,\cdots,f_i,\cdots)$，明文字母序列 $m=m_1m_2\cdots m_n$，那么密文字母序列为 $c=En_k(m)=f(m)=f_1(m_1)f_2(m_2)\cdots f_n(m_n)$。如果 f 是一个非周期性的无限序列，即对每个明文字母都采用不同的代替表进行加密，那么这种多表密码体制就是下面将要介绍的完全保密的一次一密乱码本。

在这里我们介绍一个典型的多表密码算法，即维吉尼亚密码，这个密码算法是以 16 世纪的 B. de. Vigenere 的名字命名的。

维吉尼亚密码定义如下，设 m 是某一固定的正整数，定义 $P=C=K=(Z_{26})^m$，对一个密钥 $K=(k_1,k_2,\cdots,k_m)$，定义加密和解密分别为

$$En_k(x_1,x_2,\cdots,x_m)=(x_1+k_1,x_2+k_2,\cdots,x_m+k_m)$$

$$De_k(y_1,y_2,\cdots,y_m)=(y_1-k_1,y_2-k_2,\cdots,y_m-k_m)$$

其中所有运算在 Z_{26} 中完成。

使用前面已描述过的映射 $A\leftrightarrow0$、$B\leftrightarrow1$、$\cdots$、$Z\leftrightarrow25$，使每一个密钥 K 与长度为 m 密钥字的字符串相关联。

例 1.3 假设 $m=6$，密钥字 K 是 $CIPHER$，假设明文 M 是 *this cryptosystem is not secure*。

首先将密钥字 K 和明文 M 转化为相对应的数字序列，即 $K=(2,8,15,7,4,17)$，$M=(19,7,8,18,2,17,24,15,19,14,18,24,18,19,4,12,8,18,13,14,19,18,4,2,20,17,4)$。把这些明文以 6 个为一组写下来，然后模 26 加 K，过程如下：

明文	19	7	8	18	2	17	24	15	19	14	18	24
密钥	2	8	15	7	4	17	2	8	15	7	4	17
密文	21	15	23	25	6	8	0	23	8	21	22	15

明文	18	19	4	12	8	18	13	14	19	18	4	2	20	17	4
密钥	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15
密文	20	1	19	19	12	9	15	22	8	25	8	19	22	25	19

把上表中的密文序列转化为相应的字母得到

$$VPXZGIAXIVWPUBTTMJPWIZITWZT$$

解密过程与加密过程类似，区别在于加密使用模 26 加，而解密使用模 26 减。

在维吉尼亚密码中，长度为 m 的可能密钥字的长度是 26^m，这对于一个小的 m 值，穷举密钥空间都将需要很长的时间，例如，$m=5$，密钥空间超过 1.1×10^7，这个已经大到足以阻止手工的穷举密钥搜索，因此这种密码体制在手工计算的时代是安全的，当然它对于计算效率较高

的机械计算和电子计算是不安全的。

1.2.4　Hill 密码

在这一节，我们将介绍另一种多表密码体制，它是由 L. S. Hill 于 1929 年发明的 Hill 密码。Hill 密码的定义如下：

设 m 是一个固定的正整数，$P=C=(Z_{26})^m$，$K=\{Z_{26}$ 上的 $m\times m$ 级可逆矩阵$\}$，对每一个 $k_x\in K$、明文 $x\in P$ 和密文 $y\in C$，我们定义加密为 $En_k(x)=xk_x$，解密为 $De_k(y)=yk_x^{-1}$，其中所有运算都在 Z_{26} 上进行。

可以看出，Hill 密码的基本思想是取一个明文元素 m 个字母的 m 个线性组合，产生一个密文元素中的 m 个字母。其加、解密过程需要使用线性代数中的矩阵乘法运算，下面我们对线性代数的一些相关的基本概念进行介绍。

如果 $A=(a_{i,j})$ 是 $l\times m$ 的矩阵，$B=(b_{j,k})$ 是 $m\times n$ 的矩阵，那么矩阵的乘积定义为

$$AB=(c_{i,k}):c_{i,k}=\sum_{j=1}^{m}a_{i,j}b_{j,k}，\text{其中 } 1\leqslant i\leqslant l,1\leqslant k\leqslant n$$

即 AB 的第 i 行第 k 列元素是取 A 的第 i 行和 B 的第 k 列的相应元素相乘，然后相加而得到的。最后得到一个 $l\times n$ 级矩阵。

矩阵乘法满足结合率，即 $(AB)C=A(BC)$；一般情况下，矩阵乘法不满足交换律，即 $AB=BA$ 这个等式并不是总能成立。

$m\times m$ 的单位矩阵记为 I_m，它是一个主对角线为 1，其他元素都为 0 的 $m\times m$ 的矩阵。比如 2×2 的单位阵 $\boldsymbol{I}_2=\begin{bmatrix}1&0\\0&1\end{bmatrix}$。

如果 $m\times m$ 的矩阵 A 存在逆矩阵 A^{-1}，那么满足 $AA^{-1}=A^{-1}A=I_m$。并不是所有的矩阵都有逆矩阵，但如果存在逆矩阵，那么它必定是唯一的。

基于上面的知识，我们不难看出，Hill 密码的加、解密运算是互逆的，即 $yk_x^{-1}=(xk_x)k_x^{-1}=x(k_xk_x^{-1})=xI_m=x$。

下面通过一个简单的例子来说明 Hill 密码的加密和解密过程。

例 1.4　假设 Hill 密码的加密密钥 $\boldsymbol{k}_x=\begin{bmatrix}2&1\\0&2\end{bmatrix}$，解密密钥 $\boldsymbol{k}_x^{-1}=\begin{bmatrix}\frac{1}{2}&-\frac{1}{4}\\0&\frac{1}{2}\end{bmatrix}$，假设对明文 (2,3) 进行加密，其计算过程如下：

加密：$(y_1,y_2)=(x_1,x_2)\begin{bmatrix}2&1\\0&2\end{bmatrix}=(2x_1,x_1+2x_2)$，即 $(2,3)\begin{bmatrix}2&1\\0&2\end{bmatrix}=(4,8)$；

解密：$(x_1,x_2)=(y_1,y_2)k_x^{-1}=(4,8)\begin{bmatrix}\frac{1}{2}&-\frac{1}{4}\\0&\frac{1}{2}\end{bmatrix}=(2,3)$。

可以看出 Hill 密码能够正确实现加、解密。

Hill 密码对于唯密文攻击具有较高的安全性，但是对于已知明文攻击是不安全的。