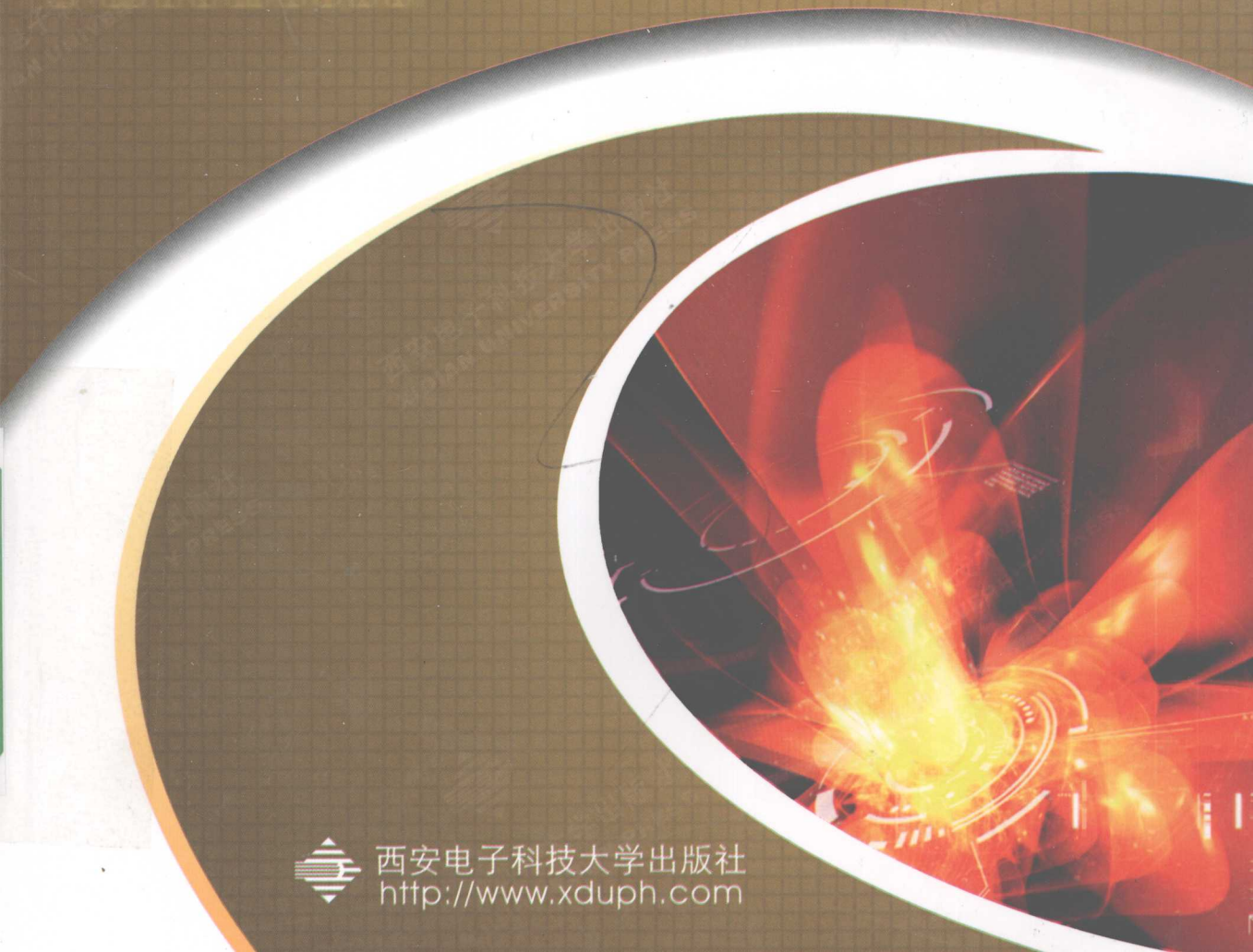
高等学校电子与通信类专业“十一五”规划教材

密码学基础

编著 范九伦 张雪锋
刘宏月 谢 勰
主审 李 晖



西安电子科技大学出版社
http://www.xduph.com

高等学校电子与通信类专业“十一五”规划教材

密码学基础

编著　范九伦　张雪锋
　　刘宏月　谢　勰
主审　李　晖

西安电子科技大学出版社

2008

内 容 简 介

本书系统地介绍了密码学的基本原理、基本算法，并对算法的安全性进行了相应的分析。主要内容包括古典密码、分组密码、序列密码、Hash 函数、公钥密码、数字签名、密钥管理和计算复杂性等。

本书主要供信息安全、网络工程、计算机科学与技术、通信工程等本科专业的高年级学生使用，也可供相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

密码学基础/范九伦等编著．—西安：西安电子科技大学出版社，2008.8
高等学校电子与通信类专业“十一五”规化教材
ISBN 978-7-5606-2084-8
Ⅰ．密… Ⅱ．范… 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 100858 号

策　　划　曹　昱
责任编辑　张　梁　曹　昱
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　编　710071
http://www.xduph.com　　E-mail：xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西光大印务有限责任公司
版　　次　2008 年 8 月第 1 版　2008 年 8 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印张 11.5
字　　数　265 千字
印　　数　1～4000 册
定　　价　16.00 元
ISBN 978-7-5606-2084-8/TP・1071
XDUP 2376001-1

西安电子科技大学出版社
高等学校电子与通信类专业“十一五”规划教材
编审专家委员会名单

主　任：杨　震（南京邮电大学校长、教授）

副主任：张德民（重庆邮电大学通信与信息工程学院副院长、教授）

秦会斌（杭州电子科技大学电子信息学院院长、教授）

通信工程组

组　长：张德民（兼）

成　员：（成员按姓氏笔画排列）

王　晖（深圳大学信息工程学院副院长、教授）

巨永锋（长安大学信息工程学院副院长、教授）

成际镇（南京邮电大学通信与信息工程学院副院长、副教授）

刘顺兰（杭州电子科技大学通信工程学院副院长、教授）

李白萍（西安科技大学通信与信息工程学院副院长、教授）

张邦宁（解放军理工大学通信工程学院卫星系系主任、教授）

张瑞林（浙江理工大学信息电子学院院长、教授）

张常年（北方工业大学信息工程学院院长、教授）

范九伦（西安邮电学院信息与控制系系主任、教授）

姜　兴（桂林电子科技大学信息与通信学院副院长、教授）

姚远程（西南科技大学信息工程学院副院长、教授）

康　健（吉林大学通信工程学院副院长、教授）

葛利嘉（中国人民解放军重庆通信学院军事信息工程系系主任、教授）

电子信息工程组

组　长：秦会斌（兼）

成　员：（成员按姓氏笔画排列）

王　荣（解放军理工大学通信工程学院电信工程系系主任、教授）

朱宁一（解放军理工大学理学院基础电子学系系主任、工程师）

李国民（西安科技大学通信与信息工程学院院长、教授）

李邓化（北京信息工程学院信息与通信工程系系主任、教授）

吴　谨（武汉科技大学信息科学与工程学院电子系系主任、教授）

杨马英（浙江工业大学信息工程学院副院长、教授）

杨瑞霞（河北工业大学信息工程学院院长、教授）

张雪英（太原理工大学信息工程学院副院长、教授）

张　彤（吉林大学电子科学与工程学院副院长、教授）

张焕君（沈阳理工大学信息科学与工程学院副院长、副教授）

陈鹤鸣（南京邮电大学光电学院院长、教授）

周　杰（南京信息工程大学电子与信息工程学院副院长、教授）

欧阳征标（深圳大学电子科学与技术学院副院长、教授）

雷　加（桂林电子科技大学电子工程学院副院长、教授）

项目策划：毛红兵

策　　划：曹　昳　寇向宏　杨　英　郭　景

前　言

密码学有着悠久而神秘的历史，最早的密码技术可以追溯到古罗马时代。1949 年，Claude Shannon 在 Bell System Technical Journal 上发表的论文“The Communication Theory of Secrecy Systems”，标志着密码学研究进入了崭新的时代。20 世纪 70 年代以来，分组密码和公钥密码技术得到了迅速发展，取得了丰富的研究成果，也被广泛应用于信息安全的各个领域。随着互联网技术和计算机技术的发展和普及，越来越多的人认识到密码学的重要性。为了能为在校本科生学习密码学提供内容较新、论述较系统的教材，也能为相关领域的科研人员提供一本内容充实、具有一定实用性的参考书，我们编写了《密码学基础》这本教材。

本书系统介绍了密码学的基本原理，在此基础上详细介绍了密码学中的基本算法及其应用，详细介绍了当前广泛应用的密码算法及其理论基础，并对其安全性进行了相应的分析。本书内容以当前广泛应用的密码技术为主，重点放在密码学研究的核心问题上，既突出了广泛性，又注重对主要知识内容的深入讨论。本书的每一章后都附有相应的习题，便于读者对书中的内容进行总结和应用，同时也对思维和智力进行相应的锻炼。作为示例，本书给出了常用的基本加密算法——DES 和 RSA 算法的 C 语言程序。

本书主要供信息安全、网络工程、计算机科学与技术、通信工程等本科专业的高年级学生使用。学习该课程的学生需要具备高等数学和线性代数的基础知识，同时应该掌握基本的编程技术和数据结构的基本知识。通过对本课程的学习，学生可以掌握基本的密码学算法原理，对加/解密技术具备一定的实际应用能力。为了便于学生学习和理解本课程，我们以结论性的方式在附录 A 中给出了学习密码学需要具备的数论基础知识。对于已经具备相关数论知识的学生，这一部分内容可以作为了解内容；对于不具备相关数论基础知识的学生，这一部分内容可以作为自学内容。本书计划课时为 48～64 学时，其中对密码学基础知识的介绍大约需要 48 学时，具有扩展性的知识用 * 号给出了标记。在讲授本书的过程中，建议根据课时量和授课对象来选择和组织相关内容。

全书共分 8 章和 3 个附录，第 1 章由范九伦编写，第 2、3、4 章由张雪锋编写，第 5、6、7 章和附录 A 由刘宏月编写，第 8 章和附录 B、C 由谢勰编写。全书由范九伦负责整理和统稿。

衷心感谢本书的主审李晖教授，他为本书提出了许多宝贵的意见和建议，使我们受益匪浅。衷心感谢西安电子科技大学出版社的编辑们，是他们的辛勤劳动，使本书得以顺利出版。为了使本书既包含密码学的基础知识，又能反映这些基础知识涉及到的最新研究成果，本书在编写过程中参考了国内外许多同行的论文、著作，引用了其中的观点、数据与结论，在此一并表示感谢。

由于作者学识有限，书中缺点在所难免，敬请批评、指正。

作　者

2008 年 4 月于西安

目　录

第1章 古典密码

古典密码(Classical Cipher)是现代密码的基础。本章在简要介绍密码学基本概念的基础上，介绍一些典型的古典密码体制，通过对古典密码学进行分析，给出密码分析学的基本概念和原理。

1.1 密码学的基本概念

密码学有着悠久而神秘的历史，人们很难对密码学的起始时间给出准确的定义。一般认为人类对密码学的研究与应用已经有几千年的历史，该学科一直广泛应用于军事领域。密码学正式作为一门科学的理论基础应该首推1949年美国科学家Shannon的一篇文章《保密通信的信息理论》，他在研究保密机的基础上，提出了将密码建立在解某个已知数学难题基础上的观点。20世纪70年代，以公钥密码体制的提出和数据加密标准DES的问世为标志，现代密码学开始蓬勃发展。随着计算机技术和网络技术的发展，互联网的普及和网上业务的大量开展，人们更加关注密码学，更加依赖密码技术。

保密是密码学的核心。密码学的基本目的是面对攻击者Oscar，在被称为Alice和Bob的通信双方之间应用不安全的信道进行通信时，设法保证通信安全。密码学研究对通信双方要传输的信息进行何种保密变换以防止未被授权的第三方对信息的窃取。此外，密码技术还可以用来进行信息鉴别、数据完整性检验、数字签名等。

在通信过程中，Alice和Bob也分别被称为信息的发送方和接收方。Alice要发送给Bob的信息称为明文(Plaintext)。为了保证信息不被未经授权的Oscar识别，Alice需要使用密钥(Key)对明文进行加密，加密得到的结果称为密文(Ciphertext)。密文一般是不可理解的，Alice将密文通过不安全的信道发送给Bob，同时通过安全的通信方式将密钥发送给Bob。Bob在接收到密文和密钥的基础上，可以对密文进行解密，从而获得明文；对于Oscar，他可能会窃听到信道中的密文，但由于无法得到加密密钥，因此无法知道相应的明文。

图1-1给出了保密通信的一般机制。根据加密和解密过程所采用密钥的特点可以将加密算法分为两类：对称加密算法和公开密钥加密算法。

对称加密算法也称为传统加密算法，是指解密密钥与加密密钥相同或者能够从加密密钥中直接推算出解密密钥的加密算法。通常在大多数对称加密算法中解密密钥与加密密钥是相同的，所以这类加密算法要求Alice和Bob在进行保密通信前，通过安全的方式商定一个密钥。对称加密算法的安全性依赖于密钥的选择。

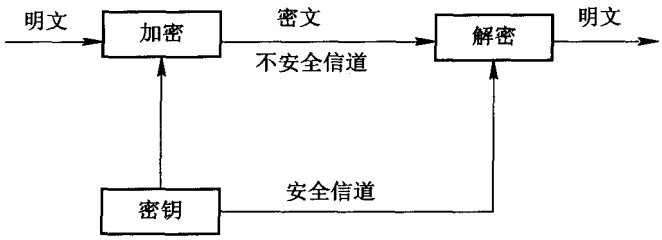


图 1-1 保密通信的一般机制

公开密钥加密算法也称为公钥加密算法，是指用来解密的密钥不同于进行加密的密钥，也不能够通过加密密钥直接推算出解密密钥的加密算法。一般情况下，加密密钥是可以公开的，任何人都可以应用加密密钥来对信息进行加密，但只有拥有解密密钥的人才可以解密出被加密的信息。在以上过程中，加密密钥称为公钥，解密密钥称为私钥。

在图 1-1 所示的保密通信机制中，为了在接收端能够有效地恢复出明文信息，要求加密过程必须是可逆的。从上述图示可见，加密方法、解密方法、密钥和消息(明文、密文)是保密通信中的几个关键要素，它们构成了相应的密码体制。

定义 1.1.1 密码体制 密码体制的构成包括以下要素：

(1) M：明文消息空间，表示所有可能的明文组成的有限集。

(2) C：密文消息空间，表示所有可能的密文组成的有限集。

(3) K：密钥空间，表示所有可能的密钥组成的有限集。

(4) E：加密算法集合。

(5) D：解密算法集合。

该密码体制应该满足的基本条件是：对任意的 $key \in K$，存在一个加密规则 $e_{key} \in E$ 和相应的解密规则 $d_{key} \in D$，使得对任意的明文 $x \in M$，$e_{key}(x) \in C$ 且 $d_{key}(e_{key}(x)) = x$。

在以上密码体制的定义中，最关键的条件是加密过程 e_{key} 的可逆性，即密码体制不仅能够对明文 x 应用 e_{key} 进行加密，而且应该可以使用相应的 d_{key} 对得到的密文进行解密，从而恢复出明文。

显然，密码体制中的加密函数 e_{key} 必须是一个一一映射。要避免出现在加密时 $x_1 \neq x_2$，而对应的密文 $e_{key}(x_1) = e_{key}(x_2) = y$ 的情况，否则在解密过程无法准确确定密文 y 对应的明文 x。

1.2 几种典型的古典密码体制

古典密码是密码学的渊源，虽然古典密码都比较简单而且容易破译，但研究古典密码的设计原理和分析方法对于理解、设计以及分析现代密码技术是十分有益的。本节介绍几种典型的古典密码体制。

1.2.1 棋盘密码

棋盘密码是公元前 2 世纪前后由希腊人提出来的，在当时得到了广泛的应用。棋盘密码通过将 26 个英文字母设法变成十位数来达到加密的目的。棋盘密码的密钥是一个 5×5

的棋盘，将 26 个英文字母放置在里面，其中字母 i 和 j 被放在同一个方格中，如下表所示：

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

在给定了字母排列结果的基础上，每一个字母都会对应一个数字 $\alpha\beta$，其中 α 是该字母所在行的标号，β 是该字母所在列的标号。通过设计的棋盘就可以对英文消息进行加密，如 u 对应的是 22，f 对应的是 34。

例 1.1 如果明文消息是

Information Security

则相应的密文序列是

23 54 34 24 14 55 31 15 23 24 54 32 13 51 22 14 23 15 21

解密过程应用相同的棋盘排列，根据密文给出的字母所在位置来恢复相应的明文消息。

棋盘密码的任一个密钥是 25 个英文字母(将字母 i 和 j 看成一个字母)在 5×5 的棋盘里的一种不重复排列。由于所有可能的排列有 25! 种，因此棋盘密码的密钥空间大小为 25!。所以，对于棋盘密码，如果采用密钥穷举搜索的方法进行攻击，计算量会相当大。

1.2.2 移位密码

移位密码的加密对象为英文符号。移位密码采用每一字母向前推移 key 位的方式实现加密。换句话说，移位密码实现了 26 个英文字母的循环移位。由于英文字符有 26 个字母，因此可以在英文字母表和 $Z_{26}=\{0, 1, \cdots, 26\}$ 之间建立一一对应的映射关系。当取密钥 $key=3$ 时，得到的移位密码称为凯撒密码，因为该密码体制首先被 Julius Caesar 所使用。

定义 1.2.1 移位密码体制 令 $M=C=K=Z_{26}$。对任意的 $key\in Z_{26}$，$x\in M$，$y\in C$，定义

$$e_{key}(x)=(x+key) \bmod 26$$

$$d_{key}(y)=(y-key) \bmod 26$$

在使用移位密码体制对英文符号进行加密之前，首先需要在 26 个英文字母与 Z_{26} 中的元素之间建立一一对应关系，然后应用以上密码体制进行相应的加密计算和解密计算。

例 1.2 设移位密码的密钥为 $key=7$，英文字符与 Z_{26} 中的元素之间的对应关系如下表所示：

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

假设明文为 ENCRYPTION，则加密过程如下：

首先将明文根据对应关系表映射到 Z_{26}，得到相应的整数序列

04 13 02 17 24 15 19 08 14 13

然后将每个数字与 7 相加，同时对 26 进行取模运算，得到

11 20 09 24 05 22 00 15 21 20

最后再应用对应关系表将以上数字转化成英文字符，即得相应的密文为

LUJYFWAPVU

解密是加密的逆过程。首先应用对应关系表将密文转化成数字，再将每个数字减去 7 后和 26 进行取模运算，对计算结果使用原来的对应关系表即可还原成英文字符，从而解密出相应的明文。

移位密码的加密和解密过程都是循环移位运算，由于 26 个英文字母顺序移位 26 次后还原，因此移位密码的密钥空间大小为 25。

1.2.3 代换密码

26 个英文字母和 Z_{26} 的元素之间可以建立一个一一对应关系，于是 Z_{26} 上的任一个置换也就对应了 26 个英文字母表上的一个置换。因此可以借助 Z_{26} 上的置换来改变英文字符的原有位置，以达到加密的目的，Z_{26} 上的置换看成了加密所需的密钥。这样可以将加密和解密过程直接看做是对英文字母表进行了置换变换。

定义 1.2.2 代换密码体制 令 $M=C=Z_{26}$，K 是 Z_{26} 上所有可能置换构成的集合。对任意的置换 $\pi\in K$，$x\in M$，$y\in C$，定义

$$e_\pi(x)=\pi(x)$$

$$d_\pi(y)=\pi^{-1}(y)$$

这里 π 和 π^{-1} 互为逆置换。

例 1.3 设置换 π 如下：

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

其中大写字母为明文字符，小写字母为密文字符。根据以上对应关系，置换 π 对应的逆置换 π^{-1} 为

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

假设明文为 ENCRYPTION，则相应的密文为 tfeknhzogf。

代换密码的任一个密钥 π 都是 26 个英文字母的一种置换。由于所有可能的置换有 26! 种，因此代换密码的密钥空间大小为 26!。所以，对代换密码如果采用密钥穷举搜索的方法进行攻击，计算量会相当大。

1.2.4 维吉尼亚密码

前面介绍的移位密码和代换密码体制中，一旦加密密钥被选定，则英文字母表中每一个字母对应的数字都会被加密成惟一的一个密文数字。这种密码体制被称为单表代换密码。本小节介绍一种多表代换密码——维吉尼亚密码(Vigenère Cipher)，它是由法国人 Blaise de Vigenère 在 16 世纪提出的。

定义 1.2.3 维吉尼亚密码体制 令 m 是一个正整数，相应地定义 $M=C=K=(Z_{26})^m$。对任意的密钥 $key=(k_1, k_2, \cdots, k_m)\in K$，$(x_1, x_2, \cdots, x_m)\in M$，$(y_1, y_2, \cdots, y_m)\in C$，定义

$$e_{key}(x_1, x_2, \cdots, x_m)=(x_1+k_1, x_2+k_2, \cdots, x_m+k_m) \bmod 26$$
$$d_{key}(y_1, y_2, \cdots, y_m)=(y_1-k_1, y_2-k_2, \cdots, y_m-k_m) \bmod 26$$

如果已经在 26 个英文字母和 Z_{26} 之间建立了一一对应的关系，则每一个密钥 $key\in K$ 都相当于一个长度为 m 的字母串，被称为密钥字。

例 1.4 令 $m=8$，密钥字为 Computer，则根据例 1.2 中的对应关系可知，密钥字对应的数字序列为 $key=(02, 14, 12, 15, 20, 19, 04, 17)$。假设明文消息为

Block cipher design principles

加密过程首先将明文字符串对应为数字，每 8 个分为一组，使用密钥字对分组明文消息进行模 26 下的加密运算，加密过程如下所示：

明文	01	11	14	02	10	02	08	15	07	04	17	03	04	18
密钥	02	14	12	15	20	19	04	17	02	14	12	15	20	19
密文	03	25	00	17	04	21	12	06	09	18	03	18	24	11
明文	08	06	13	15	17	08	13	02	08	15	11	04	18	
密钥	04	17	02	14	12	15	20	19	04	17	02	14	12	
密文	12	23	15	03	03	23	07	21	12	06	13	18	04	

所以相应的密文序列为

Dzarevmgjsdsylmxpddxhvmgnse

解密过程使用相同的密钥字，进行相应的逆运算即可。

维吉尼亚密码的密钥空间大小为 26^m，所以即使 m 的值较小，相应的密钥空间也会很大。在维吉尼亚密码体制中，一个字母可以被映射为 m 个字母中的某一个，这样的映射关系也比单表代换密码更为安全一些。

1.2.5 仿射密码

仿射密码是代换密码的一个特例。仿射密码的密码体制定义如下。

定义 1.2.4 仿射密码体制 令 $M=C=Z_{26}$，$K=\{(k_1, k_2)\in Z_{26}\times Z_{26}: \gcd(k_1, 26)=1\}$。

对任意的密钥 $key=(k_1, k_2)\in K$，$x\in M$，$y\in C$，定义

$$e_{key}(x)=(k_1x+k_2) \bmod 26$$

$$d_{key}(y)=k_1^{-1}(y-k_2) \bmod 26$$

其中，k_1^{-1} 表示 k_1 在 Z_{26} 中的乘法逆，$\gcd(k_1, 26)=1$ 表示 k_1 与 26 互素。

根据数论中的相关结论，当且仅当 $\gcd(k_1, 26)=1$ 时，同余方程 $y\equiv(k_1x+k_2) \bmod 26$ 有惟一解 x。当 $k_1=1$ 时，仿射密码变成了移位密码。

例 1.5 设已知仿射密码的密钥 $k=(11, 3)$，则可知 $11^{-1} \bmod 26=19$。假设明文为 13，那么相应的密文为

$$y=(11\times 3+3) \bmod 26=16$$

解密过程为

$$x=19\times(16-3) \bmod 26=13$$

在 Z_{26} 中，满足条件 $\gcd(k_1, 26)=1$ 的 k_1 只有 12 个值(它们分别是 1,3,5,7,9,11,15,17,19,21,23,25)，因此仿射密码的密钥空间大小为 $12\times 26=312$。

有关元素的乘法逆的具体计算方法，本书在附录中给出了详细的计算过程。对于 Z_{26} 中与 26 互素的元素，相应的乘法逆为

$$1^{-1} \bmod 26=1$$

$$3^{-1} \bmod 26=9$$

$$5^{-1} \bmod 26=21$$

$$7^{-1} \bmod 26=15$$

$$11^{-1} \bmod 26=19$$

$$17^{-1} \bmod 26=23$$

$$25^{-1} \bmod 26=25$$

上面给出的 Z_{26} 上与 26 互素的元素逆元结论很容易通过乘法逆的定义进行验证，如 $11\times 19=209\equiv 1 \bmod 26$。

1.2.6 置换密码

前面几小节介绍的加密方式的共同特点是通过将英文字母改写成另一个表达形式来达到加密的效果。本节介绍另一种加密方式，通过重新排列消息中元素的位置而不改变元素本身的方式，对一个消息进行变换。这种加密机制称为置换密码(也称为换位密码)。置换密码是古典密码中除代换密码外的重要一类，它被广泛应用于现代分组密码的构造。

定义 1.2.5 置换密码体制 令 $m\geqslant 2$ 是一个正整数，$M=C=(Z_{26})^m$，K 是 $Z_m=\{1, 2, \cdots, m\}$上所有可能置换构成的集合。对任意的$(x_1, x_2, \cdots, x_m)\in M$，$\pi\in K$，$(y_1, y_2, \cdots, y_m)\in C$，定义

$$e_\pi(x_1, x_2, \cdots, x_m)=(x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(m)})$$

$$d_\pi(y_1, y_2, \cdots, y_m)=(y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \cdots, y_{\pi^{-1}(m)})$$

其中，π 和 π^{-1} 互为 Z_m 上的逆置换，m 称为分组长度。对于长度大于分组长度 m 的明文消息，可对明文消息先按照长度 m 进行分组，然后对每一个分组消息重复进行同样的置乱加密过程。

例 1.6 令 $m=4$，$\pi=(\pi(1), \pi(2), \pi(3), \pi(4))=(2, 4, 1, 3)$。假设明文为

Information security is important

加密过程首先根据 $m=4$，将明文分为 6 个分组，每个分组 4 个字符。

Info rmat ions ecur ityi simp orta nt

然后应用置换变换 π 加密成下面的密文：

noif mtra osin creu tiiy ipsm raot tn

解密密钥为

$$\pi^{-1}=(\pi(1)^{-1},\ \pi(2)^{-1},\ \pi(3)^{-1},\ \pi(4)^{-1})=(3,\ 1,\ 4,\ 2)$$

在以上加密过程中，首先应用给定的分组长度 m 对消息序列进行分组，当消息长度不是分组长度的整数倍时，可以在最后一段分组消息后面添加足够的特殊字符，从而保证能够以 m 为消息分组长度。例 1.6 中，我们在最后的分组消息 tn 后面增加了 2 个空格，以保证分组长度的一致性。

对于固定的分组长度 m，Z_m 上共有 $m!$ 种不同的排列，所以相应的置换密码共有 $m!$ 种不同的密钥。应注意的是，置换密码并未改变密文消息中英文字母的统计特性，所以置换密码对于抗频度分析技术来说是不安全的。

1.2.7 Hill 密码

置换密码的主要思想体现在“分组—置换”，置换方式过于简单会使其安全性不高。为了进一步增加安全性，1929 年 Hill 提出了一种多表代换密码——Hill 密码。该算法保留了置换密码的加密框架，所不同的是将分组后的每个部分采用线性变换的方式得到密文。即将明文消息按照步长 m 进行分组，对每一组的 m 个明文字母通过线性变换将其转换成 m 个相应的密文字母。这样密钥由一个较为简单的排列问题改变成较为复杂的 $m\times m$ 阶可逆矩阵。在使用 Hill 密码前，首先将英文的 26 个字母和数字 1～26 按自然顺序进行一一对应以方便处理。

定义 1.2.6 Hill 密码体制 令 $m\geqslant 2$ 是一个正整数，$M=C=(Z_{26})^m$，$\boldsymbol{K}$ 是定义在 Z_{26} 上的所有大小为 $m\times m$ 的可逆矩阵的集合。对任意的 $\boldsymbol{A}\in\boldsymbol{K}$，定义

$$e_A(x)=x\boldsymbol{A} \bmod 26$$

$$d_A(y)=y\boldsymbol{A}^{-1} \bmod 26$$

例 1.7 令 $m=4$，密钥为

$$\boldsymbol{A}=\begin{bmatrix}8 & 6 & 9 & 5\\ 6 & 9 & 5 & 10\\ 5 & 8 & 4 & 9\\ 10 & 6 & 11 & 4\end{bmatrix}$$

则相应的 Z_{26} 上的逆矩阵为

$$\boldsymbol{A}^{-1}=\begin{bmatrix}23 & 20 & 5 & 1\\ 2 & 11 & 18 & 1\\ 2 & 20 & 6 & 25\\ 25 & 2 & 22 & 25\end{bmatrix}$$

明文为

Hill

将以上明文转换成对应的数字序列

7 8 11 11

根据密钥 $\boldsymbol{A}$ 可知，相应的密文为

$$[y_1 \quad y_2 \quad y_3 \quad y_4]=[7 \quad 8 \quad 11 \quad 11]\cdot\begin{bmatrix}8 & 6 & 9 & 5\\ 6 & 9 & 5 & 10\\ 5 & 8 & 4 & 9\\ 10 & 6 & 11 & 4\end{bmatrix} \bmod 26$$

$$=[24 \quad 19 \quad 8 \quad 23]$$

于是相应的密文序列为

Ytix

已知密文消息和密钥 $\boldsymbol{A}$ 的逆矩阵 $\boldsymbol{A}^{-1}$，根据 Hill 密码体制的定义，对应的解密过程如下：

$$[x_1 \quad x_2 \quad x_3 \quad x_4]=[24 \quad 19 \quad 8 \quad 23]\cdot\begin{bmatrix}23 & 20 & 5 & 1\\ 2 & 11 & 18 & 1\\ 2 & 20 & 6 & 25\\ 25 & 2 & 22 & 15\end{bmatrix}$$

$$=[7 \quad 8 \quad 11 \quad 11]$$

于是相应的明文消息为 Hill。

通过例 1.7 可以发现，Hill 密码对于相同的明文字母，可能有不同的密文字母与之对应。一般情况下，Hill 密码能够较好地抵御基于字母出现频率的攻击方法。

在上面介绍的几个典型的古典密码体制里，含有两个基本操作：代换和置换。代换实现了英文字母外在形式上的改变；置换实现了英文字母所处位置的改变。这两个基本操作具有原理简单且容易实现的特点。随着计算机技术的飞速发展，古典密码体制的安全性已经无法满足实际应用的需要，但是代换和置换这两个基本操作仍是构造现代对称加密算法最重要的核心方式。举例来说，代换和置换操作在数据加密标准(DES)和高级加密标准(AES)中都起到了核心作用。几个简单密码算法的结合可以产生一个安全的密码算法，这就是简单密码仍被广泛使用的原因。除此之外，简单的代换和置换密码在密码协议上也有广泛的应用。

1.3 古典密码的统计分析

自从有了加密算法，对加密信息的破解技术就应运而生。加密算法的对立面称做密码分析，也就是研究密码算法的破译技术，加密和破译构成了一对矛盾体。假设攻击者 Oscar 完全能够截获 Alice 和 Bob 之间的通信，密码分析是指在不知道密钥的情况下恢复出明文的方法。根据密码分析的 Kerckhoffs 原则：攻击者知道所用的加密算法的内部机理，不知道的仅仅是加密算法所采用的加密密钥。常用的密码分析攻击分为以下四类：

(1) 惟密文攻击(Ciphertext Only Attack)：攻击者有一些消息的密文，这些密文都是用相同的加密算法进行加密得到的。攻击者的任务就是恢复出尽可能多的明文，或者能够推算出加密算法采用的密钥，以便可以采用相同的密钥解密出其他被加密的消息。