无线网络安全
——技术与策略

金　纯　郑　武　陈林星　编著
刘益良　审校

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

全书分 10 章：第 1、2 章为常用加密和签名算法基础；第 3 章介绍短距离低功耗无线通讯技术标准，即蓝牙技术的安全性；第 4 章介绍无线网络以广播方式在物理层传送报文带来的安全威胁和 IEEE 802.11 认证服务；第 5 章介绍广泛使用的移动通信系统的安全机制；第 6 章具体介绍红外光通信系统的安全结构、安全策略和发展趋势；第 7 章介绍卫星通信网络的组成、安全策略和发展趋势；第 8 章介绍病毒和攻击等安全威胁及其防护措施及安全策略；第 9 章从无线网络干扰的角度介绍各种抗自然和人为干扰的技术和发展趋势；第 10 章介绍目前尚未最后形成业界公认的统一标准的第三代无线通信系统（3G 系统）的组成结构，安全网络和安全机制。

本书可供从事无线网络安全设计、系统维护和应用开发的技术人员阅读，也可作为相关专业师生的教学参考书。

图书在版编目(CIP)数据

无线网络安全：技术与策略/金纯等编著. —北京：电子工业出版社，2004.6
ISBN 7-120-00058-6

Ⅰ. 无… Ⅱ. 金… Ⅲ. 无线电通信—通信网—安全技术 Ⅳ.TN92

中国版本图书馆 CIP 数据核字（2004）第 046970 号

责任编辑：竺南直
印　　刷：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：13.75　字数：348 千字
印　　次：2004 年 6 月第 1 次印刷
印　　数：5 000 册　　定价：20.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

序

近年来，随着笔记本电脑和个人数字代理（PDA）以及家电数字化等技术的发展，人们利用信息技术进行通信联系和信息交流的空间和灵活性不断拓展。“无线网络”成为技术发展和社会应用的新宠，受到全社会的普遍欢迎，同时也成为网络发展商们争相抢占的新领域。“无线网络”的确能逐步使网络从有形的设备网线发展成无形的“连接无限”。但无线接入在给我们带来众多便利的同时，也将信息安全问题客观地摆在我们面前。众所周知，利用无线电源传递信息时，信道上的安全威胁，包括截取、窃听、干扰和篡改等，均相当现实，于是为无线网络寻求安全保护成了信息安全领域的又一大急务。在短短的几年内，学术界和产业界已分别提出了包括软件方案、硬件设备、专业服务等在内的系统解决办法，内容涉及协议、算法、标准和管理等，可谓洋洋大观。西方国家先后推出了相应的专著和专题会议，我国也制定了 WAPI 标准并引起了不小的国际争议，全面了解无线网络的安全问题对广大科技人员和社会民众而言就显得尤为重要。故而当我看到刘益良教授等人编写和审校的《无线网络安全——技术与策略》一书的清样时，有一种“及时雨”的欣喜之感。奉读之后，感到该书有三个特点：一是基础性，该书对无线网络安全问题的介绍不是简单地从具体的安全事件入手，而是从密码学这一科学基础出发，对深奥的密码学和安全应用的知识介绍则择其精要，深入浅出；二是系统性，该书并未将无线网络仅仅局限在近年炙手可热的蓝牙、802.××等内容上，而是兼顾传统技术，将移动通信、红外、卫星通信和军用通信等也纳入视野；三是技术性，该书作者多是长期从事通信和信息安全研究的工程技术人员，全书结构的组织和内容的表述，保留了较明显的工程意味，掩卷之余，给人以同技术人员切磋交流的感觉。

当然，无线网络技术正处在高速发展与演进之中，对其安全问题的分析与把握也有一个与时俱进的问题。况且，当今信息技术的发展和具体应用的普及除科技的含量之外，还有很强的商业选择因素，故而对无线网络安全问题的研讨远非一本著述、一段时间可以定论。但我相信本书的出版，对无线网络的应用和信息安全技术的发展均有裨益。也正因如此，我乐于将读后的感受草就成篇。是为序。

吴世忠
于中国信息安全产品测评认证中心
2004 年 5 月 20 日

前　言

局域网互联的传输介质通常使用有线介质，在某些特定的场合存在无法有效传输信息的问题。例如，普通拨号线的低传输速率不能满足带宽需求，建设费用高和周期长制约 ISDN 和 ADSL 专线、同轴电缆、光纤在特定场合使用。有线网络存在的移动困难、后期维护成本高、系统覆盖面积小和结构扩展易影响系统安全性等问题，随着无线网络的应用而得到解决。

目前，无线网络的技术性能特别是安全性逐步完善，应用成本大幅降低，已经完全可以和有线网络相媲美，某些方面甚至超过有线网络。无线网络具有的特有优点，如一般无线网络安装相对方便，不受地区限制，可以连接有线介质无法连接或者建设比较困难的场合，特别适合港口、码头、古建筑群、市中心两幢高楼之间低成本的组网。技术的完善使无线网络安全解决方案更加成熟，目前各种无线网络已经广泛应用于各种军事、民用领域。

信息系统的安全问题是人们广泛关心的问题，无线网络的安全问题则往往被人们认为是难以解决的问题。这主要源于无线网络特殊的内置安全特性不为人所知，产生了严重的误解。如上面介绍的，在某些特定场合无线网比有线网具有更好的安全性。

无线网络安全主要包括系统安全、网络安全和应用安全等内容，也遵循安全风险分析、安全结构设计和安全策略确定的基本实施规律。无线网络的开放性特点增加了确定无线网络安全机制的难度，形成了与有线网络系统完全不同的实现安全目标的方式。系统认识和解决无线网络系统的安全问题应该成为研究者、开发者和使用者长期不懈的任务。为了帮助无线网络维护、应用开发的专业技术人员或者希望了解无线网络安全的读者站在系统的角度学习无线网络安全基础知识，了解各种无线通信系统的安全特点，本书全面地介绍了目前常用的无线通信系统、无线网络安全牵涉的常用加密和签名算法、系统安全结构、安全机制和实现安全策略的各种途径和方案。

全书共分 10 章。第 1, 2 章为常用加密和签名算法基础，主要介绍加密算法中常用的数论和离散数学知识，对数字认证过程中牵涉的标准和协议也做了简要介绍。第 3 章介绍了短距离、低功耗无线通信技术标准，即蓝牙技术的安全性；第 4 章介绍无线网络以广播方式在物理层传送报文带来的安全威胁和 IEEE 802.11 认证服务。第 5, 6, 7 章从系统的角度介绍了目前广泛使用的无线通信网络，如 GSM, CDMA, GPRS（CDMAIX）, WCDMA, CDMA2000 和 TD-SCDMA 系统，以及红外无线光通信系统和卫星通信系统的组成、安全策略和发展趋势。对逐渐广泛应用于军事战术和其他安全敏感领域应用的移动多跳无线分组(Ad Hoc)网络也做了详细介绍。第 8 章主要介绍病毒和攻击等安全威胁及其防护措施和安全策略。第 9 章则从无线网络干扰的角度介绍各种抗自然和人为干扰的技术和发展趋势。第 10 章作为附录专门介绍目前尚未最后形成业界公认的统一标准的第三代无线通信系统（3G 系统），目的是为了帮助读者对其组成结构、安全风险和安全机制有系统的了解。

本书能够帮助大专院校学生了解无线网络安全的知识，也可以作为相关专业研究生和从事无线网络安全结构设计、系统维护和应用开发的技术人员参考资料。

参加本书编著的人员长期从事信息系统安全研究和应用开发，其中第 1, 3, 4 章由金纯

执笔完成，第 6, 7, 9 章由郑武完成，第 10 章由陈林星完成，第 2, 5, 8 章内容由参编人员共同完成，整书内容和结构的编排、修改和审定由刘益良完成。李楠参加了本书的校对工作，在此表示感谢。

由于信息安全的内容和技术日新月异，本书难免存在表述不准确甚至错误的地方，欢迎读者给予指正。

编著者

2004 年 5 月 20 日于重庆

目　录

第 1 章　加密算法基础及经典加密算法

本章简单介绍了在加密算法中常用的一些数论、离散数学知识及常用经典加密算法，熟悉这些内容的读者可跳过本章。

1.1　加密算法中常用的数论知识

1.1.1　素数和互为素数

1．整除与因子

设 **Z** 是整数集合，a，$b\in\mathbf{Z}$，$b>0$，则存在惟一的整数对 q，r 使得

$$a=qb+r，0\leq r<b$$

当 $r=0$ 时，我们定义 b 整除 a，记为 $b|a$。当 $b|a$ 时，b 是 a 的一个因子。

2．素数

素数 p 是大于 1 且因子仅为 ±1 和 $\pm p$ 的整数。素数在数论和本章将要讨论的技术中起着至关重要的作用。

任何大于 1 的整数 a 都能被因式分解为如下的惟一形式：

$$a = P_1^{a_1} P_2^{a_2} \cdots P_t^{a_t}$$

其中 $P_1>P_2>\cdots>P_t$ 都是素数，且 $a_i>0$ (i=1, 2, …, t)。

3．互为素数

符号 gcd(a, b)用来表示 a 和 b 的最大公因子。正整数 c 是 a 和 b 的最大公因子，如果满足以下条件：

（1）c 是 a 和 b 的因子；

（2）任何 a 和 b 的因子也是 c 的因子。

因为通常要求最大公因子为正，而 gcd(a,b)=gcd(a,-b)=gcd(-a,b)=gcd(-a,-b)。一般 gcd(a,b) = gcd (|a|,|b|)。此外，由于 0 均能被所有非零整数整除，因此有 gcd(a,0)=|a|。

如果 gcd(a,b) = 1，则认为 a 和 b 互素。

1.1.2　模运算

1．定义

给定任一正整数 n 和任一整数 a，如果用 a 除以 n，得到商 q 和余数 r 将满足如下关系：

$$a=qn + r　0\leq r<n; q=\lfloor a/n \rfloor$$

其中$\lfloor x \rfloor$表示小于或等于 x 的最大整数。

如果 a 是一个整数，而 n 是一个正整数，定义 $a \bmod n$ 为 a 除以 n 的余数。因此，对任一整数 a，可表示为：

$$a=\lfloor a/n \rfloor \times n+(a \bmod n)$$

2．模运算的操作

模运算有如下性质：

（1）$[(a \bmod n) + (b \bmod n)] \bmod n=(a+b) \bmod n$

（2）$[(a \bmod n) - (b \bmod n)] \bmod n=(a-b) \bmod n$

（3）$[(a \bmod n) \times (b \bmod n)] \bmod n=(a \times b) \bmod n$

下面证明第一条性质：

定义$(a \bmod n)=r_a$,$(b \bmod n)=r_b$,则可得 $a=r_a+jn$，j 为某一整数;$b=r_b+kn$,k 为某一整数。有：

$$\begin{aligned}(a+b) \bmod n&=(r_a+jn+r_b+kn) \bmod n\\&=(r_a+r_b+(k+j)n) \bmod n\\&=(r_a+r_b) \bmod n\\&=[(a \bmod n)+(b \bmod n)] \bmod n\end{aligned}$$

余下的性质也很容易证明。

3．模运算的性质

定义集合 $\boldsymbol{Z}_n$ 为小于 n 的所有非负整数集合：

$$\boldsymbol{Z}_n=\{0,1,\cdots,(n-1)\}$$

该集合也被当做模 n 的余数集合。如果在该集合上实行模运算，$\boldsymbol{Z}_n$ 中的整数保持如下性质：

（1）交换律：$(x+y) \bmod n=(y+x) \bmod n$

$(x \times y) \bmod n=(y \times x) \bmod n$

（2）结合律：$[(x+y)+z] \bmod n=[x+(y+z)] \bmod n$

$[(x \times y) \times z] \bmod n=[x \times (y \times z)] \bmod n$

（3）分配律：$[x \times (y+z)] \bmod n=[(x \times y)+(x \times z)] \bmod n$

（4）恒等律：$(0+x) \bmod n=x \bmod n$

$(1 \times x) \bmod n=x \bmod n$

（5）加法逆元$(-x)$：对每一个 $x \in \boldsymbol{Z}_n$，存在一个 y，使得$(x+y) \bmod n=0$

1.1.3 同余类

1．定义

若 $m|(a-b)$，即 $a-b=km$，我们就说 a 和 b 模 m 同余，记以

$$a \equiv b \bmod m$$

m 称为这个同余式的模。

2．关于同余类的定理

定理 1　模 m 的同余关系满足以下性质：

（1）自反性，即 $a \equiv a \bmod m$；

（2）对称性，即若 $a \equiv b \bmod m$，**则**

$$b \equiv a \bmod m$$

（3）传递性，即若 $a \equiv b \bmod m$，$b \equiv c \bmod m$，**则**

$$a \equiv c \bmod m$$

定理 2　若 $a \equiv b \bmod m,\ c \equiv d \bmod m$，**则**

（1） $a \pm c \equiv (b \pm d) \bmod m$

（2） $ac \equiv bd \bmod m$

证明：因 $a \equiv b \bmod m,\ c \equiv d \bmod m$，**所以**

$$a = km + b,\ c = hm + d$$

$$a \pm c = (k \pm h)m + (b \pm d)$$

从而

$$a \pm c \equiv (b \pm d) \bmod m$$

同理可证： $ac \equiv bd \bmod m$

定理 3　若 $ac \equiv bc \bmod m$，**且** c **和** m **互素，则**

$$a \equiv b \bmod m$$

证明：由 $ac \equiv bc \bmod m$，**可知**

$$ac = km + bc$$

即

$$c(a - b) = km$$

由于 c **和** m **互素，因此** $c \mid k$。**设** $k = hc$，**则**

$$c(a - b) = hcm$$

$$a \equiv b \bmod m$$

定理 4　若 $ac \equiv bc \bmod m$，$d = (c, m)$，**则**

$$a \equiv b \bmod m/d$$

1.1.4　欧拉定理

1．欧拉函数

所有模 m **和** r **同余的整数组成一个剩余类**$[r]$。**显然这个剩余类中的任何一个数都可以确定这个剩余类。每个整数总是和** m **个数**

$$0, 1, 2, \cdots, |m| - 1$$

中的一个数同余，而且仅和其中的一个数同余。$0, 1, 2, \cdots, |m| - 1$ **中任意两个数模** m **不同余。**

一组整数 r_1，r_2，…，r_m 分别属于不同的同余类时，则称它构成一个模 m 的完全剩余类。

剩余类[r]中的每一个数可表示为

$$r+km \qquad k=0, \pm1, \pm2,\cdots$$

所以剩余类[r]中的每一个数和 m 互素的充要条件是 r 和 m 互素。和 m 互素的同余类的数目用ϕ(m)表示，我们称$\phi(m)$为 m 的欧拉函数。

2．与欧拉函数有关的几个定理

定理 1 若 m_1 和 m_2 互素，则

$$\phi(m_1 m_2)=\phi(m_1)\phi(m_2)$$

证明：设 x 是一个正整数，满足

$$0\leq x\leq |m_1 m_2|$$

设 $$x\equiv r_1 \bmod m_1,\ x\equiv r_2 \bmod m_2$$

其中 $$0\leq r_1\leq m_1,\ 0\leq r_2\leq m_2$$

则 r_1、r_2 为 x 所惟一确定。

反之，给定 r_1、r_2 可惟一确定 x，即 x 和一对数偶（r_1, r_2）一一对应。x 和 m_1m_2 互素，当且仅当 x 和 m_1、m_2 都互素，同时 x 和 m_i 互素的充要条件是 r_i 和 m_i 互素，i=1,2。

这就证明了与 m_1m_2 互素的数 x 的数目等于数偶（r_1，r_2）的数目，其中 r_1 和 m_1 互素，r_2 和 m_2 互素。比 m_1 小而与 m_1 互素的 r_1 数目为$\phi(m_1)$，小于 m_2 而与 m_2 互素的 r_2 数目为$\phi(m_2)$，这样的数偶的数目为$\phi(m_1)\ \phi(m_2)$。

定理 2 若 $m=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$，则

$$\phi(m)=m(1-\frac{1}{p_1})(1-\frac{2}{p_2})\cdots(1-\frac{1}{p_k})$$

3．欧拉定理

若 a 和 m 互素，则

$$a^{\phi(m)}\equiv 1 \bmod m$$

证明：设$\phi(m)=k$，并令 r_1，r_2，…，r_k 是与 m 互素的模 m 剩余类。显然，由于 a 和 m 互素，ar_1，ar_2，…，ar_k 也和 m 互素，且两两不相同余，否则若

$$ar_i\equiv ar_j \bmod m$$

则 $r_i\equiv r_j \bmod m$（根据同余类的定理 3）

与假设矛盾。所以

$$a^k r_1 r_2\cdots r_k\equiv r_1 r_2\cdots r_k \bmod m$$

由于 r_1, r_2, …, r_k 与 m 互素，故得

$$a^k \equiv 1 \bmod m$$

4．费马定理

若 p 是素数，则

$$a^p \equiv a \bmod p$$

从 $a^{\phi(m)} \equiv 1 \bmod m$ 可知，若 a 和 m 互素，则相对于模 m, a 的逆元素为 $a^{\phi(m)-1}$。

1.2 群和有限域

1.2.1 群

1．代数系统

一个集合 A 连同若干个定义在该集合上的运算 $f_1, f_2, \cdots, f_k$ 所组成的系统就称为一个代数系统，记做$<A, f_1, f_2, \cdots, f_k>$。

2．群的定义

设$<G, *>$是一个代数系统，$*$是 G 上的一个二元运算，如果满足：

① 运算$*$是封闭的

② 运算$*$是可结合的

③ 存在幺元 e

④ 对于每一个元素 $x \in G$，存在它的逆元 x^{-1}

则称$<G, *>$是一个群。

3．交换群

如果群$<G, *>$是中的运算是可交换的，则称该群为阿贝尔群，或称交换群。

4．循环群

设$<G, *>$为群，若在 G 中存在一个元素 a，使得 G 中的任意元素都由 a 的幂组成，则称该群为循环群，元素 a 称为循环群的生成元。

5．群的性质

（1）群的单位元 e 是惟一的

证明：若 e_1 和 e_2 都是群 G 的单位元，则根据定义有

$$e_1 e_2 = e_1,\ e_1 e_2 = e_2$$

所以 $e_1 = e_2$

（2）$a, b, c \in G$，若 $ab = ac$，则 $b = c$；若 $ab = cb$，则 $a = c$。

现证其一。若 $ab = ac$，用 a^{-1} 互乘等式两端得

$a^{-1}(ab) = a^{-1}(ac)$，根据结合律

$a^{-1}(ab) = (a^{-1}a)b = (a^{-1}a)c$

所以 $b = c$

（3）G 的每一元素的逆元是惟一的。

（4）群<G，*>的元素 a，若

$$(a)^n=(a*a*\cdots*a)=e$$

使上式成立的最小正整数 n 称为元素 a 的阶。

有限群 G 的每一元素的阶是有限的。

证明：设 G 的元素个数为 g，作 $a, a^2,\cdots, a^g, a^{g+1}$，由于 $a^n\in G$, n=1, 2,⋯, g, g+1，而 G 的元素只有 g 个，故存在 $1\leq i<j\leq g+1$ 使得

$$a^i=a^j$$

$$a^{j-i}=e$$

故 a 的阶是有限的。

1.2.2 域

1．域的定义

设<A，+，·>是一个代数系统，如果满足：

（1）<A,+>是阿贝尔群

（2）<$A-\{\theta\}$，·>是阿贝尔群（θ为零元）

（3）运算·对运算+是可分配的

则称<A，+，·>是域。

对于域 F，若元素个数是有限的，则 F 叫做有限域或伽罗瓦(Galois)域，否则叫无限域。

2．域的特征

在域 F 中，最小子域的元素个数称为域 F 的特征。

3．域的阶

q 元的有限域记为 F_q 或 GF(q)，q 称为域 F_q 的阶。当 $q=p$ 是素数时，F_q 称为素域，此时 $F_p=Z_p=\{0, 1,\cdots, p-1\}$。

4．伽罗瓦域 GF(p^n)

多项式

$$p(x)=a_0+a_1x+\cdots+a_kx^k,\ a_i\in F,\ i=0, 1, 2,\cdots, k。$$

如果 F 的元素个数为 p，则不同的多项式 $p(x)$全数为 p^{k+1}，即 $p(x)$和 k+1 位 p 进制数 $a_ka_{k-1}\cdots a_2a_1a_0$ 一一对应。

例如 F=GF(2)={0,1}。二次以下的多项式

0 次： $p_{000}(x)=0$　　$p_{001}(x)=1$

1 次： $p_{010}(x)=x$　　$p_{011}(x)=1+x$

2 次： $p_{100}(x)=x^2$　　$p_{101}(x)=1+x^2$　　$p_{110}(x)=x+x^2$　　$p_{111}(x)=1+x+x^2$

若 p 是素数，系数在 GF(p)中多项式用 GF[p,x]表示。若 $p(x)$和 $q(x)$都是属于 GF[p,x]的

两个多项式，而且 $p(x)$的方次高于 $q(x)$的方次，则存在属于 GF[p,x]的多项式 $s(x)$, $r(x)$，使

$$p(x)=s(x)q(x)+r(x)$$

其中 $r(x)$的方次小于 $q(x)$的方次。多项式 $r(x)$称为 $p(x)$除以 $q(x)$的余项。

如果 $p(x)$不能表示以属于 GF[p, x]的两个非常数的多项式 $s(x)$, $q(x)$之积，则称 $p(x)$在 GF[p,x]上是不可化约的。

若 $p(x)$，$s(x)$，$q(x)$都属于 GF[p, x]的多项式，而且等式

$$p(x)=s(x)q(x)$$

成立，则称 $s(x)$，$q(x)$是多项式 $p(x)$的因子。

各整除相似可证：若 $p(x)$和 $q(x)$互素，即不存在除了 1 以外的公因子，则存在多项式 $a(x)$, $b(x)$使得

$$a(x)p(x)=b(x)q(x)=1$$

设 $m(x)$是系数在 GF(p)上不可约的 n 次多项式，则 GF[p, x]在 mod $m(x)$的意义下分成若干个同余类，这些同余类的全体用 GF[p, $m(x)$]表示。则关于通常意义下的多项式的“ + ”和“ · ”运算在 GF[p, $m(x)$]上构成一元素个个数为 p^n 的域，用 GF(p^n)表示。

定理 1 若 a 是 GF[p, $m(x)$]的非零元素，则

$$a^{p^n-1}=1$$

证明：令 $p^n-1=k$，设属于 GF[p,$m(x)$]的 k 个非零元素为 a_1, a_2,…, a_k。a 为其中任一元素，则

$$aa_1,\ aa_2,\cdots,\ aa_k$$

互不相同。否则设

$$aa_i=aa_j$$

那么

$$a(a_i-a_j)=0,\ a_i=a_j$$

故

$$\prod_{i=1}^{k}(aa_i)=a^k\prod_{i=1}^{k}a_i=\prod_{i=1}^{k}a_i$$

即

$$(a^k-1)\prod_{i=1}^{k}a_i=0$$

所以

$$a^k=1$$

定理 2 若 0, a_1, a_2,…, a_k 是 GF[p, $m(x)$]的全体元素，则在 GF[p, $m(x)$]中有

$$x^{p^n}-x=x(x-a_1)(x-a_2)\cdots(x-a_k)$$

证明：从略。