天津市科协专著基金
TAST Fund For Academic Publications

应用统计与信息丛书

近代密码学

Modern Cryptography

沈世镒 编著
By Shen Shiyi

广西师范大学出版社
Guangxi Normal University Press

应用统计与信息丛书

近代密码学

沈世镒 编著

广西师范大学出版社
Guangxi Normal University Press

近代密码学

南开大学　沈仕鎰

责任编辑：余鑫晖　　封面设计：张　明　涂灵策

广西师范大学出版社出版发行　　邮政编码：541001

（广西桂林市中华路 36 号）

核工业中南 310 印刷厂印刷

*

开本：850×1168　1/32　　印张：5.375　　字数：135 千字

1998 年 11 月第 1 版　　1998 年 11 月第 1 次印刷

印数：0001～1000 册

ISBN 7-5633-2761-4/O・031

定价：（精）11.00 元

出　版　说　明

即将到来的21世纪是一个信息的时代，掌握信息、了解信息、处理信息是企业、政府、个人必须面对的问题，信息处理中统计方法是十分重要的，因此我们出版这一套《应用统计与信息丛书》，来推动这一方面的发展.

我们聘请了国内统计与信息方面的著名专家，撰写一系列的著作，结合国内实际，介绍国外的动向，发挥自己的专长，就一个个主题作深入浅出的讨论，既能使广大的读者受益，又有相当的学术水平，把我国的应用统计与信息处理推向一个新的高峰.

希望这套丛书的出版能受到读者的欢迎.

广西师范大学出版社
1998年8月

有 关 记 号

X,Y,Z,K：集合记号，在密码体制中分别表示信号空间或字母表.

A,B,C,D：集合记号，或子集合记号.

x,y,z,k,a,b,c,d：字母、符号或元素记号.

$A\cup B,A\cap B$(或 AB)，$A\backslash B$：分别为集合 A 与 B 的并、交、差集.

$A\times B$：集合 A 与 B 的积，这时 $A\times B=\{(a,b):a\in A,b\in B\}$.

A^C：集合 A 的余集，这时 $A^C=X\backslash A$.

$\varnothing$：空集记号.

$F_2=\{0,1\}$：二元域.

$\{0,1\},\{\pm1\}=\{-1,+1\}$：二元集合(或二元空间).

$R=(-\infty,\infty)$：实数空间.

$Z=\{\cdots,-1,0,1,2,\cdots\}$：全体整数集合.

$Z_0=\{0,1,2,\cdots\}$：全体非负数集合.

$Z_+=\{1,2,3,\cdots\}$：全体自然数集合.

$N=\{1,2,\cdots,n\},K=\{1,2,\cdots,k\}$：非负整数集合.

英文大写字母有时也表示算子或矩阵，如 $T(\quad)$ 为算子；

又如 $M=[M_{i,j}]_{n\times n}$ 表示 $n\times n$-阶矩阵.

$\alpha=\alpha(k)=\{i(1),i(2),\cdots,i(k)\}$：集合 N 中的子集，其中

$$1\leqslant i(1)<i(2)<\cdots<i(k)\leqslant n.$$

$Z_q=\{0,1,\cdots,q-1\}$：q-元环或域.

$GF(q)$：q-元域.

$a+b,a\cdot b$(或 ab)：$GF(q)$域或 Z_q 环中的加、乘运算.

$F_a[x], F_q[x]_{p(x)}$：域 F_q 上的多项式环.

$f(x), g(x), h(x), f(x_1, \cdots, x_n)$：一元或多元多项式.

∂f：多项式的阶.

$X^{(n)} = \prod_{i=1}^{n} X_i$，$X_i = X$：$X$ 的 n-维乘积空间.

$X^{\infty} = \prod_{i=1}^{\infty} X_i$，$X_i = X$：$X$ 的无穷维乘积空间.

$Y^{(n)}, Z^{(n)}, U^{(n)}, V^{(n)}$：与 $X^{(n)}$ 类似定义.

$x^{(n)} = (x_1, x_2, \cdots, x_n)$：$X^{(n)}$ 空间中的向量，其中 $x_i \in X$.

$y^{(n)}, z^{(n)}, u^{(n)}, w^{(n)}$：与 $x^{(n)}$ 类似定义.

$0^{(n)} = (\overbrace{0, 0, \cdots, 0}^{n\text{个}})$：$n$-维零向量.

$1^{(n)} = (\overbrace{1, 1, \cdots, 1}^{n\text{个}})$：$n$-维幺向量.

$x^{\infty} = (x_1, x_2, \cdots)$：$X^{\infty}$ 空间中无穷维向量.

$X \oplus Y$：线性空间 X, Y 的直和，$X \oplus Y = \{x + y : x \in X, y \in Y\}$.

$x(\alpha) = (x_i : i \in \alpha) = (x_{i(1)}, x_{i(2)}, \cdots, x_{i(k)})$：$x^n$ 的子向量，其中 $\alpha = \{i(1), \cdots, i(k)\}$.

σ^n：数 σ 的 n 次幂. 当 σ 表示置换或轮换运算时，σ^n 表示运算 σ 的 n 次幂运算.

T：算子(如推移算子，矩阵算子等).

$T^n = \overbrace{T(T(\cdots T(}^{n\text{个}} \quad \overbrace{)\cdots)}^{n\text{个}})$：算子 T 的 n 次幂.

$A^{(n,m)} = [a_{i,j}]_{n \times m}$：$n \times m$-阶矩阵，或 n-行，m-列矩阵.

$A^T = [a_{j,i}]_{m \times n}$：矩阵 A 的转置矩阵.

$I^{(n)} = [\delta_{i,j}]_{(n,n)}$：$n$-阶幺矩阵，其中 $\delta_{i,j} = \begin{cases} 1, & \text{如果 } i = j, \\ 0, & \text{否则.} \end{cases}$

$a_{i\cdot} = (a_{i,1}, a_{i,2}, \cdots, a_{i,n})$：$A$ 矩阵的行向量；

$a_{\cdot,j}=(a_{1,j},a_{2,j},\cdots,a_{n,j})$：$A$ 矩阵的列向量.

$(x^{(n)},y^{(n)})=\sum_{i=1}^{n}x_i\cdot y_i$：向量 $x^{(n)}$ 与 $y^{(n)}$ 的内积.

$|A|$：如果 A 是矩阵时，$|A|$ 为 A 矩阵的行列式；

如果 A 是向量 $x^{(n)}$ 时，$|x^{(n)}|$ 为向量 $x^{(n)}$ 的模.

$|a|$：数 a 的绝对值.

$\|A\|$：集合 A 的元素个数.

$d_H(x^{(n)},y^{(n)})=\sum_{i=1}^{n}d_H(x_i,y_i)$：离散向量 $x^{(n)}$ 与 $y^{(n)}$ 的 Hamming 距离.

$d_H(x^{(n)})=\sum_{i=1}^{n}d_H(x_i)$：离散向量 $x^{(n)}$ 的 Hamming 势，其中

$$d_H(x_i,y_i)=\begin{cases}0,\text{ 当 } x_i=y_i \text{ 时},\\ 1,\text{ 否则},\end{cases}\qquad d_H(x_i)=\begin{cases}0,\text{ 当 } x_i=0 \text{ 时},\\ 1,\text{ 否则}.\end{cases}$$

$d(x^{(n)},y^{(n)})=\sum_{i=1}^{n}(x_i-y_i)^2$：向量 $x^{(n)}$ 与 $y^{(n)}$ 的欧几里德距离.

$d(x^{(n)})=\sum_{i=1}^{n}(x_i)^2$：向量 $x^{(n)}$ 的欧几里德势(或长度).

$\exp(z),\exp_2(z)$：指数函数，分别以 e 与 2 为底.

$\ln(z),\log_2(z)$：对数函数，分别以 e 与 2 为底.

ξ,η,ζ(或 x^*,y^*,z^*)：分别取值于 X,Y,Z 空间的随机变量.

(ξ,η)：取值于 $X\times Y$ 空间的二维随机向量.

$\xi^{(n)}=(\xi_1,\xi_2,\cdots,\xi_n)$：取值于 $X^{(n)}$ 的随机向量.

$p(A)$：事件 A 的概率.

$p(z)$：随机事件 $\xi=z$ 的概率或概率分布密度.

$P_r\{\xi\in A\},P_r\{\xi\in A|\eta\in B\}$：概率与条件概率记号.

$p(A|B)$：事件 A 关于事件 B 的条件概率.

$p(x|y)$：$\xi=x$ 关于 $\eta=y$ 的条件概率或条件概率分布密度.

$p^{(n)}=(p_1,p_2,\cdots,p_n),q^{(n)}=(q_1,q_2,\cdots,q_n)$：离散型随机变量

的概率分布，其中

$$p_i \geqslant 0,\ i=1,2,\cdots,n,\ \sum_{i=1}^{n} p_i = 1;$$

$$q_i \geqslant 0,\ i=1,2,\cdots,n,\ \sum_{i=1}^{n} q_i = 1.$$

$\mathrm{E}\{\xi\}$：随机变量 ξ 的数学期望（或均值）.

$\mathrm{Var}(\xi)$：随机变量 ξ 的方差.

$\mathrm{Cov}(\xi,\eta)=\mathrm{E}\{(\xi-E\xi)(\eta-E\eta)\}$：随机变量 (ξ,η) 的协方差.

$G=\{A,L\}$：图，其中 A 为图 G 的点集，L 为图 G 的弧集.

$\mathrm{H}(\varepsilon)=-\varepsilon\log_2\varepsilon-(1-\varepsilon)\log_2(1-\varepsilon)$：二元 Shannon 熵.

$\mathrm{H}(p^{(n)})=-\sum_{i=1}^{n} p_i\log_2 p_i$：离散型随机变量（或概率分布）的 Shannon 熵.

$\mathrm{H}(p)=-\int_R p(x)\log_2 p(x)\mathrm{d}x$：连续型随机变量（或概率分布）的 Shannon 熵.

$\mathrm{D}(p^{(n)},\ q^{(n)})=\sum_{i=1}^{n} q_i\log_2\frac{q_i}{p_i}$：概率分布 $p^{(n)}$ 对 $q^{(n)}$ 的互熵（或 Kullback 熵）.

目　　录

第一部分　概论，古典密码学

第一章　概论

§1.1　发展历史与意义

1. 密码学的发展历史

密码学的发展历史大体上分为三个阶段，即古代加密方法，古典密码体制与近代密码体制.

古代加密方法的事例很多，如古希腊墓碑的铭文志，我国古代的行帮会话等. 这种加密方法通过原始的约定，把需要表达的内容限制在一定范围内流通. 这种加密方法已体现了密码学的若干要素，但它的迅速发展还是随着通信技术迅速发展的要求而发展的.

古典密码体制是在有线与无线电通讯产生后兴起，尤其是在军事上，由于无线电通讯的普遍使用，“密电码”就显得格外重要. 它的加密一般通过某种方式的文字置换进行，这种文字置换一般通过某种手工或机械变换方式进行转换，同时简单地使用了数学运算. 著名的 CASER 加密体制就是典型的一种古典密码体制. 古典密码体制发展的终点是二战时期的转轮体制，这是一种用机械转动与电路相结合的加密方法，在二战时期普遍使用.

近代密码体制的主要标志是密码体制与计算机密切结合，无论是它的算法还是它的应用目标都与计算机、电子通信技术密不可分. 另外，在理论方法与应用范围上都有很大的扩张. 其应用范围由政府、军事领域扩展到民间各个领域，如企业、金融、新闻、商

业乃至个人生活等许多方面.而其理论方法的多样性也十分明显，各种加密思想，加密方法，加、解密的算法体制不断出现，同时为了论证各种加密方法的安全性，相应的理论分析与复杂度指标也相继出现，内容十分丰富.

2. 密码学的发展意义

密码学的发展意义是十分明显的.一系列战争的实例说明了密码学是取得战争胜利的重要条件，尤其在近代战争中，电子密码战是其他形式战争的先导.同时，近代密码学在政治、外交、新闻、金融中发挥重要作用.例如，新闻报导的时间差在新闻价值中起关键作用，因此密码学在各通信社的新闻战中发挥重要作用；又如，在金融业中，对大量用户的计算机管理及各种形式的金融卡与电子货币的出现，密码学是金融业实行安全管理的必不可少的一个组成部分，同时也与一般居民发生密切关系.

特别值得一提的是，密码学的作用在计算机网络、国际互联网络中的作用更为突出.人们往往把计算机网络比作信息传递公路（或高速公路），那么密码学就是高速公路上的管理系统，只有在密码学管理下的数据运行才是安全的.

密码学的发展推动了电子技术、计算机技术与数学等学科的发展.众所周知，计算机就是二战期间进行密码分析而产生的，目前在许多国家中，计算机的最大用户仍然是密码学的用户.

3. 密码学的分类

密码学大体分为密码体制、密码分析与数据安全三大部分，它们相互沟通但各有特点.

密码体制主要研究密码的构造与加、解密的算法，它是密码理论的基础，也是保密系统设计的基础.

密码分析主要是指对加密信号的攻击分析，其目的是通过密

文获取对方的真实信息.在进行密码体制设计时,必须与密码分析同时考虑,也就是在进行密码体制设计时,必须是地考虑密码分析中的安全性的条件与指标,否则所设计的密码体制是不可靠的.因此,密码体制与密码分析的研究是密切不可分的.

所谓数据安全是指对数据防干扰,防破坏.其中包括防病毒、防丢失、密钥管理等一系列问题.另外,从学科内容来看,密码学除了理论研究之外,还包括软件、芯片与系统的建立与开发,网络系统中的数据管理等.它们是针对不同的使用部分与不同的层次要求进行的研究内容.

关于密码学的发展情况可见[5],[9],[10],[11],[15],[21],[22],[27],[45],[50]等文.

4.本著作的基本内容

本著作主要介绍密码学的基本原理与基本内容,内容分一般理论与古典密码学、近代密码学和序列密码学三大部分.其中一般理论与古典密码学介绍密码学发展的简单历史与建立密码学的基本原理与意义;近代密码学主要介绍国际上流行的几种码体制的构造与应用特征;而序列密码学则是研究最为深入的一种密码理论,同时在应用上也有重要意义.

§1.2 密码体制的基本原则

密码体制的基本原则是指在进行密码体制设计或评价时应考虑的基本原则.常用的密码体制的基本原则有以下六项:

原则一 不可破原则

所谓不可破原则是指该密码体制在理论上或实际上是不可破的.所谓理论上不可破,是指密钥变化的范围是一个无穷大量,无

论用任何计算方法，都无法破译. 理论上不可破的密码体制是一种理想的密码体制，在密钥用计算机生成的条件下，理论上不可破的密码体制是无法实现的. 因此，实际使用的密码体制都是实际上是不可破的密码体制.

实际上是不可破的密码体制是指在不同情况下，对密码体制的强度可以有不同的要求. 例如：

(1) 要破译该密码体制的实际计算量(计算时间或费用)十分巨大，以至在实际上是无法实现的.

(2) 要破译该密码体制所需要的计算时间超过该体制包含信息的有效时间，如新闻报导消息，需要保密的时间往往只有几个小时.

(3) 要破译该密码体制的费用超过该体制包含信息的价值，以至不值得去破译它.

原则二　部分信息丢失不危及整个系统的安全

一个加密系统是由许多部分组成的，如硬件设备、加密算法、管理人员等，这些因素都可能为该密码体制提供一些信息. 这些信息的丢失不危及整个系统的安全，即使这些信息全部为对手掌握，也不会使整个系统的安全受到威胁.

部分信息的另外一个含义是指全部密文与部分明文(如已过时的明文信息)，这些信息的丢失仍不会危及整个系统的安全.

因此，近代密码学的加密强度主要体现在密钥上，可使用的密钥不仅数量上要足够多，使对手无法猜出，而且可以随时更换.

原则三　与计算机、通信系统匹配原则

这就是指密码体制不独立存在，它必须在计算机或通信系统中使用，并与之匹配.

原则四　费用是便宜的

为加密所需的附加费用应是便宜的，因加密所需的附加费用一般不超过设备总费用的 10%.

原则五　设备是轻便的

要求设备是轻便的，在计算机系统中，只可增加一个插片或一个芯片卡. 其专用设备一般要求是轻便小巧的.

原则六　使用是简单的

一般要求操作人员是非专业密码人员，经短期简单培训就可掌握使用.

以上六原则可简化为：理论或实际的不可破性；加密的关键问题是密钥，密钥是可随时更改的；成本低廉与使用简单四个要点. 在密码学中，涉及的原则还有很多，例如 Shannon 的密码体制构造等，它们对这些问题还有更为精确的定量化说明，对此我们以后还要论述.

§1.3　密码学的基本要素

密码学的基本要素是指我们在研究密码学所涉及的基本内容，同时我们也要解释密码学中的基本名词与概念. 密码学的基本要素有：

1. 明文信源

明文系指一般人们能懂得的语言、文字与符号. 明文信源是指产生明文的来源，如电报局每日发送的电报等. 在数学上，一个明文信源可用一个具有概率分布的随机过程来描述.

2. 密文、密钥、加密运算与密钥空间

密文是加工后的明文，非授权者无法看懂. 明文加工成密文的运算为加密运算，一个加密体制的加密运算是由一个算法类组成，这个算法类中不同的运算可用不同的参数来表示，这些参数分别代表不同的加密算法，我们称之为密钥. 密钥参数的取值范围叫密钥空间.

3. 密码体制

密码体制一般是指密钥空间与相应的加密运算结构，但同时还包括明文信源与密文的结构特征，这些结构特征对我们建立加密运算与密钥空间是有直接关系的.

4. 用户与对手

密码体制的使用者为用户，而密码体制的破坏者为对手.

对手的类型分“窃听型”与“干扰型”两种. “窃听型”是从密码体制中窃取数据，达到获取对方信息的目的. 而“干扰型”是向密码体制输入数据，达到破坏对方获得正确信息的目的.

关于密码体制的信息传递框图如下：

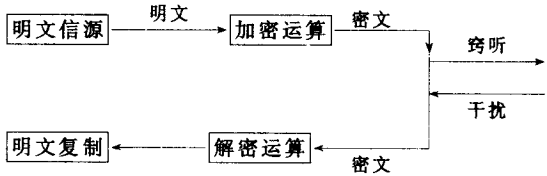

图 1.3.1　密码体制的信息传递框图

因此，密码体制的设计必须同时考虑防“窃听”与防“干扰”的两种保护手段. 对这两种不同的保护手段，在密码学中既有共同的基础，也有不同的处理方式.

§1.4 若干数学工具

如上所述，近代密码学是一门涉及多学科的新型学科，是计算机科学与数学的交叉结合. 如计算机科学与数学中的复杂性理论是密码分析学的基础，而复杂性理论本身就是计算机科学与数学结合的产物. 另外，在数学中还涉及到数论、代数学、组合学、图论与概率统计理论等. 对在本书中涉及到的这些问题我们将在各章节中作简要论述与介绍，使非数学专业的读者也能阅读本书.

由于本书中基本内容都是在有限域(或有限环)中讨论，因此本书中所涉及的运算都是有限域(或有限环)中的运算，对特殊情形我们另作说明.