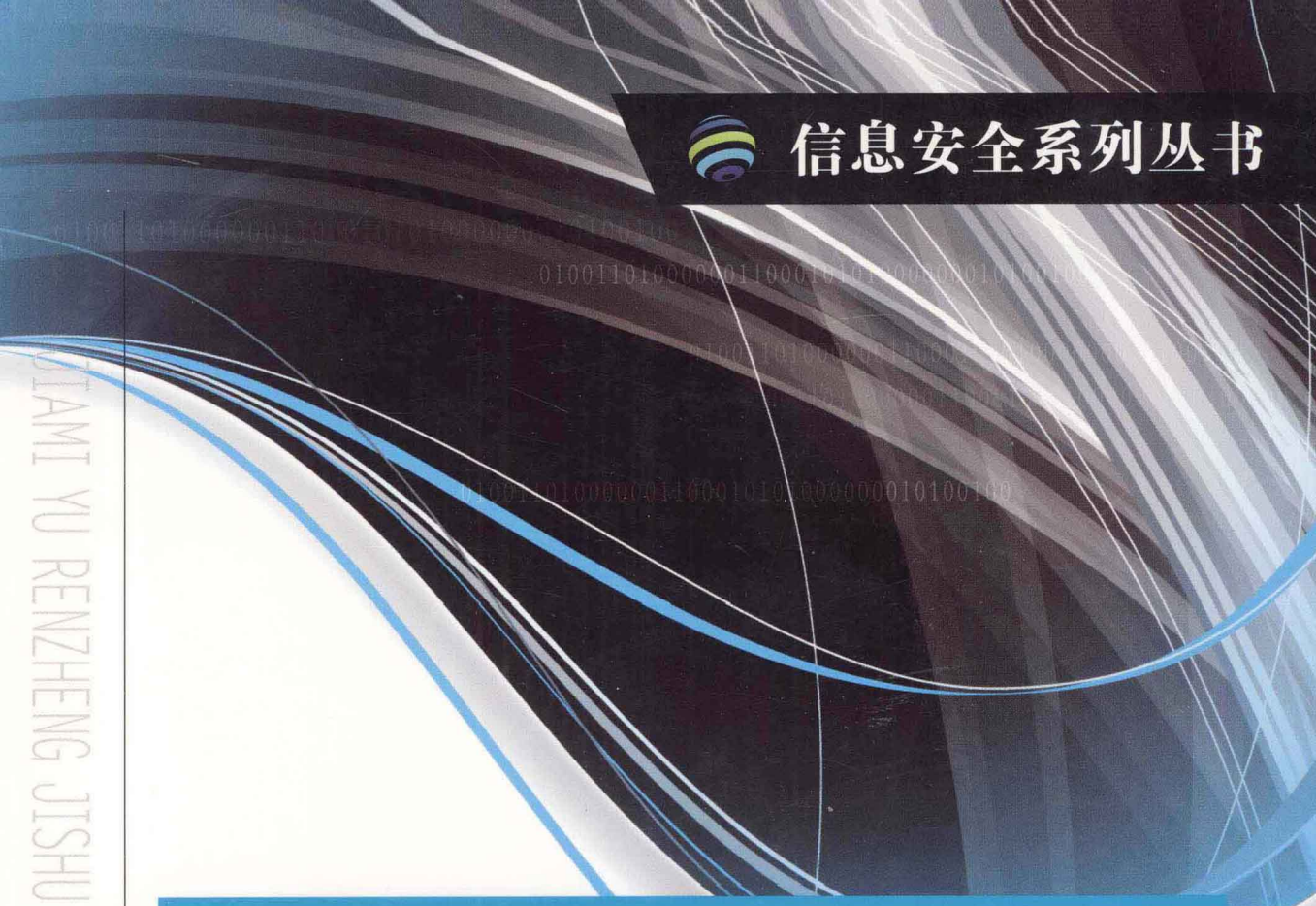

信息安全系列丛书

JIAMI YU RENZHENG JISHU DE SHUXUE JICHU

加密与认证技术的数学基础

张焕炯 编著

- 数学知识与加密和认证技术的完美结合
- 透彻介绍知识点的实质内容和背景
- 强调基本的思路和方法的训练

国防工业出版社
National Defense Industry Press

信息安全系列丛书

加密与认证技术的数学基础

张焕炯　编著

国防工业出版社

·北京·

内 容 简 介

本书系统地介绍了加密算法与认证技术所需要的数学基础知识，它们涉及到布尔代数、线性代数、数论、抽象代数和椭圆曲线等内容，并就这些数学知识在加密与认证等技术中的应用也进行了简要的分析介绍。本书共分8章，第1章介绍了加密与认证技术与相关数学基础的关系；第2章介绍了布尔代数中的有关异或运算的性质；第3章重点论述了矩阵的相关运算；第4章着重介绍了整数之间的相除及最大公因数、最小公倍数等相关知识；第5章涉及同余及同余式的求解问题，对各种同余式及同余式组的解的存在性、解的个数及如何求解进行了深入分析；第6章涉及素性检验问题，对各种重要的素性检验方法进行了梳理，这其中也包括某些最新的检验方法；第7章分别就群、环、域和模等抽象代数的基本概念进行梳理分析；第8章主要介绍了椭圆曲线的相关性质。这样把包括三个数学难解问题在内的、面向单钥制和双钥制加密及相关认证技术的数学基础知识进行了完整的梳理，构成了相对完备的数学知识体系。

本书注重思想方法和技能的训练及培养，可作为信息安全、通信工程、信息工程及计算机专业等本科生及相关研究生的教材，也可作为从事相关专业科研、工程技术等人员的参考书。

图书在版编目(CIP)数据

加密与认证技术的数学基础/张焕炯编著. —北京：国防工业出版社，2013.6
(信息安全系列丛书)
ISBN 978-7-118-08803-8

Ⅰ.①加... Ⅱ.①张... Ⅲ.①加密技术②认证协议 Ⅳ.①TN918

中国版本图书馆CIP数据核字(2013)第134778号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路23号 邮政编码100048)
北京嘉恒彩色印刷责任有限公司
新华书店经售
*
开本 787×1092 1/16 印张 9¾ 字数 219千字
2013年6月第1版第1次印刷 印数 1—2500册 定价 29.00元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776
发行传真：(010)88540755 发行业务：(010)88540717

前　言

本书主要介绍用于加密算法和认证技术的数学基础知识，为了佐证所介绍的数学的有用性，也简要地涉及到加密算法和认证技术本身的相关内容。

在信息安全成为研究和应用的热点当下，如何提供完备而又紧致的数学基础知识，使信息安全中的基本理论和方法能成为自我完备的知识体系，这不仅是信息安全知识体系自身的需要，也是信息安全学科的一种内在要求，更是信息安全专业人才培养中最基本的前提条件之一。

分析信息安全的相关知识体系结构，不难发现，加密算法和认证技术是其中最主要的部分，信息安全的理论发展和技术创新离不开这两个部分，所以加密算法和认证技术的支撑理论自然成了不折不扣的基础知识，因此把在加密算法和认证技术中用到的数学知识进行归纳，把它们辑成一个整体，就构成了《加密与认证技术的数学基础》这样一本书籍。相比较于其他相关的书籍，本书有以下基本特点：一是，它针对重要的加密算法和认证技术，把数学知识与相应的加密和认证技术等进行了具体的知识链接，实现了抽象知识与具体应用的较好结合，更把相关的数学理论与密码学和认证技术中的知识进行互相印证，既顾及到了相关数学的抽象性，又能尽可能地展现这些知识的应用性特性，使得学生学习这些知识时能最大限度地减少认知上的抽象性观感和畏难情绪，并尽可能激发他们学好该课程的内在动力；二是，在介绍知识点时，在尽可能体现知识的严谨性和紧致性的同时，努力通过诸如举例、类比等手法来透彻地介绍实质内容和相应的背景；三是，本着“授人以渔”的想法，强调基本的思路和方法的训练，培养如何解决问题的能力等。

本书共分8章，第1章为绪言；第2章为布尔代数理论中的有关异或运算的相关知识介绍；第3章介绍线性代数中的向量与矩阵等的基本内容；第4章介绍数论中的整数整除运算等基本的概念；第5章着重介绍同余式的求解，分别介绍了一次同余式、二次同余式，及高次同余式的解的存在性、解的个数及相关同余式解的具体解法等；第6章讨论素性检验问题，对主要的几种素性检验方法进行了深入探讨；第7章介绍抽象代数的相关内容，分别介绍了群、环、域和模的相关知识；第8章介绍椭圆曲线及基于椭圆曲线上的离散对数难解问题的密钥体制。这样，把目前最主要的加密算法和认证技术所需要的数学知识进行了完备的论述。

因为某种机缘，本人要讲授“信息安全数学基础”课程，因时时思考如何把这门课程讲好，让学生接受相应知识的同时，更有一种思想方法和技能的训练和相应能力的提高，若干年下来，积累了一些心得体会，在试着把这些心得体会用到具体的授课中的同时，也

希望把它记录下来形成文字，这便成了编写这本书的最深层的一个动因。

本书是在学习其他优秀教材等资料的基础上撰写而成的，对提供优质资料的相关专家表示真挚的谢意。虽然书稿的具体撰写和相关结论的推演过程相对枯燥而进程缓慢，但也不乏有乐在其中的真切体验，度过了很多快乐的好时光。此外，感谢家人的支持和鼓励，他们对我的帮助让我忘记背后、努力面前，向着标杆直跑。

张焕炯

2013 年 5 月于杭州

目　录

第1章 绪 言

1.1 加密与认证技术

目前,信息安全不仅涉及到传统的通信、政治、军事、经济等相关的领域,更在IT业蓬勃发展的大背景下,已经有了非常广泛的拓展,几乎到了无所不在(Ubiquitous)的程度,在生物信息学、医学信息、图书信息管理、市场、金融等方面都离不开信息安全;信息安全更作为一种个体的人身保护的有效手段,进入了普通人的日常生活,它的应用是如此的广泛而深入,它当之无愧地成为了研究的热点。

信息安全,是一个相对宽泛的统称概念,它既可以看成是一个学科,也可以看成是一个方向,更可以看成是一种理论与技术。但它的实质可以归纳为通过一定的信息处理,达到信息不被窃听、并分辨出伪造信息等目的,信息在具体的传输等过程中,实现安全性、有效性、完整性、可用性和不可抵赖性等的统一。信息的安全处理既包含技术层面的,也包含非技术层面的。在非技术层面上,诸如法令、法规及共同遵守的准则等都可以起到一定的作用;而在技术层面上,则主要通过加密算法和认证技术来有效实现信息安全。此外,从某种意义上来看,也可把协议等看成是以技术层面为基础的结合非技术层面等因素的一种综合性的安全举措。

加密和认证技术是实施信息安全的主要手段,对于加密来说,它可用来防窃听;自从出现了数字认证技术后,用认证技术可以有效地防伪造。加密算法是密码学的核心,它的发展历史非常悠久,可以说自从有了人类族群,相应的密码等运用到了人类的交流之中,在古代凯撒时期,就有一种用替换的方式实现的密码出现。据历史记载,凯撒有效地使用了这种密码技术,使得他的军事活动大获全胜。随后,随着历史的进展,以保密为目的的具体新技术也不断出现,到了现代,形成了以对称密钥为主的单钥制密码体制,经典的单钥制密码体制的主要代表是流密码和块密码,流密码通过明文(Plaintext)与密钥(Key)的逐位异或运算,获得相对安全的密文(Ciphertext);同时,在同步的要求下,密文与相同的密钥再次进行异或运算,得到相应的明文,实现一个完整的加密与解密过程;块密码的实质就是用一个个类似于向量的明文块与密钥块进行线性变换等方式的处理,从而获得相应的密文,仙农(Shannon)曾经总结过相关的处理方式,认为替代(Substitution)、扩散(Extensive)和混淆(Complex)是最主要的手段;在20世纪70年代,以美国发布数据加密标准(Data Encryption Standard,DES)为代表的块密码,它以具体的加密标准出现,极大地促进了块密码技术的发展,虽然DES作为标准已经被废弃不用,但它的好的构思及相关的理念被很好地传承,由此催生了诸如AES和多重DES等的新标准。同样,在20世纪70年代,Whitfield Diffie和Martin Hellman等人提出了非对称加密的新概念,认为加密密钥与解密密钥可以分开,这使得加密过程与解密过程更加互相独立;根据这个理论,以RSA为代表的双钥制密码体制也随之出现,由此开启了双钥制密码体制的时代,现今,RSA公钥体

制，基于离散对数难解问题的公钥体制，以及在椭圆曲线上的密码公钥体制（ECC）等相继出现，它们在加密等方面表现出来的优越性能越来越被人们所认识。

同样的，数字认证（Digital Certification）技术也得到了长足的发展，数字认证作为传统的认证技术的延伸和拓展，有效地实现了防伪造的功能。现今，已经出现的认证技术已经很多，有基于 RSA 的认证技术，基于大数分解难解问题的 Fiat - Schamir 签名体制、以离散对数难解问题为基础的 ElGamal 签名体制、Okamoto 签名体制、Neberg - Rueppel 签名体制等，除此外，还有基于 ECC 的签名体制以及 Diffie - Hellman 密钥协商体制等。这些认证技术既具有严谨的理论依据，同时也展现了灵活多姿的应用前景，尤其在计算机网络技术迅猛发展的当今，先进的认证技术用到相关以通信为媒介的各个领域，实现信息在每一个环节中的安全，构成了很具活力的发展态势。

1.2 加密与认证技术的基础数学

加密算法与认证技术的发展离不开相关数学的支撑，在很多时候，一种加密算法或认证方法是否可行，要归结于它的数学基础是否牢固或先进，从最深层的层面上来看，它们的实质就是相关数学本身。

但是加密算法与认证技术的数学基础并不完全等同于一般的学科的数学基础，它涉及到诸如逻辑函数、线性代数、门限函数、数论中的素数等理论，抽象代数中的群、环、域、有限域、有限域上的曲线等基本的数学理论，以及有关计算复杂度、NP 问题等。并随着相关技术的进一步发展，相应地，所需用到的数学基础知识也会越来越多的同时，也会越来越深入。

分析针对加密算法与认证技术的相关数学内容，不难发现，与公钥密码体制及数字认证技术相关的数学内容占了绝大部分，而这些数学涉及到比较抽象的数论、近世代数（Abstract Algebra）中构造性代数结构等的相关理论。迄今为止，公钥密码体制与数字认证技术都是依据某些单向函数（One - way Function）的逆向求解为难解问题的相关理论所设计的，这些难解问题具体包括大整数因数分解的难解问题、离散对数难解问题以及椭圆曲线和超椭圆曲线上的离散对数难解问题等。大整数因数分解的难解问题具体涉及到相关的数论，它的基本描述是在已知两个大素数，求它们的乘积运算相对简单，但反过来，对一个大整数进行因数分解就很难，RSA 公钥体制就是基于这个难解问题设计的；同样地，在一个具有有限循环群结构的代数中，由它的生成元及所给定的整数，可以很容易地得到有限循环群中的相关元素，但反过来，在有限循环群中，由所给定的元素及生成元来求出相关的整数就非常困难；同样的道理，只要把在椭圆曲线上的点所构成的交换群代替有限循环群，就可以得到椭圆曲线上的离散对数难解问题。随着研究的深入，在超椭圆等曲线上的代数结构中来分析离散对数难解问题的相关结论也已经出现，成为了密码及认证技术发展的新方向之一，也引起许多人的注意。

所以，不难发现，这些支撑加密算法和认证技术的数学理论自然成了不折不扣的基础知识，每一位想要了解加密算法与认证技术的人，都必须了解这些所要用到的数学基础。它们不仅仅是必要条件，更是对想在这个领域中有所创新的人来说，熟练掌握这些知识，有利于更好地开展他们的创新性工作。鉴于此，把在加密算法和认证技术中用到的数学

知识进行归纳并辑录成一个整体，是非常有必要的。

本书把加密算法与认证技术中所要用到的数学知识进行了系统地归纳，使之成为一个相对完备的知识体系，全书共分成8章，除第1章绪言外，其他的章节都较详细地介绍了具体的数学内容。

第2章主要介绍逻辑代数理论中的有关异或运算等相关知识，除此外，还介绍了随机数和单向函数等概念，以及有流密码的基本概念。第3章主要介绍线性代数中的向量与矩阵等的基本内容，以及块密码的基本概念，及提升安全性所采用的替代、扩散及混淆等概念，替代、等运算都要用到矩阵和向量的初等变换等理论。第4章介绍了数论中的整数整除运算等基础内容，重点介绍了欧几里得除法及有关最大公约数、最小公倍数的概念和性质；第5章着重介绍同余式的求解问题，分别介绍了一次同余式、二次同余式、及高次同余式的解的存在性、解的个数及相关同余式的具体求解法等，内容还包括中国剩余定理、欧拉判别法、高斯引理及二次互反定律、指数、原根和指标等概念；第6章着重讨论了素数论中的素性检验问题，对主要的几种素性检验方法进行了深入探讨；第7章介绍抽象代数的相关内容，分别介绍了群、环、域和模的相关知识；第8章则介绍了椭圆曲线及在椭圆曲线上的离散对数难解问题的密钥体制，尤其指出，在某些曲线上来构建代数结构，对解决一些重大数学难题是一种可行的方法，Wiles 对 Fermat 大定理的完美解决可谓是一个成功的范例。这样，把现今最主要的加密算法和认证技术所需要的数学知识进行了完备的辑录。

思 考 题

1. 加密算法与认证技术各有何种特别的目的。
2. 加密与认证技术的数学基础有何特点。
3. 加密与认证的技术创新需要哪些条件。

第 2 章　布尔代数基础

在密码学中，流密码等密码体制是以逐位加密运算为基本着力点的，它的理论基础就是布尔代数，布尔代数是用具体的符号来进行逻辑推演的一套工具，在遵循一定的规律的条件下，它是对相关事件进行合乎逻辑的推演运算的数学表述，因此，它的实质就是数理逻辑代数。布尔代数有很广泛的应用。

这里就与流密码体制有关的布尔代数中的异或运算以及随机数等内容进行介绍。

2.1　布尔代数中的逻辑变量(值)

布尔代数又被称为逻辑代数，它是关于逻辑推理的具体数学表述，因此需要有用来表示的逻辑变量。这些变量，用来表征具体可能的逻辑状态，逻辑状态不同，所取的逻辑变量也不同，一般的有三值逻辑、四值逻辑等多值逻辑，但最常用的还是二值逻辑。

所谓二值逻辑，就是布尔代数中的逻辑值仅取两种数值，它实际上代表两种不同的甚至相反的逻辑表示，通常记为 0 和 1。这两个值几乎可囊括所有相反的事物的逻辑状态表示，如数量的大与小，变量的增与减，开关的开与关，事物的肯定与否定，以及二电平的电信号的数字表述等。

更需要指出的是，因为 0 和 1 可看成整数被 2 除后的可能余数，由此二值逻辑与模 2 运算之间存在内在的联系。此外，由于通信信号在二进制条件下也表示为 0 与 1 的信息比特流，它们之间的逐位运算可看成布尔代数的相关运算，由此可揭示它们之间的内在关系。

2.2　二值条件下的布尔代数的基本运算

虽然关于布尔代数的基本运算的界定不尽相同，在有些场合以“并”“交”和“补”等运算作为基本布尔运算；但有很多时候，基本的布尔运算主要指的是“与”“或”与“非”等逻辑运算。

所谓逻辑“与”运算，可用“缺一不可，全是才是”来概括，该运算的定义：若所给各变量中任一个是 0，结果就是 0；当且仅当各变量都是 1 时，结果才是 1，它用“ × ”作为运算符号，可称为逻辑乘，运算结果可称“积”，具体有可表示为

$$1 \times 0 = 0$$
$$1 \times 1 = 1$$
$$0 \times 1 = 0$$
$$0 \times 0 = 0$$

逻辑“与”的运算规则如表 2.1 所列。

逻辑“或”运算，可以用“有一即为有，全无才是无”来概括，该运算的定义：若所给的变量中存在1，那么结果就是1，只有当所给变量全为0时，结果才为0；它可以用“+”这种运算符号表示，称为逻辑加，结果可称为“和”，具体可表示为

$$1+0=1$$
$$1+1=1$$
$$0+1=1$$
$$0+0=0$$

逻辑“或”的运算规则如表2.2所列。

表2.1 “与”的运算规则表

给定变量 A	给定变量 B	结果 E
0	0	0
0	1	0
1	0	0
1	1	1

表2.2 “或”的运算规则表

给定变量 A	给定变量 B	结果 E
0	0	0
0	0	1
1	0	1
1	1	1

还有一个基本运算称为逻辑“非”，也就是反演，该运算的定义：结果值是所给变量的否定，被记为

$$\bar{1}=0$$
$$\bar{0}=1$$

逻辑“非”的运算规则如表2.3所列。

表2.3 “非”的运算规则表

给定变量 A	结果 B
1	0
0	1

在这三种运算是其他相关布尔运算的基础，也就是说，其他的运算可由这三者具体表示，相关的规律也可由这些基本的运算推导而获得证明。

2.3 二值布尔代数中的异或运算

在密码学中，需要用到称为“异或”的布尔代数运算，用“⊕”的符号表示两个变量之间的运算，它记为 $a \oplus b, a \in \{0,1\}, b \in \{0,1\}$，它的具体运算规则可由基本的布尔运算定义为

$$a \oplus b = a \times \bar{b} + \bar{a} \times b, a \in \{0,1\}, b \in \{0,1\}$$

根据该定义，可以得到

$$1 \oplus 0 = 1 \times 1 + 0 \times 0 = 1 + 0 = 1$$
$$1 \oplus 1 = 1 \times 0 + 0 \times 1 = 0 + 0 = 0$$
$$0 \oplus 1 = 0 \times 0 + 1 \times 1 = 0 + 1 = 1$$
$$0 \oplus 0 = 0 \times 1 + 1 \times 0 = 0 + 0 = 0$$

这些就构成二值布尔代数中的异或运算的规则，一般地，把异或运算记为XOR运算，它的运算规律与整数做模2加运算所得的结果是一致的。但需要明确的是，异或运算中

的变量含义完全不同于求模运算的含义。

异或运算的具体规则如表 2.4 所列。

表 2.4　异或(XOR)的运算规则表

输入变量 A	输入变量 I	输出结果 E
0	0	0
0	1	1
1	0	1
1	1	0

若设变量为 $a \in \{0,1\}$，$b \in \{0,1\}$，$c \in \{0,1\}$，该运算有以下一些基本性质：

(1) 交换律：$a \oplus b = b \oplus a$。

(2) 结合律：$a \oplus (b \oplus c) = (a \oplus b) \oplus c$。

(3) 分配律：$a \times (b \oplus c) = (a \times b) \oplus (a \times c)$。

(4) $a \oplus 1 = \bar{a}$。

(5) $a \oplus 0 = a$。

(6) $a \oplus a = 0$。

(7) $a \oplus \bar{a} = 1$。

(8) $\bar{a} \oplus \bar{b} = a \oplus b$。

这些性质都可根据布尔代数的基本运算及相关定义，容易获得证明。

在密码学中，把这种异或运算看成一种信号信息流的逐位处理，这样它实际上就构成一个信息处理器，具有如图 2.1 所示的结构。

由此可得到异或处理的规则表，如表 2.5 所列。

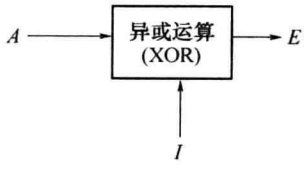

图 2.1　异或运算的实现

表 2.5　异或(XOR)处理的运算真值规则表

A	输入 I	输出 E
0	0	0
0	1	1
1	0	1
1	1	0

2.4　单向函数

运用布尔代数中的基本运算，可以构建逻辑的单向阈门，它的实质就是一种单向函数(One - way Function)，简单地说，设 $y = f(x)$，$x \in D$，其中 D 为定义域，它是一个单向函数，那么在已知 $x_0 \in D$ 的条件下，由 $f(x_0)$ 求得函数值 y_0 是容易实现的；但反过来，由 y_0 通过 $y_0 = f(x_0)$ 而求得具体的 x_0 就很难。除了这种较简单的形式外，还有迭代型的单向函数，它的定义如下：

$$\begin{cases} H_0 = IV \\ H_i = f(H_{i-1}, Y_{i-1}), i = 1,2,\cdots,k \\ H(x) = H_k \end{cases}$$

在这里，IV 是初始值，可以随机选取。把输入 x 分成 k 组的分组，分别记为 $Y_0, Y_1, \cdots, Y_{k-1}$，函数 f 满足一定的压缩等条件，它有两项输入，一项是上一轮迭代的输出；另一项是分组后对应的一部分，如此一轮轮做下去，到最后一轮，实际上把原来 x 的所有部分都进行了运算，它的输出就构成单向函数的值，即为 $H(x) = H_k = f(H_{k-1}, Y_{k-1})$。

总结单向函数的特性，大致可归纳如下：

（1）函数可公开的。

（2）函数的输入可以任意长，但输出是固定长度的。

（3）给出函数 $H(\cdot)$ 和 x，很容易计算 $H(x)$。

（4）给定 y，根据 $y = H(x)$，计算 x 很难，甚至是不可行的。

（5）给出 x，寻找 $x_1(x_1 \neq x)$，使得 $H(x_1) = H(x)$ 在计算上是不可行的，即它具有很强的单一性，进一步，对于任意的两个不同的输入 x_i 和 x_j，$H(x_i) = H(x_j)$ 在计算上是不可行的，这就建立了输入与单向函数值之间的一一对应，可以成为输入的一个表征元素，这种具体的特性也被看成是一种指纹（Fingerprint），用它可对相关数据进行认证，进而可鉴别其具体的“身份”。

单向函数除了以上这些特性外，它还具有很强的构造性，也就是可以通过具体的设计构造获得，易于实现，因此在加密与认证等领域有很广泛的应用。

2.5 流密码简介

在称为流密码（Stream Cryptography）的逐位加密的对称密钥体制中，需要用到具体的异或运算，记明文源集合为 $M = \{a_1 a_2 \cdots a_n \cdots\}$，密文源集合为 $C = \{c_1 c_2 \cdots c_n \cdots\}$，而相应的密钥集合为 $T_1 = \{b_1 b_2 \cdots b_n \cdots\}$ 的条件下，在发送端实现加密（Encryption）的过程可描述为

$$c_i = a_i \oplus b_i, i = 1,2,\cdots,n,\cdots,$$

同样地，记明文宿集合为 $M' = \{y_1 y_2 \cdots y_n \cdots\}$，密钥集合 $T_2 = \{b'_1 b'_2 \cdots b'_n \cdots\}$，在接收端实现解密（decryption）的过程可用如下的式子描述：

$$y_i = c_i \oplus b'_i, i = 1,2,\cdots,n,\cdots$$

当满足 $b_i = b'_i, i = 1,2,\cdots,n,\cdots$ 这个条件时，则最后解密的过程可进一步描述为

$$y_i = c_i \oplus b'_i = a_i \oplus b_i \oplus b'_i = a_i \oplus 0 = a_i, i = 1,2,\cdots,n,\cdots$$

这样就达到了完全解密的目的。

用流密码加密和解密的过程如图 2.2 所示。

流密码中涉及到具体的密钥流，密钥流的生成也需要用到逐位异或运算，在通常的时候，密钥流由移位寄存器产生，移位寄存器是由若干个互相时延的存储器的串联而成，它的结构如图 2.3 所示。

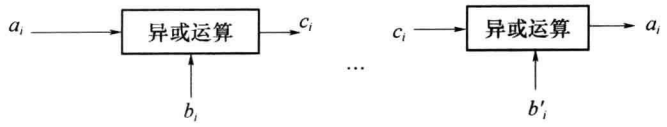

图 2.2　流密码的加密、解密图

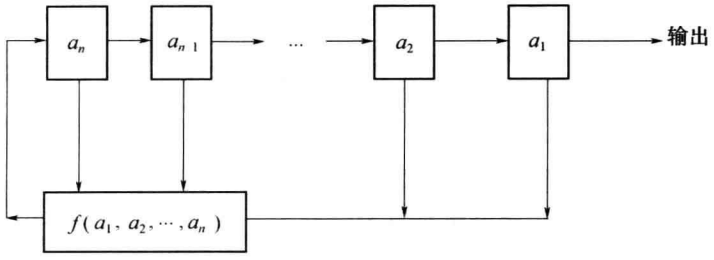

图 2.3　n 级反馈移位寄存器结构图

n 级移位寄存器的工作进程可归纳如下：设在某时刻，这 n 个存储器中的元素的状态为$(a_1, a_2, \cdots a_i, \cdots, a_n)$构成一个 n 维的向量，称为状态向量，在这里确定为初始状态向量，由此根据$f(a_1, a_2, \cdots, a_n)$这一关系式，可得到一个新的值，然后把所获得的新值反馈给第 n 个存储器 a_n，并把第 n 个存储器中原来的值移到前一个存储器 a_{n-1} 位置中，如此逐一前移，以此类推，把存储器中的原来的值移存到前一个存储器中，直到 a_2 位置上的值移到最后一个寄存器 a_1 位置，而原 a_1 位置上的值则直接输出，这样重复进行，则可由 a_1 位置源源不断地输出相应的值，形成一个序列流，这一输出序列流就构成相应的密钥流。在这个过程中$f(a_1, a_2, \cdots, a_n)$函数称为反馈函数，它决定了所生成的反馈值的具体形式，当反馈函数$f(a_1, a_2, \cdots, a_n)$是关于 $a_1, a_2, \cdots, a_i, \cdots, a_n$ 的线性函数时，则移位寄存器被称为 LFSR(Linear Feedback Shift Register)，此时反馈函数可写成：

$$f(a_1, a_2, \cdots, a_n) = c_n a_1 \oplus c_{n-1} a_2 \oplus \cdots \oplus c_1 a_n \triangleq \sum_{i=1}^{n} \oplus c_i a_{n-i}$$

式中：$c_i \in \{0,1\}$，符号⊕为异或运算，符号 $\sum \oplus$ 表示多个异或运算。

线性移位寄存器的结构和工作原理图如图 2.4 所示。

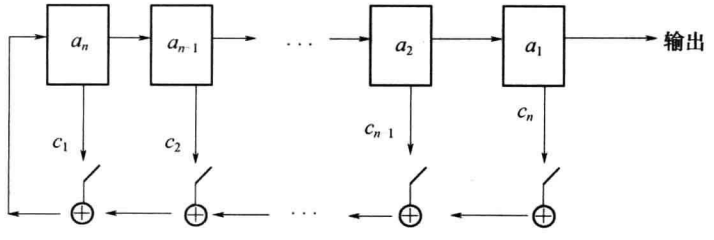

图 2.4　n 级线性移位寄存器结构图

例如，设四级线性移位寄存器，它的反馈函数为

$$f(a_1, a_2, a_3, a_4) = a_1 \oplus a_3 \oplus a_4$$

而初始值为

$$(a_1,a_2,a_3,a_4) = (0,1,0,1)$$

则相应的移位寄存器可得到相应的状态向量分别为

$$(a_1,a_2,a_3,a_4) = (0,1,0,1)$$
$$(a_1,a_2,a_3,a_4) = (1,0,1,1)$$
$$(a_1,a_2,a_3,a_4) = (0,1,1,1)$$
$$(a_1,a_2,a_3,a_4) = (1,1,1,0)$$
$$(a_1,a_2,a_3,a_4) = (1,1,0,0)$$
$$(a_1,a_2,a_3,a_4) = (1,0,0,1)$$
$$(a_1,a_2,a_3,a_4) = (0,0,1,0)$$
$$(a_1,a_2,a_3,a_4) = (0,1,0,1)$$

对应的输出序列流为…|0111010|0111010。它可以构成密钥流，然后与明文(Plaintext)流一道，逐位做异或运算，就可以得到密文(Ciphertext)；同样地，用移位寄存器生成的相同(位数相同，且同步)的密钥流与密文进行逐位异或运算，实施解密过程，最终得到相应的明文。

2.6 随机数及伪随机数

随机数可理解为随机(Random)产生的数字或序列，它具有两个显著的特性，分别是随机性与不可预测性，而随机性可由如下两个具体的准则来描述。

(1) 均匀分布，就是序列中每一个数出现的频率至少是近似相等的，此时每一个数所对应的先验概率几乎相等，由最大熵原理可知，此时达到最大熵，也就是出现某一个数是最不确定的。

(2) 独立性，独立性体现在后一个出现的数 a_i 与前面已经出现的数 $a_{i-1},\cdots,a_1$ 之间满足 $P(a_i|a_{i-1},\cdots,a_1) = P(a_i)$，由此，对应的互信息 $I(a_i;a_{i-1},\cdots,a_1) = 0$。

而不可预测性，实际上也反映了后面生成的数不受前面已经生成的数的影响特质，它从随机数生成的角度来反映其特性。

随机数在很多加密与认证技术中需要用到，但是具体生成又非常困难，在现实世界中，仅仅如物理噪声(Noise)发生器、气体放电管、宇宙射线等可产生真正的随机数，但这些都难以为网络等所用，由此，需要用一种伪随机数来替代正真的随机数。伪随机序列的本质是一种依据相关规律而生成的序列，但它遵循 Golomb 的三个随机性公设：

(1) 在序列中，一个周期长的符号，0 与 1 的个数差至多为 1。

(2) 在一个周期内的符号，长度为 m 的游程的个数占总游程个数的 $\frac{1}{2^m}(m=1,2,\cdots)$，且等长的游程中，0 与 1 各自的游程数相同。

(3) 异相自相关函数是常数。

在 Golomb 公设中，提到了“流程”这个概念，所谓“流程”，是指在序列中连着的相同符号串，若相同符号串的符号个数为 m，则称该符号的游程为 m，它反映了序列中符号之