密码学基础

陈少真 编著

Basic Cryptology

科学出版社
www.sciencep.com

密码学基础

陈少真 编著

科学出版社
北京

内 容 简 介

本书全面讲解密码学的基本知识，在阐述密码理论的同时，还介绍了大量的算法和标准. 特别在序列密码体制、分组密码体制和公开密钥密码体制的章节中，不仅介绍了经典的密码体制和算法，而且阐述了部分算法的安全性分析以及相关领域的最新研究成果. 为使读者更好地掌握密码学知识，本书讲授必要的数学背景，并在附录中提供相关参考资料，以便读者进行相关研究. 本书表达清晰、论证严谨、习题丰富.

本书可作为高等院校应用数学、通信和计算机等专业密码学、通信安全和网络安全等课程的教材或参考书，也可供信息安全系统设计开发人员、密码学和信息安全爱好者参考.

图书在版编目(CIP)数据

密码学基础/陈少真编著. —北京：科学出版社，2008

ISBN 978-7-03-021264-1

Ⅰ.密… Ⅱ.陈… Ⅲ.密码-理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字 (2008) 第 029178 号

责任编辑：王丽平 王日臣 / 责任校对：张小霞

责任印制：赵德静 / 封面设计：杜剑平

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

铭浩彩色印装有限公司印刷

科学出版社发行 各地新华书店经销

*

2008 年 5 月第 一 版 开本：B5(720×1000)

2008 年 5 月第一次印刷 印张：19 1/2

印数：1—4 000 字数：371 000

定价：58.00 元

(如有印装质量问题，我社负责调换〈明辉〉)

前　言

随着计算机网络的广泛应用, 信息的保密和认证、网络的安全与防护越来越受到社会各界的广泛关注. 因此, 解决信息的安全问题成为各国的一大战略课题, 有关密码学的理论和技术的书籍也开始不断涌现, 从事密码学研究的人也越来越多. 为了适应时代的需要, 根据现有的公开书籍和资料, 并结合教学实践, 我们编写了这本基础理论型的密码学著作《密码学基础》.

在编写本书的过程中, 编者力求语言表达清晰、论证严谨、内容新颖、选材精良、习题丰富. 由于密码学是一门包含很多数学背景知识且涉及广泛的学科, 大多数初学者开始学习密码学时会感到困难. 编者采用需要时才引用相应的数学背景的手段, 以弥补初学者数学背景知识的不足, 并在本书的最后部分增加了教学背景知识方面的附录, 以方便读者学习. 本书除了对密码理论的阐述, 同时还加入了大量的算法和标准, 使读者对密码学理论的实践更加了解. 希望本书能对培养信息安全方面的人才起到承前启后、抛砖引玉的作用.

本书共分 9 章. 带 $*$ 号的章节可以作为知识拓展内容.

第 1 章介绍密码学与信息安全的关系、密码体制的类型, 阐述了密码分析的类型、方法、主要依据及需具备的知识; 同时, 对密码学的相关基础知识 —— 香农 (Claude Shannon) 理论和计算复杂性理论加以介绍.

第 2 章介绍古典密码和近代机械密码的体制及其分析.

第 3 章介绍布尔函数相关知识.

第 4 章着重介绍序列密码体制的理论基础和设计思想.

第 5 章介绍分组密码的设计思想、数据加密标准 DES 和高级数据加密标准 AES 的加密原理、分组密码的工作模式.

第 6 章介绍公开密钥密码体制的产生背景、两个著名的公钥密码体制 (RSA 和 ElGamal 公钥体制) 的加密原理和安全性分析.

第 7 章介绍了数字签名和 Hash 函数的概念, 并着重介绍了数据杂凑算法 —— SHA-1 算法、RSA 和 ElGamal 签名体制.

第 8 章介绍有关密钥管理问题, 主要是密钥分配和密钥协商协议及对称密钥密码体制与非对称密钥密码体制密钥管理的不同之处.

第 9 章介绍有关身份认证的知识.

在此感谢李光松博士和博士生田甜在本书的撰写工作中所给予的协助.

在本书的编写过程中, 很多同事给予我鼓励, 指出了本书草稿中的书写和排版

的错误, 对选材的处理给予建议, 在此表示感谢! 还要特别感谢校院系领导给予的鼓励和支持. 由于时间仓促, 书中一定还有许多不足之处, 希望读者不吝指教.

作　者

2008 年 1 月 28 日

目　录

第1章 引 论

本章主要对密码学中的基本概念进行简要介绍, 并对密码学中常用的一些符号和密码分析的类型加以说明, 同时对密码学相关的信息论和计算复杂性基础知识加以阐述.

1.1 密码学与信息安全概述

研究信息的保密和复原保密信息以获取其真实内容的学科称为密码学 (cryptology). 它包括:

密码编码学 (cryptography): 研究对信息进行编码, 实现隐蔽信息的一门学科.

密码分析学 (cryptanalytics): 研究复原保密信息或求解加密算法与密钥的学科.

在邮政系统和信息的电气化传输发展以前, 通信主要由秘密信使来完成. 然而信使有被抓获和叛变的可能, 所以人们希望他们的通信不能为那些没有获得他们所提供的特殊的解密信息的人们所理解. 完成这一目的的技术就构成了密码编码学. 因此, 密码编码学是一门使传递的信息只为预定的接收者所理解而不向他人泄漏的学科. 这里所说的信息包括文字、语音、图像和数据等一切可用于人们进行思想交流的工具.

密码的出现迫使人们使用这样或那样的方法去揭示使用了密码技术的保密通信的秘密. 当然, 这一过程是在缺乏隐蔽此消息的密码技术的任何细节知识的情况下进行的. 完成这一目的的过程就构成了密码分析学, 有时也称为破译或攻击. 因此, 密码分析学是研究如何获得使用了密码技术的保密通信的真实内容的一门学科.

密码方法的使用和研究起源颇早. 四千多年以前, 人类创造的象形文字就是原始的密码方法. 我国周朝姜太公为军队制定的阴符 (阴书) 就是最初的密码通信方式.

19 世纪末, 无线电的发明使密码学进入一个开始发展的时期. 这一时期密码的主要标志是以手工操作或机械操作实现的, 通常称之为初等密码. 这类密码的编码思想是: 要么错乱明文的顺序, 要么用一个字母去替换另一个明文字母, 要么用一组字母去替换另一组明文字母, 要么对明文信息进行多次代替和置换, 以达到文字加密的目的. 这一阶段始于 20 世纪之初, 一直延续到 20 世纪 50 年代末. 这

些密码广泛应用于第一次世界大战和第二次世界大战. 例如, 第一次世界大战中使用的单表代替密码、多表代替密码、多码代替密码, 第二次世界大战中德军使用的 Enigma(恩尼格玛) 密码、盟军使用的 Hagelin(哈格林) 密码、日军使用的 "蓝密" 和 "紫密" 都是这种类型的密码. 这些密码几乎已全部被破解. 已经证明只要给予足够数量的已加密的消息, 整个消息可以被解开. 本书第 2 章介绍这样的一些密码及其破译方法.

1949 年, 香农发表了 "秘密体制的通信理论"(*The Communication Theory of Secrecy Systems*), 从此密码学发展成为一个专门学科, 密码学的发展也进入一个快速发展的时期. 这一时期的密码的主要标志是以电子技术代替了手工操作和机械操作, 极大地提高了加密和解密的速率, 因此通常称之为电子密码. 电子密码包括序列密码 (stream cipher)、分组密码 (block cipher) 和公开密钥密码 (public key cryptosystem).

序列密码将明文划分成字符, 并且用一个随时间变化的函数逐个对每一个字符进行加密. 此函数的时间相关性由序列密码的内部状态决定. 在每个字符被加密以后, 此密码设备依照某种规则改变状态. 因此, 相同的明文字符的两次出现通常将不会变成相同的密文字符.

分组密码将明文划分成固定大小的字块, 并且独立地处理每一个字块. 分组密码是简单的置换密码, 必须具有大容量的字母表以阻止穷举攻击. 1977 年, 美国的数据加密标准 DES(data encryption standard) 的公布, 使密码的应用进入到社会的各个领域, 特别是网络化蓬勃发展的今天, 密码的应用更加显示出广阔的前景.

促成初等密码向电子密码过渡的主要原因有两条: 一条是香农发表的划时代论文 "秘密体制的通信理论", 它证明了密码编码学是如何置于坚实的数学基础之上; 另一条是微电子学的发展促成人们跟随香农的某些思想, 并引入新的思想和方法, 利用电子技术设计了各种类型的电子密码, 并广泛应用于军事、外交、商业等部门. 本书第 4~6 章将介绍这些密码的设计思想, 研究这些密码的一些破译方法.

1976 年, Diffie 和 Hellman 发表的革命性论文 "密码学新方向"(*New Derections in Cryptography*), 突破了传统密码体制使用秘密密钥所带来的密钥管理难题, 使密码的发展进入了一个全新的发展时期. 这一时期密码的主要标志是加密和解密使用了不同的密钥, 加密密钥可以公开, 解密密钥需要保密. 因此, 通常称之为公开密钥密码. 在这种密码体制中, 理论上可以做到不仅加密算法公开, 而且加密密钥也是公开的. 根据这种体制, 凡是要使用这种密码装置的人都分配给一个加密密钥, 并像电话号码本一样将加密密钥公布于众. 任何人想把一份消息发给某用户, 只需查阅该用户使用的加密密钥, 并用此加密密钥将消息加密后发给该用户, 而且只有该用户才能解开用此加密密钥加密的消息, 这是因为只有该用户拥有相应的解密密钥. 由于公钥体制下加密密钥是公开的, 所以人们易于采用主动攻击, 例如伪造、篡

改消息等, 达到扰乱信息、冒名顶替的目的. 为了防止消息被篡改、删除、重放和伪造, 必须使发送的消息具有被验证的能力, 使接收者或第三者能够识别和确认消息的真伪, 实现这种功能的密码系统称为认证系统. 认证系统主要包括数据源的认证和实体的认证, 数字签名是实现认证的重要技术之一.

随着人类社会的进步与发展, 密码学逐渐成为政治、军事、外交、商业等领域内相互斗争的工具. 斗争的双方围绕信息的保密和破译, 进行着激烈的甚至是生死存亡的斗争, 这种斗争也推动了密码学的不断发展. 历史充满了这样的事实: 理想的密码体制和成功的密码分析在取得外交成功、获得军事胜利、掌握贸易谈判的主动权、捕捉罪犯、制止间谍犯罪等方面起着重要的作用.

密码学家一般都相信自己所编的密码天衣无缝. 但事实往往是 "山外有山, 天外有天".

第二次世界大战时, 德国人认为自己的 Enigma 密码是不可破的. 谁知, 正是这套 "不可破译" 的密码让德国法西斯兵败如山倒. 1940 年 8 月 8 日, 德国空军元帅戈林下达了 "老鹰行动" 的命令, 雄心勃勃地要在短时间内消灭英国空军, 但他做梦也没有想到他的命令发出不到一小时就被送到了英国首相丘吉尔手中. 德国飞机还未离开法国的西海岸, 其航向、速度、高度、架数就被标在英国军用地图上. 当英国人欢呼他们空军的战绩时, 没有人想到破译者们为此做出的贡献.

1941 年 12 月, 日本海军采用无线电静默战略伪装骗过了美国人, 成功地偷袭珍珠港. 但是, 1942 年 6 月, 日本海军对中途岛发起的登陆作战因日本密码被破译, 终于遭到毁灭性的失败, 太平洋战争从此出现转机. 中途岛海战从根本上说是情报工作的胜利.

日本海军大将山本五十六, 因其行程密码电报被破而丧命于南太平洋的事实更是广为人知. 1943 年 4 月, 山本决定到所罗门群岛各基地视察, 他将自己的行程计划用高级密码通知下属. 日本人认为万无一失的密码, 其实已被美国的破译专家所破译, 山本的行程通知无异于死亡通知.

第二次世界大战后, 密码也显过多次神威. 在 1962 年的古巴导弹危机中, 苏美剑拔弩张, 形势严峻. 据悉, 美国人心生一计, 故意用能被苏联截收、破译的密码告知其军队, 准备与苏联开战. 这一招果然吓住了赫鲁晓夫, 他终于在美国人面前丢人现眼. 埃以多次开战, 以色列人频频得手, 其原因之一, 是他们破译了埃及密码, 甚至用埃及的密码调动埃及的军队. 海湾战争, 美军取得了胜利. 美参院情报委员会主席评价这场战争时说: "没有情报, 就不会有 '沙漠风暴' 的胜利."

我国历史上也有这样的教训. 甲午海战中北洋水师的覆灭, 虽然其根本的原因在于清朝廷的腐败, 但是日本人破译了清军的密码也是一个重要的原因.

第二次世界大战中, 美国还利用破译密码所获得的情报为其外交服务. 1939 年, 日本使用最高级的安全密码 "紫密" 与驻外国的 13 个使馆、领事馆进行通信. 由

于美国破译了日本的“紫密”，掌握了日本外交谈判的底牌，每每逼日本就范. 1994年，因为美国的情报机构通过截获的国际电讯，得知法国与沙特阿拉伯正在进行一笔价值数亿美元的军火交易，这使美国先行一步从法国人手中抢下了这笔大生意.

从以上事实不难看出，成功的密码分析也为打赢未来高技术条件下的局部战争提供可靠的保障.

当今时代，高新技术发展日新月异，计算机网络的建设方兴未艾. 电子政府、知识经济、数字化部队、信息化战争等等均立足于计算机网络之上，融合于计算机网络发展之中. 而要解决计算机网络的安全保密问题，必须建立信息安全保障体系. 这个体系由保护、检测、反应和恢复四大部分构成. 其中信息安全保护是信息安全保障体系的核心和基础. 信息安全保护要在构建安全体系结构的前提下，制定安全技术规范，实现安全服务，建立安全机制，以维持网络安全可靠的运行，并满足用户的合理需求和保证信息的安全. 信息安全服务依靠安全机制来完成，而安全机制主要依赖于密码技术. 所以，密码技术是计算机网络安全保障体系的支柱，这已成为信息安全专家的共识.

毫无疑问，通信的安全和保护在未来将继续发展，这不仅因为其在军事和政治方面的重要作用，也由于它在公众事业和商业领域仍是十分重要的.

1.2　密码体制与密码分析

密码编码学是改变信息形式以隐蔽其真实含义的学科. 具有这种功能的系统称为密码体制或密码系统 (cryptographic system). 被隐蔽的信息称为明文 (plaintext)，经过密码方法将明文变换成另一种隐蔽的形式称为密文 (ciphertext). 实现明文到密文的变换过程称为加密变换 (encryption)，这种变换的规则称为加密算法. 合法接收者 (receiver) 将密文还原成明文的过程称为解密变换 (decryption)，这种还原的规则称为解密算法. 加密变换和解密变换一般是可逆的. 通常，加密算法和解密算法都是在一组信息的控制下进行的. 控制加密算法或解密算法的信息分别称为加密密钥或解密密钥. 报文或数字保密通信的过程见图 1.1，其中发出信息的一方为发方，收到信息的一方为收方. 发方把信源 (明文源) 的待加密的信息 m 送入加密器，在加密密钥 k_1 的控制下，将明文 m 变换成密文 c. 密文 c 经过信道 (有线、无线或其他方式) 发给收方. 收方收到密文 c 后，将 c 送入解密器，在解密密钥 k_2 的控制下将密文 c 还原成明文 m. 在保密通信的过程中，存在着两种攻击的方式，即非法接入者的主动攻击和窃听者的被动攻击，主动攻击者将经过篡改的密文信息 C' 插入信道，而被动攻击者只是窃听密文 C 进行分析，试图获得明文 m.

设明文空间为 M，密文空间为 C，密钥空间分别为 K_1 和 K_2，其中 K_1 是加密密钥构成的集合，K_2 是解密密钥构成的集合. 如果 $K_1 = K_2$，此时加密密钥需

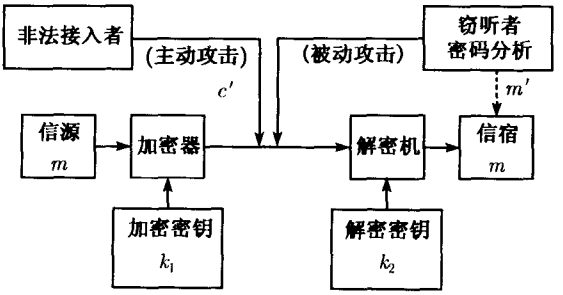

图 1.1 报文或数字保密通信示意图

经由安全密钥信道由发方传送给收方. 加密变换 $E_{k_1}: M \to C$, 其中 $k_1 \in K_1$, 它由加密器完成. 解密变换 $D_{k_2}: C \to M$, 其中 $k_2 \in K_2$, 它由解密器完成. 称总体 $(M, C, K_1, K_2, E_{k_1}, D_{k_2})$ 为一密码系统或密码体制. 对给定的明文 $m \in M$, 密钥 $k_1 \in K_1$, 加密变换将明文 m 变换成密文 c:

$$c = E_{k_1}(m) \tag{1.1}$$

收方利用解密密钥 $k_2 \in K_2$, 对收到的密文 c 施行解密变换得到原明文 m:

$$m = D_{k_2}(c) \tag{1.2}$$

如果一个密码系统的加密密钥和解密密钥相同, 或者从一个易于得到另一个, 称此密码系统为单钥体制或对称密码体制 (one-key or symmetric cryptosystem). 单钥体制的密码的保密性能主要取决于密钥的安全性. 产生满足指定要求的密钥是这类密码体制设计和实现的主要课题. 将密钥安全地分配给通信双方, 在网络通信的条件下更为复杂, 它包括密钥的产生、分配、存储、销毁等多方面的问题, 统称为密钥管理 (key management). 这是影响单钥体制的密码系统安全的关键因素. 即使密码算法很好, 倘若密钥管理不当, 也很难实现系统的安全保密.

单钥体制的密码系统可以分为:

(1) 代数作业体制: 它将明文信息输入密码机, 经过多次代替、置换, 然后输出密文信息. 初等密码中的单表代替、多表代替、多码代替和乘积密码等都属于这种类型的密码体制. 转轮密码及在转轮密码的基础上发展起来的纸带密码也属于这种类型.

(2) 序列密码体制: 它将明文信息按字符逐位加密或用序列逐位控制明文信息加密. 例如模拟话密和数字话密都属于这种类型.

(3) 分组密码体制: 它是将信息按一定长度分组后逐组进行加密.

如果一个密码系统的加密密钥和解密密钥不同, 并且从一个难于推出另一个, 称此密码系统为双钥体制或非对称密码体制 (two-key or asymmetric cryptosystem).

使用双钥体制的用户都有一对选定的密钥：一个是公开的，另一个是秘密的. 公开的密钥可以像电话号码那样注册公布，因此双钥体制又称公钥体制.

在图 1.1 中，如果敌手 (opponent) 通过某些渠道窃听或侦收到正在被发送的密文信息，然后试图用各种手段或方法去获取密钥或明文信息，那么，这种攻击方法称为被动攻击 (passive attack). 如果敌手通过更改被传送的密文信息，或将自己的扰乱信息插入到对方的通信信道之中以破坏合法接收者的正常解密，则这种攻击为主动攻击 (active attack).

密码分析 (cryptanalysis) 是被动攻击，它是在不知道解密密钥及通信者所采用的加密体制的细节的条件下，试图通过密码分析达到获得机密消息的目的. 密码分析在军事、外交、公安、商务、反间谍等领域中起着相当重要的作用. 例如，在第二次世界大战中，美军破译了日本的“紫密”，使得日本在中途岛战役大败. 一些专家们估计，同盟军在密码破译上的成功，至少使第二次世界大战缩短了八年.

密码分析的工具应包括：① 概率论和数理统计；② 线性代数和抽象代数；③ 计算的复杂性理论；④ 信息理论及其他一些特定的知识等. 例如分析语音加密要懂得语音的三大要素、语音的语图特性，分析报文加密需掌握明文的统计特性等.

密码分析的类型可以分为：

(1) 唯密文攻击 (ciphertext only attack)：破译者仅仅知道密文，利用各种手段和方法去获取相应的明文或解密密钥.

(2) 已知明文攻击 (known plaintext attack)：破译者除了有被截获的密文外，利用各种方法和手段得到一些与已知密文相对应的明文.

(3) 选择明文攻击 (chosen plaintext attack)：破译者可获得对加密机的访问权限，这样他可以利用他所选择的任何明文，在同一未知密钥下加密得到相应的密文，即可以选定任何明文–密文对来进行攻击，以确定未知密钥. 数据库系统可能最易受到这种类型的攻击，这是因为用户能够将某些要素插入数据库，然后再观察所储存的密文的变化，从而获得加密密钥.

(4) 选择密文攻击 (chosen ciphertext attack)：破译者可获得对解密机的访问权限，这样，他可以利用他所选择的任何密文，在同一未知密钥下解密得到相应的明文，即可以选定任何密文–明文对来进行攻击，以确定未知密钥. 攻击公开密钥密码体制时常采用这种攻击方法. 虽然原文是不大明了的，但密码分析者可用它来推断密钥.

密码分析的方法有穷举法和分析法两大类. 穷举法是对截获的密文依次用各种可能的密钥或明文去试译密文直至得到有意义的明文，或在同一密钥下 (即密钥固定)，对所有可能的明文加密直至得到与截获密文一致为止. 前者称为密钥穷举，后者称为明文穷举. 只要有足够的时间和存储容量，原则上穷举法是可以成功的. 但是，任何一种能保证信息安全的密码体制都会设计得使这一方法实际上不可行.

为了使这一方法实际上可计算, 破译者会千方百计地减少穷举量. 减少穷举量的方法大体上有两种. 一种是根据已经掌握的信息或密码体制上的不足, 先确定密钥的一部分结构, 或从密钥总体中排除那些不可能使用的密钥, 再利用穷举法去破译实际使用的密钥. 另一种方法是将密钥空间划分成若干个 (例如 q 个) 等可能的子集, 对密钥可能落入哪个子集进行判断 (至多进行 q 次); 在确定了密钥所在的子集后, 再对该子集进行类似的划分, 并检验实际密钥所在的子集; 依此类推, 就可以正确地判定出实际密钥.

分析法又分为确定性分析和统计分析两大类. 确定性分析是利用一个或几个已知量, 用数学的方法去求出未知量. 已知量和未知量的关系由加密和解密算法确定. 寻找这种关系是确定性分析的关键步骤. 例如 n 级线性移位寄存器序列作为加密序列时, 就可在已知 $2n$ 比特的加密序列下通过求解线性方程组破译. 应用统计的方法进行破译也可以分为两类. 一类是利用明文的统计规律进行破译. 破译者对截获的密文进行统计分析, 总结其间的规律, 并与明文的统计规律进行对照分析, 从中提取明文和密文的对应或变换信息. 第 2 章中的单表代替密码的破译方法属于这种类型. 另一类是利用密码体制上的某些不足 (例如明密信息之间存在某种相关性), 采用统计的方法进行优势判决, 以区别实际密钥和非实际密钥. 我们将在后面的章节中介绍这类方法的实现.

在破译时, 破译者必须认真研究破译对象的具体特性, 找出其内在的规律性, 才能确定应当使用何种分析方法. 一般情况下, 破译一个密码, 甚至破译一个密码体制的部分结构, 往往不是仅采用一种破译方法就可以达到破译的目的, 而是要综合利用各种已知条件, 使用多种分析手段和方法, 有时甚至要创立新的破译方法, 才能达到较满意的效果.

密码破译的结果可分为完全破译和部分破译. 如果不管采用密钥空间中哪个密钥加密的密文, 都能从密文迅速恢复原明文, 则此密码已完全破译, 这也意味着敌手能够迅速地确定该密码系统实际使用的密钥. 如果对于部分实际使用的密钥, 敌手能由密文迅速恢复原明文, 或能从密文确定部分原明文, 就说该密码部分破译. 完全破译又分为绝对破译和相对破译. 绝对破译是指破译的结果完全符合合法接收者解密密文的过程. 否则称为相对破译. 相对破译往往是根据密文可以迅速得到相应的明文, 但由明文并不一定能加密成相应的密文.

密码分析之所以能破译密码, 最根本是依赖于明文的容余度. 这是香农在 1949 年所创立的信息理论第一次透彻地阐明了密码分析的基本原理. 密码分析的成功除了靠上述的数学演绎和统计推断外, 还必须充分利用保密通信中的侧面消息和密码的编制特点.

任何一个密码体制都包含两类资料 —— 公开资料和秘密资料. 所谓公开资料是指信息加密时所用的一系列规则和算法. 公开资料是公开的. 如果密码体制是通

过硬件设计的, 其技术指标和规格都将公布, 操作说明书也可以得到. 通过软件来实现的密码体制也是如此. 公开资料也可能在一定时间内不公开, 但它绝不会像秘密资料那样绝对地保密. 因此, 所谓体制泄密是指公开资料已为人知, 然而这并未对密码的安全构成多大威胁. 所谓秘密资料就是敌方所得不到的资料, 一般是指此密码所使用的密钥, 这是一个密码绝对保密的一部分资料, 一旦泄漏便严重危害密码的安全.

破译密钥的主要任务是研究密码体制的编制特点、使用中出现的故障和侧面消息, 确定使用何种密码分析方法来获得其密钥.

侧面消息是指通信双方的各种因素的相对稳定性及其内在联系. 例如下面一段密文

DFOR KIBUC TECRELOHV DONSHU KADCRAP GEDOD LADCLIAC NOCILLN

出现在弗吉尼亚的一个中国餐馆的餐桌布上. 如同侦察案件一样, 当我们知道上述密文与汽车有关, 那么就容易得出这段密文中的单词是字母换位的结论, 从而可推出其对应的明文为

FORD BUICK CHEVROLET HUDSON PACKARD DODEG CADILLAC LINCOLN

这是一个侧面消息的例子, 它使得这段密文几乎没有什么价值了.

侧面消息还包括正在传输的数据、报文及语音等情况的相对固定性及它们之间的内在联系. 例如传输销售数据时, 用户的姓名和地址编为第一部分, 售出报单编为第二部分, 交货日期编为第三部分. 这些都是相对固定的, 报文的开头和结尾也是固定的. 同时, 在传输销售数据的一份密报中可能会多次出现像计划、交货、日期之类的词. 破译者可以根据它们去猜出部分密文的实际内容, 从而得到一些明文–密文对, 把唯密文破译转为已知明文破译.

侧面消息既可以通过保密通信双方间的联络得到, 也可以由公开渠道得到. 侧面消息的内容也是广泛的, 它可能涉及通信的内容, 也可能涉及密码机的内部结构和使用故障等.

任何一个密码体制都是按照一定的编码思想设计的. 所谓编制, 即是实现某一编码思想的全过程. 对于非代数作业的密码体制来说, 其编制是由加密器和加密密钥来实现的. 因此, 密码的编制规律是指由明信息到密信息的变换过程中所具有的整体的和个别的特征. 由于编码思想往往受各种主客观条件的影响, 所以密码体制的实现和设计不可能十全十美, 往往在体制的个别部分出现一些小的疏忽. 这些小的疏忽可以为我们破译其实际密钥打开一个缺口. 同时, 同类密码体制 (例如序列密码体制) 往往具有共同的设计思想或结构, 可以通过寻找它们的共同特征去研究具体密码的结构和特征. 破译者的任务之一是寻找密码编制上的规律, 确定或创造

出分析或破译这类密码的方法. 序列密码的相关攻击, 攻击 DES 密码的差分分析等都是利用了密码编制上的缺陷而创立的破译方法.

密码在使用过程中暴露出来的异常现象 (一般是由使用不当或机器故障造成的) 也可以被我们利用. 破译者通过侦察和分析他所截获的大量密文, 力图找出使用密码机的过程中出现的某些矛盾 (例如重复报、重码或某些异常现象等) 以获取有关密钥使用或密码体制等方面的信息.

密码体制往往受到当代科学技术的极大影响. 例如语言文字学、数学、声学、电子学、计算机理论等最新成就都不同程度地渗透到密码设计之中, 这样就决定了密码分析是一项艰巨的、复杂的、探索性很强的工作. 正如爱·伦坡所说: "人类智慧编造不出一种人类智慧所不能解开的密码." 只要认真研究密码体制及其设计思想, 努力发掘编制和使用等方面的内在规律, 总可以找到一个切实可行的分析方法.

1.3 密码体制的安全性

在以后的章节中, 我们会碰到对密码体制安全性的评价, 下面定义几个有用的准则[1].

1.3.1 计算安全性

这种度量涉及攻击密码体制所作的计算上的努力. 如果使用最好的算法攻破一个密码体制需要至少 N 次操作, 这里的 N 是一个特定的非常大的数字, 我们可以定义这个密码体制是计算安全的 (computational security). 问题是没有一个已知的实际的密码体制在这个定义下可以被证明是安全的. 但由于这种标准的可操作性, 它又成为最适用的标准之一.

1.3.2 可证明安全性

通过有效的转化, 将对密码体制的任何有效攻击归约到解一类已知难处理问题 (在本章第五节中将给出定义), 即使用多项式归约技术形式化证明一种密码体制的安全性, 称为可证明安全性 (provable security). 例如, 可以证明这样一类命题: 如果给定的整数是不可分解的, 那么给定的密码体制是不可破解的. 但必须注意, 这种途径只是说明了安全性和另一个问题是相关的, 并没有完全证明是安全的.

1.3.3 无条件安全性

这种度量考虑的是对攻击者的计算量没有限制时的安全性. 即使提供了无穷的计算资源, 也是无法被攻破的, 我们定义这种密码体制是无条件安全的 (unconditional security).