高等院校信息科学系列教材

现代密码学

陈鲁生　沈世镒　编著

科学出版社

高等院校信息科学系列教材

现代密码学

陈鲁生　沈世镒　编著

科学出版社

2002

内 容 简 介

本书系统地介绍现代密码学的基本内容，取材具有典型性. 全书共分9章，第1章介绍密码学中的一些基本概念，第2章介绍古典密码的加密方法和一些典型的古典密码体制，第3章介绍Shannon的密码学理论，第4章和第5章分别讨论分组密码和公钥密码，第6章介绍序列密码和线性移位寄存器序列，第7章和第8章分别讨论数字签名和Hash函数，第9章介绍一些重要的密码协议. 本书每章末均附有习题，其中有些习题是对正文内容的补充，以供学生复习巩固书中所学内容.

本书可作为高等院校信息科学专业或其他相关专业本科生的教材，也可作为相关领域中的教学、科研人员以及工程技术人员的参考书.

图书在版编目(CIP)数据

现代密码学/陈鲁生，沈世镒编著. —北京：科学出版社，2002
ISBN 7-03-010607-5

Ⅰ. 现… Ⅱ. ①陈… ②沈… Ⅲ. 密码-理论 Ⅳ. TN918.1

中国版本图书馆CIP数据核字(2002)第046822号

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2002年7月第 一 版 开本：720×1000
2002年7月第一次印刷 印张：10 1/2.
印数：1—5 000 字数：197 000

定价：14.00元

（如有印装质量问题，我社负责调换〈环伟〉）

序　言

1998年教育部进行高校专业调整时，设立了《信息与计算科学》专业. 该专业的设立，受到很多高等院校的热烈响应，据不完全统计，几年来已有约280所院校招收了该专业的本科生，其中大部分院校计划开设信息科学方面的系列课程.

为了配合高等院校在学科专业设置上的改革与深化，来自几十所高等院校的有关专业的部分领导和教师，于1999年、2000年召开了第一、二届《信息科学专业发展与学术研讨会》，与会者热烈讨论并探讨了许多与信息学科的学科发展和建设的基本问题. 会议一致认为教材建设是目前最为紧迫的任务，因此成立了教材编审协调组来组织该系列教材的编写.

2001年教材编写协调组召集了有多位经验丰富的教师和出版社参加的教材建设会议. 会议明确了教材建设是一项长期的工作，并决定首先编写和出版这套教材来满足近期急需. 为了保证教材的质量，会议对每本教材的要求、内容和大纲进行了具体研讨，并请具有多年教学经验的重点院校教授担任各教材的负责人.

为了贴近教学的实际，每部教材都配有习题或思考题，同时对内容也做了结构化安排，以便教师能根据实际情况部分选讲. 本套教学用书不仅适用于教学，也可供相关读者参考.

在教材编写和出版过程中，作者对内容的取舍、章节的安排、结构的设计以及表达方式等方面多方听取意见，并进行了反复修改. 在感谢作者们辛勤劳作的同时，编委会还特别感谢科学出版社的鞠丽娜编辑，她不辞辛劳，在统筹印刷出版、督促进度、征求意见、组织审校等方面做了大量工作. 这套教材能在保证质量的前提下，及时与读者见面，和她的努力是分不开的.

从长远的教学角度考虑，为了适应不同类型院校、不同要求的课程需要，教材编审协调组将不断组织教材的修订、编写(译)，从而使信息科学教学用书做到逐步充实、完善、提高和多样化. 在此衷心希望采用该系列用书的教师、学生和读者对书中存在的问题及时提出修改意见和建议.

高等院校信息科学系列教材编委会

2002年3月

前　言

随着计算机和通信网络的广泛应用，信息的安全性已受到人们的普遍重视. 信息安全已不仅仅局限于政治、军事以及外交等领域，而且现在也与人们的日常生活息息相关. 现在，密码学理论和技术已得到了迅速的发展，它是信息科学和技术中的一个重要研究领域.

多年来，我们一直在南开大学为信息科学专业的本科生和研究生讲授现代密码学课程，本书就是在此基础上编写而成的，旨在为高等院校信息科学专业或相关专业的本科生提供一本关于现代密码学的教材.

本书系统地介绍了现代密码学的基本内容. 全书共 9 章. 第 1 章介绍密码学中的一些基本概念. 第 2 章介绍古典密码，讨论了古典密码的基本加密方法和分析方法，并介绍了一些典型的古典密码体制. 第 3 章介绍 Shannon 的密码学理论. 第 4 章讨论分组密码，主要介绍数据加密标准 DES 和高级加密标准 AES，这是两种不同类型的分组密码. 第 5 章讨论公钥密码，介绍三种常见的公钥密码体制，并对公钥密码中用到的大素数的生成方法进行了讨论. 第 6 章介绍序列密码和线性移位寄存器序列. 第 7 章和第 8 章分别讨论数字签名和 Hash 函数. 第 9 章介绍一些重要的密码协议.

在本书的编写过程中，我们力求简明扼要，容易理解. 对书中介绍的密码体制的数学基础，我们都做了简明扼要的介绍. 书中所用到的数学结论基本上都做了证明，只有少数的数学结论由于证明过于复杂或者牵扯到更多的数学知识，我们只给出了结论，而没有给出证明，有兴趣的读者可以参阅相应的文献. 众所周知，如果没有相应的数学基础，要理解一个密码体制是困难的. 我们假定本书的读者具备了简单的概率论、高等代数、有限域以及数论等基本知识. 另外，了解一点有关计算复杂性的知识对于理解各种密码体制和密码协议是有用的. 由于严格地定义计算复杂性需要用到理论计算机科学中的一些知识，所以本书对此只做了一点简单的直观描述，感兴趣的读者可以参阅有关的文献.

本书适合高等院校信息科学、计算机科学以及通信等专业的高年级本科生使用，也可供相关领域的科研人员以及工程技术人员参考.

由于时间仓促，书中难免有疏漏和不当之处，敬请读者批评指正.

作　者

2002 年 5 月

试读结束：需要全本请在线购买：　www.ertongbook.com

目　录

第1章 引 言

1.1 密码学的发展概况

密码学是一门既古老又年轻的学科，其历史可以追溯到几千年以前.

古代的行帮暗语和一些文字猜迷游戏等，实际上就是对信息的加密. 这种加密方法通过原始的约定，把需要表达的信息限定在一定的范围内流通.

古典密码主要应用于政治、军事以及外交等领域，可以说，自从有了战争，就有了保密通信. 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.

在1949年之前，密码技术基本上可以说是一门技巧性很强的艺术，而不是一门科学. 在这一时期，密码专家常常是凭借直觉和信念来进行密码设计和分析，而不是推理证明.

在1949年，C. E. Shannon发表了“保密系统的通信理论(Communication Theory of Secrecy Systems)”一文，为密码学奠定了坚实的理论基础，使密码学成为一门真正的科学. 但从1949年至1975年，密码学的理论研究工作进展不大.

1976年，W. Diffie和M. E. Hellman发表了“密码学中的新方向(New Directions in Cryptography)”一文，提出了一种崭新的密码设计思想，导致了密码学的一场革命. 他们首次证明了从发送端到接收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元. 1977年，美国国家标准局(National Bureau of Standards)正式公布了数据加密标准DES(Data Encryption Standard)，将DES算法公开，从而揭开了密码学的神秘面纱. 从此，密码学的研究进入了一个崭新的时代.

随着计算机科学的蓬勃发展，社会已进入信息时代. 电子计算机和通信网络的广泛应用，一方面为人们的生活和工作提供了很大的方便，另一方面也提出了许多亟待解决的问题，其中信息的安全性就是一个突出的问题. 因此，密码学理论和技术已成为信息科学和技术中的一个重要研究领域. 随着计算机网络的迅速发展，特别是近年来电子商务的兴起，现代密码学的应用已不仅仅局限于政治、军事以及外交等领域，其商用价值和社会价值也已得到了充分的肯定.

1.2 密码学的基本概念

没有加密的信息称为明文(plaintext). 加密后的信息称为密文(ciphertext). 从明

文到密文的变换称为加密(encryption). 从密文到明文的变换称为解密(decryption).

加密和解密都是在密钥(key)的控制下进行的. 给定一个密钥,就可确定一对具体的加密变换和解密变换.

一个密码体制(cryptosystem)通常由五部分组成:

(1) 明文空间 $\mathscr{M}$:全体明文的集合.

(2) 密文空间 $\mathscr{C}$:全体密文的集合.

(3) 密钥空间 $\mathscr{K}$:全体密钥的集合. 通常每个密钥 k 都由加密密钥 k_e 和解密密钥 k_d 组成,$k=\langle k_e,k_d\rangle$,k_e 与 k_d 可能相同也可能不同.

(4) 加密算法 $\mathscr{E}$:由加密密钥控制的加密变换的集合.

(5) 解密算法 $\mathscr{D}$:由解密密钥控制的解密变换的集合.

设 $m\in\mathscr{M}$ 是一个明文,$k=\langle k_e,k_d\rangle\in\mathscr{K}$ 是一个密钥,则

$$c = E_{k_e}(m) \in \mathscr{C},$$

$$m = D_{k_d}(c) \in \mathscr{M},$$

其中 E_{k_e} 是由加密密钥 k_e 确定的加密变换,D_{k_d} 是由解密密钥 k_d 确定的解密变换. 在一个密码体制中,要求解密变换是加密变换的逆变换. 因此,对任意的 $m\in\mathscr{M}$ 都有

$$D_{k_d}(E_{k_e}(m)) = m$$

成立.

密钥空间中不同密钥的个数称为密码体制的密钥量. 它是衡量密码体制安全性的一个重要指标.

如果一个密码体制的加密密钥与解密密钥相同,则称其为单密钥密码体制或对称密码体制;否则,称其为双密钥密码体制或非对称密码体制.

在一个双密钥密码体制中,由加密密钥 k_e 计算解密密钥 k_d 是困难的,公开 k_e 不会损害 k_d 的安全性,则可以将加密密钥 k_e 公开. 这样的密码体制称为公钥密码体制(public-key cryptosystem).

一个好的密码体制至少应该满足下述两个条件:

(1) 在已知明文 m 和加密密钥 k_e 时,计算 $c=E_{k_e}(m)$容易. 在已知密文 c 和解密密钥 k_d 时,计算 $m=D_{k_d}(c)$容易.

(2) 在不知解密密钥 k_d 时,不可能由密文 c 推知明文 m.

对于一个密码体制,如果能够根据密文确定明文或密钥,或者能够根据明文和相应的密文确定密钥,则我们说这个密码体制是可破译的;否则,称其为不可破译的.

密码分析者攻击密码体制的方法主要有以下三种:

(1) 穷举攻击:密码分析者通过试遍所有的密钥来进行破译. 显然,可以通过增大密钥量来对抗穷举攻击.

(2) 统计分析攻击:密码分析者通过分析密文和明文的统计规律来破译密码.

对抗统计分析攻击的方法是设法使明文的统计特性与密文的统计特性不一样.

(3) 解密变换攻击:密码分析者针对加密变换的数学基础,通过数学求解的方法来设法找到相应的解密变换.为对抗这种攻击,应该选用具有坚实的数学基础和足够复杂的加密算法.

密码分析者通常可以在下述四种情况下对密码体制进行攻击:

(1) 唯密文攻击(ciphertext-only attack):密码分析者仅知道一些密文.

(2) 已知明文攻击(known-plaintext attack):密码分析者知道一些明文和相应的密文.

(3) 选择明文攻击(chosen-plaintext attack):密码分析者可以选择一些明文,并得到相应的密文.

(4) 选择密文攻击(chosen-ciphertext attack):密码分析者可以选择一些密文,并得到相应的明文.

其中唯密文攻击的强度最弱,其他情况下的攻击强度依次增加.

对于一个密码体制,如果密码分析者无论截获了多少密文以及无论用什么方法进行攻击都不能破译,则称其为绝对不可破译的密码体制.绝对不可破译的密码在理论上是存在的.但是,如果能够利用足够的资源,那么任何实际的密码都是可以破译的.因此,更有实际意义的是在计算上不可破译(computationally unbreakable)的密码.所谓计算上不可破译是指密码分析者根据可利用的资源来进行破译所用的时间非常长,或者破译的时间长到使原来的明文失去保密的价值.

应当指出,对任何一种攻击方法,我们都假定密码分析者事先知道所使用的密码体制,这一点称为 Kerckhoff 假设,是由 Auguste Kerckhoff(1835－1903)提出的.在设计密码体制时,应当记住的一点是永远不要低估密码分析者的能力.

图 1.1 给出的是一个密码系统模型.

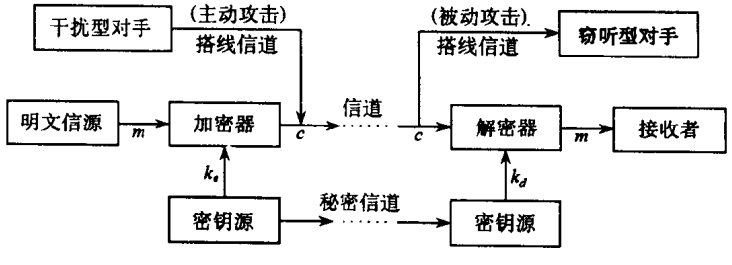

图 1.1 密码系统模型

密码系统的使用者通常称为用户.密码系统的破坏者有时称为对手.对手分为"窃听型"和"干扰型"两种."窃听型"对手只是截取信道上传送的信息,而"干扰型"对手则会篡改信道上传送的信息.

试读结束:需要全本请在线购买: www.ertongbook.com

第 2 章　古典密码

本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一些破译方法. 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是十分有益的.

2.1　古典密码中的基本加密运算

明文字母表 X 是指明文空间 $\mathscr{M}$ 中出现的所有不同的字母的集合. 密文字母表 Y 是指密文空间 $\mathscr{C}$ 中出现的所有不同的字母的集合.

对于一个密码体制,如果明文字母对应的密文字母在密文中保持不变,则称其为单表密码体制;如果明文中不同位置的同一明文字母在密文中对应的密文字母不同,则称其为多表密码体制.

设 q 是一个正整数,$Z_q=\{0,1,2,\cdots,q-1\}$,则 Z_q 在模 q 加法和模 q 乘法运算下构成一个交换环. 记 $Z_q^*=\{k\in Z_q \mid \gcd(k,q)=1\}$,则 Z_q^* 在模 q 乘法运算下构成一个乘法群,其中 $\gcd(k,q)$ 表示 k 和 q 的最大公因子.

2.1.1　单表古典密码中的基本加密运算

1. 加法密码

设 $X=Y=Z_q$,$\mathscr{K}=Z_q$. 对任意 $m\in X$,$k\in\mathscr{K}$,密文

$$c = E_k(m) = (m + k) \bmod q.$$

显然,加法密码的密钥量为 q.

2. 乘法密码

设 $X=Y=Z_q$,$\mathscr{K}=Z_q^*$. 对任意 $m\in X$,$k\in\mathscr{K}$,密文

$$c = E_k(m) = km \bmod q.$$

解密变换为

$$m = k^{-1}c \bmod q.$$

关于 k 模 q 求逆的算法将在 5.2.4 节中介绍. 显然,乘法密码的密钥量为 $\varphi(q)$. 这里 $\varphi(q)$ 是小于 q 且与 q 互素的非负整数的个数,称为 Euler 函数.

3. 仿射密码

设 $X=Y=Z_q$,$\mathscr{K}=\{(k_1,k_2)\mid k_1\in Z_q,k_2\in Z_q^*\}$. 对任意 $m\in X$,$k=(k_1,k_2)\in$

$\mathscr{K}$，密文

$$c = E_k(m) = (k_1 + k_2 m) \bmod q.$$

解密变换为

$$m = k_2^{-1}(c - k_1) \bmod q.$$

显然，加法密码和乘法密码都是仿射密码的特例. 仿射密码的密钥量为 $q\varphi(q)$.

4. 置换密码

设 $X=Y=Z_q$，$\mathscr{K}$ 为 Z_q 上全体置换的集合. 对任意 $m\in X$，$k=\sigma\in\mathscr{K}$，密文

$$c = E_k(m) = \sigma(m).$$

显然，仿射密码是置换密码的特例. 置换密码的密钥量为 $q!$.

2.1.2 多表古典密码中的基本加密运算

1. 简单加法密码

设 $X^n=Y^n=Z_q^n$，$\mathscr{K}=Z_q^n$. 对任意 $m=(m_1,m_2,\cdots,m_n)\in X^n$，$k=(k_1,k_2,\cdots,k_n)\in\mathscr{K}$，密文

$$c = E_k(m) = (m_1 + k_1, m_2 + k_2, \cdots, m_n + k_n),$$

其中的加法都是模 q 加法. 显然，简单加法密码的密钥量为 q^n.

2. 简单乘法密码

设 $X^n = Y^n = Z_q^n$，$\mathscr{K} = \{(k_1, k_2, \cdots, k_n) \mid k_i \in Z_q^*, 1 \leqslant i \leqslant n\}$. 对任意 $m=(m_1,m_2,\cdots,m_n)\in X^n$，$k=(k_1,k_2,\cdots,k_n)\in\mathscr{K}$，密文

$$c = E_k(m) = (k_1 m_1, k_2 m_2, \cdots, k_n m_n),$$

其中的乘法都是模 q 乘法. 显然，简单乘法密码的密钥量为 $\varphi(q)^n$.

3. 简单仿射密码

设 $X^n=Y^n=Z_q^n$，

$$\mathscr{K} = \{(\langle k_{11}, k_{21}\rangle, \langle k_{12}, k_{22}\rangle, \cdots, \langle k_{1n}, k_{2n}\rangle) \mid k_{1i} \in Z_q, k_{2i} \in Z_q^*, 1 \leqslant i \leqslant n\}.$$

对任意 $m=(m_1,m_2,\cdots,m_n)\in X^n$，$k=(\langle k_{11},k_{21}\rangle,\langle k_{12},k_{22}\rangle,\cdots,\langle k_{1n},k_{2n}\rangle)\in\mathscr{K}$，密文

$$c = E_k(m) = (k_{11} + k_{21} m_1, k_{12} + k_{22} m_2, \cdots, k_{1n} + k_{2n} m_n),$$

其中的加法和乘法都是模 q 加法和乘法. 显然，简单仿射密码的密钥量为 $q^n\varphi(q)^n$.

4. 简单置换密码

设 $X^n=Y^n=Z_q^n$，$\mathscr{K}=\{(k_1,k_2,\cdots,k_n)\mid k_i$ 是 Z_q 上的置换，$1\leqslant i\leqslant n\}$. 对任意 $m=(m_1,m_2,\cdots,m_n)\in X^n$，$k=(k_1,k_2,\cdots,k_n)\in\mathscr{K}$，密文

$$c = E_k(m) = (k_1(m_1), k_2(m_2), \cdots, k_n(m_n)).$$

显然，简单置换密码的密钥量为$(q!)^n$.

5. 换位密码

设$X^n=Y^n=Z_q^n$，密钥空间$\mathscr{K}$为$\{1,2,\cdots,n\}$上的全体置换的集合. 对任意明文$m=(m_1,m_2,\cdots,m_n)\in X^n$，$k=\sigma\in\mathscr{K}$，密文

$$c=E_k(m)=(m_{\sigma(1)},m_{\sigma(2)},\cdots,m_{\sigma(n)}).$$

显然，换位密码的密钥量为$n!$.

6. 广义置换密码

设$X^n=Y^n=Z_q^n$，$\mathscr{K}$为Z_q^n上的全体置换的集合. 对任意$m\in X^n$，$k=\sigma\in\mathscr{K}$，密文

$$c=E_k(m)=\sigma(m).$$

显然，广义置换密码的密钥量为$(q^n)!$.

7. 广义仿射密码

设$X^n=Y^n=Z_q^n$，$\mathscr{K}=\{(\alpha,H)\mid\alpha\in Z_q^n$，$H$为$Z_q$上的$n$阶可逆方阵$\}$. 对任意$m=(m_1,m_2,\cdots,m_n)\in X^n$，$k=(\alpha,H)\in\mathscr{K}$，密文

$$c=E_k(m)=\alpha+mH,$$

其中的运算都是模q运算. 显然，广义仿射密码的密钥量为$q^n r_n$，其中r_n是Z_q上不同的n阶可逆方阵的个数.

2.2 几种典型的古典密码体制

表2.1给出了英文字母表{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}和整数集Z_{26}之间的一一对应关系.

表2.1 字母与数字的对应关系

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

为方便起见，在本节中表示字母的符号同时也将表示字母所对应的整数，根据上下文能够容易地区分一个符号是表示字母还是表示字母所对应的整数.

2.2.1 几种典型的单表古典密码体制

1. Caesar 体制

Caesar 体制是一种典型的加法密码，其密钥 $k=3$. 表 2.2 给出了 Caesar 体制中明文字母与密文字母的对应关系.

表 2.2 Caesar 密表

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

2. 标准字头密码体制

这是一种置换密码. 它利用一个密钥字来构造置换作为密钥. 譬如，如果选择 cipher 作为密钥字，则标准字头密码体制中明文字母与密文字母的对应关系如表 2.3 所示.

表 2.3 标准字头密码体制的密表

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	c	i	p	h	e	r	a	b	d	f	g	j	k	l	m	n	o	q	s	t	u	v	w	x	y	z

2.2.2 几种典型的多表古典密码体制

1. Playfair 体制

Playfair 体制被英国军队作为一种战地密码体制使用多年，在第一次世界大战期间，美国和英国军队使用过一段时间. Playfair 体制是由英国的著名科学家——“Wheatstone 电桥”的设计者 Charles Wheatstone 发明的，但名字取自于率先发起应用这种密码体制的 Liones Playfair.

Playfair 体制的密钥是一个 5×5 的矩阵 $P=(p_{ij})_{5\times5}$. 构造方法如下：

(1) 构造字母表{a,b,c,d,e,f,g,h,i,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}的一个置换. 这里将 j 当作 i，实际上只有 25 个字母.

(2) 将上述置换按行排列成一个 5×5 的矩阵 $P=(p_{ij})_{5\times5}$.

用 Playfair 体制对明文字母串进行加密时，首先在明文字母串的适当位置插入一些特定的字母，譬如字母 q，使得明文字母串的长度为偶数，并且将明文字母串按两个字母一组进行分组，每组中的两个字母不同. 对任意的明文字母对 m_1m_2，

设它们对应的密文对为 c_1c_2，加密方法如下：

(1) 如果 m_1 和 m_2 在 P 中同一行，则密文 c_1 和 c_2 分别为紧靠 m_1 和 m_2 右端的字母. 这里将第一列看作是最后一列的右端.

(2) 如果 m_1 和 m_2 在 P 中同一列，则密文 c_1 和 c_2 分别为紧靠 m_1 和 m_2 下方的字母. 这里将第一行看作是最后一行的下方.

(3) 如果 m_1 和 m_2 既不在 P 中的同一行，也不在同一列，则密文 c_1 和 c_2 分别为由 m_1 和 m_2 确定的矩形的其他两个角上的字母. c_1 和 m_1 同行，c_2 和 m_2 同行.

例 2.1 设密钥矩阵

$$P=\begin{pmatrix} c & i & p & h & e \\ r & a & b & d & f \\ g & k & l & m & n \\ o & q & s & t & u \\ v & w & x & y & z \end{pmatrix},$$

明文为

Playfair cipher was actually invented by wheatstone.

将明文分组为

pl ay fa ir ci ph er wa sa ct ua lq
ly in ve nt ed by wh ea ts to ne

则密文为

bs dw rb ca ip he cf ik qb ho qf ks
mx ek zc mu hf dx yi if ut uq uf □

2. Vigenere 体制

Vigenere 体制是 1586 年由法国密码学家 Blaise de Vigenere 发明的. Vigenere 体制就是多表简单加法密码.

设明文 $m=m_1m_2\cdots m_n$，密钥 $k=k_1k_2\cdots k_n$，则密文

$$c=E_k(m)=c_1c_2\cdots c_n,$$

其中 $c_i=(m_i+k_i) \bmod 26, i=1,2,\cdots,n$.

当密钥的长度比明文短时，密钥可以周期性地重复使用，直至完成明文中每个字母的加密.

表 2.4 称为 Vigenere 方阵，利用它可以方便地进行加密和解密. 当用密钥字母 k_i 对明文字母 m_i 进行加密时，Vigenere 方阵中的第 k_i 行第 m_i 列的字母就是相应的密文字母.

表 2.4 Vigenere 方阵

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

例 2.2 设明文为

This cryptosystem is not secure,

密钥为 cipher，则密文为

VPXZGI AXIVWP UBTTMJ PWIZIT WZT. □

3. Beaufort 体制

Beaufort 体制与 Vigenere 体制非常相似，也是一种多表简单加法密码.

试读结束：需要全本请在线购买： www.ertongbook.com