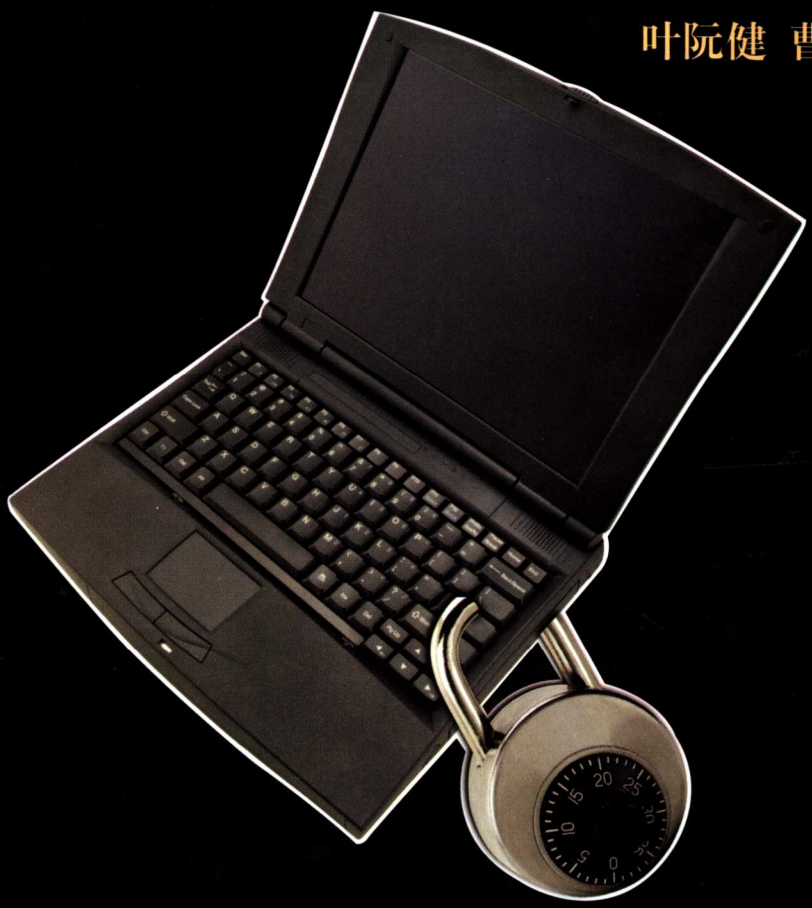
世界著名计算机教材精选

PEARSON Prentice Hall

经典密码学与现代密码学

(美) Richard Spillman 著
叶阮健 曹 英 张长富 译



CLASSICAL AND CONTEMPORARY CRYPTOLOGY

清华大学出版社

Pearson Education

EISBN: 0-13-182831-2

图书在版编目(CIP)数据

经典密码学与现代密码学/(美)斯皮尔曼(Spillman, R.)著; 叶阮健,曹英,张长富译. —北京: 清华大学出版社,2005.7
(世界著名计算机教材精选)
书名原文: Classical and Contemporary Cryptology
ISBN 7-302-10740-8

Ⅰ. 经… Ⅱ. ①斯… ②叶… ③曹… ④张… Ⅲ. 密码—理论—高等学校—教材 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字(2005)第 027345 号

出 版 者: 清华大学出版社 地 址: 北京清华大学学研大厦
http://www.tup.com.cn 邮 编: 100084
社 总 机: 010-62770175 客户服务: 010-62776969
印 刷 者: 北京市清华园胶印厂
装 订 者: 三河市化甲屯小学装订二厂
发 行 者: 新华书店总店北京发行所
开 本: 185×260 印张: 16.75 字数: 412 千字
版 次: 2005 年 7 月第 1 版 2005 年 7 月第1 次印刷
书 号: ISBN 7-302-10740-8/TP·7152
印 数: 1~3000
定 价: 35.00 元

前　言

本书的目标是介绍密码学这一令人向往的世界。这是一个多面的世界，对一些人来说，它是一个侦探与保密的世界，对另一些人来说，它是数学与计算机的世界。无论你如何看待它，密码学都是神秘而富有冒险色彩的。它还超越了传统的学术学科。它不只是计算机科学的内容，密码学的研究包括历史、政治学、工程、语言军事学、伦理、数学和工业技术学等。任何单本书都不可能从所有这些方面来介绍密码学，因此，密码学的学生必须具有宽广的知识背景。本书只是作为学习这些知识和理解这些复杂但有益的内容的一个起点。

有两个原则指导本书的写作。第一个是密码学并不是始于计算机的发明。而现代密码学全部是基于计算机的，但它们很大程度上还是要归功于经典加密技术开发者的早期工作。这些开发者利用手工和铅笔工作，以发现经典加密法中的弱点。没有计算机，甚至没有计算器的帮助，他们必须训练成能认识加密的替换模式，进行数据组织。因此，要学习如何像译解密码者那样“思考”，你需要理解和意识到经典加密法的智慧和毅力。

第二个指导原则是，密码学课程不是(也不应该是)程序设计课程。编写一两个实现加密法或分析工具的程序可能对学生很有帮助，学习为所有重要的加密法和工具编写和调试代码将花费不少时间，这势必要减少真正学习密码学知识的时间。编写加密程序应该是算法或程序设计课程的任务。因此，与本书配套有一个软件包，即密码分析软件(CAP)，可以从 www.tup.com.cn 下载，它提供了经典加密法和现代加密法的实现，并含有一套分析这些加密法的工具。本教材和该软件一起将为你的密码学学习提供真实的动手体验。

密码学的初级学生、密码学爱好者和高级学生，都将从本书和配套的软件程序 CAP 中获益。第一部分介绍了密码学的经典问题，这对不熟悉密码学领域但准备开始学习的人很有帮助。高级学生可能会快速浏览一下如何运行 CAP 软件的内容，而将更多的时间花在那些不太熟悉的加密法和分析技术上。第二部分介绍了现代密码学，包括流加密法、块加密法和公共密钥加密法。这些内容可能对高级学生更有用。第三部分介绍了密码学的未来，并对量子加密法进行了简单介绍。

目　录

第二部分　现代加密法

第三部分 密码学的未来

第1章　密码学概论

1.0　概　　述

我们生活在一个令人兴奋、快节奏的世界，任何东西的改变都比不上我们处理信息的方法快。利用 Internet，我们可以利用一些以前想都想不到的方式来访问和使用信息。不用去银行或在取款机前排队等候，我们在家就可以支付账单、签发支票和转账，而且是每周 7 天每天 24 小时都可以。不用出家门就可以申请和接收贷款。可以在 Internet 上买书、食品、礼物以及其他任何东西。不用周末去跳蚤市场，通过网络就可以在任何时间卖东西。我们还可以买卖股票，给他人邮寄信息。随着无线技术的出现，我们用手机在全球任意地方都可以完成所有以上事情，甚至不止这些。

诚然，这些都是令人兴奋的事，但也有不好的一面。同样的技术可以使我们的生活更方便，但若被罪犯利用，就将危及我们的生活。例如，在当今的美国，窃取身份证是增长最快的犯罪之一。它之所以盛行，是因为法律惩罚没有跟上犯罪的步伐，而且这种犯罪很容易实施。这是因为大多数的个人信息缺乏保护。要享受新技术给予的好处，避免陷阱，就必须具有一些保护我们身份和个人信息的方法。如何实现这些正是本书的主题。本书是关于“秘密书写”的，这已有几个世纪的历史了，但现在已经成为了保护和辅助信息技术发展的一个重要作用力。这个领域就称为密码学(cryptography)。

密码学研究的是编码和加密法。David Kahn 在他的被称为“密码学圣经”的著作中是这样定义密码学的：“密码术(cryptology)就是保护。通信对于现代人来说，就好比甲壳对于海龟、墨汁对于乌贼、伪装对于变色龙一样重要。”它已有好几百年的历史了，但仍是年轻、新颖和令人兴奋的。它是一个不断变化且出现新挑战的领域。因此，本书不是一本只让计算机和数学人员感兴趣的干巴巴的教科书。本书同时还介绍了历史、政治学、语言、军事策略，甚至是博弈。本书涵盖了秘密隐藏在我们所生活的世界中的很多知识。

1.1　密　码　学

从某种角度来说，本书是一部肥皂剧。该剧是关于 Alice、Bob 和 Eve 三人的故事。这三个人的名字一直以来就被密码员(cryptographer)用来说明密码学和密码分析法的原理。人们总是这样认为，Alice 和 Bob 相互发送消息，而 Eve 则企图获取 Alice 和 Bob 之间的交谈内容。由于 Alice 和 Bob 都清楚 Eve 的意图，所以他们都尽量防止 Eve 发现他们的消息的内容。这个小型的肥皂剧如图 1.1 所示。

Alice 和 Bob 相互发送的消息称为明文(plaintext)，因为这些文字对任何人都是可读的。当他们第一次开始通信时，所发送的明文没有任何保护。但他们很快就发现，如果不对

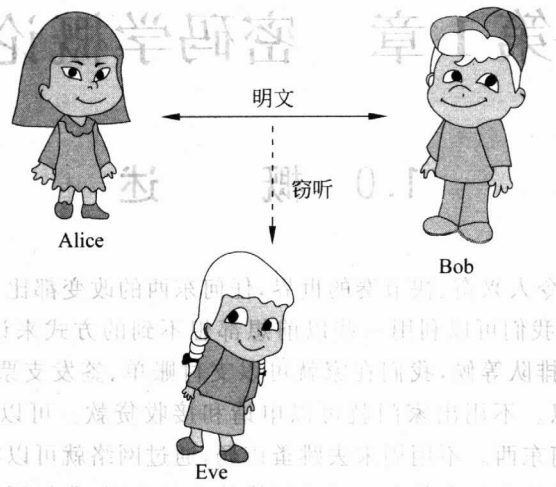


图 1.1 典型的通信模型

这些消息进行任何保护，包括 Eve 在内的任何人都可以阅读它们，因此，为了防止 Eve 阅读他们的明文消息，Alice 和 Bob 决定以某种方式对消息进行保密(hide)，这种方式就是他们自己可以还原(recover)明文，而 Eve 则不能。以这种方式隐藏消息从而使其内容保密的过程称为加密(encryption)。经加密后的消息称为密文(ciphertext)。从密文还原明文的过程称为解密(decryption)。加密和解密过程由某种算法决定，并由一个密钥(key)控制，该密钥只有 Alice 和 Bob 才拥有。Alice 用该密钥对其明文加密，然后将密文发送给 Bob。Bob 利用同一密钥将密文解密成明文。即使 Eve 截获了该密文，该密文对她来说也是毫无意义的，因为她没有密钥。这一过程如图 1.2 所示。

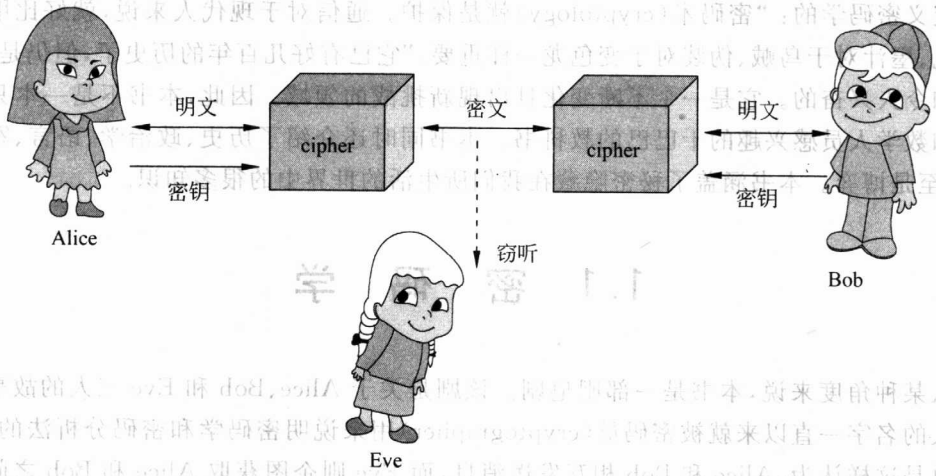


图 1.2 典型的通信模型

Alice 和 Bob 所面临的问题是，Eve 不仅聪明，而且很有毅力。一旦他们使用某种加密方法后，Eve 要破解(break)这种加密法只是时间问题。这就是说，Eve 总是可以不用密钥来还原明文，或从密文中还原密钥。这就迫使 Alice 和 Bob 去尝试更加复杂的加密方法。因此，Alice、Bob 和 Eve 的故事是没有结尾的。Alice 和 Bob 总是企图领先 Eve 一步，而

Eve 则总是以更聪明的方法来破解这种加密法(cipher)。通过本书的学习,你可以顺着这个有趣的故事发展下去,看看 Alice 和 Bob 如何开发新的加密计算,而 Eve 又是如何找到新的工具来破解的。但是,在开始这个故事之前,有必要先来定义一些基本术语。

1.2 重要术语

密码术(cryptology)是构建和分析不同加密—解密方法的科学(某种程序上也可以说是艺术)。该科学实际上是包含两部分。**密码学**(cryptography)是构建功能更强大、更有效的新的加密—解密方法的科学。**密码分析学**(cryptanalysis)则是发现已有加密法的弱点,以便不用密钥就能还原成明文的科学。本书介绍了这两部分内容。你将学习如何保护数据,如何发现当前数据加密法的弱点。对这两个方面的学习,使你更好地了解它们。了解加密的不同方法让你更容易发现某些加密算法的弱点。另外,只有理解加密解析法,才可能判断给定加密法的价值。这就是说,任何一位优秀的**密码师**(cryptologist)必须站在 Eve 的角度,以便判断他们的加密算法的安全性。

首先必须区分的是**编码法**(code)和**加密法**(cipher)这两个术语。因为有时会错误地用它们来描述同一过程。这两者都是用来加密信息的方法,但它们是以完全不同的方式进行的。编码法就是用字、短语或数字来替代明文。例如,"bomb"可能在消息中以数字"1508"的形式出现。**从码文**(codetext)还原明文不存在算法或密钥。生成码文或还原明文需要一本**编码簿**(codebook),它列出了所有数字(或替代字符)和与之相对应的明文字、短语或字母。加密法则是使用算法或密钥来加密信息。

如果一段时间内频繁使用某种编码法,由于编码簿的大小有限,终将给系统的安全性带来威胁。而且,编码的任何改动都需要重新印刷和发布一本新的厚厚的编码簿。潜在的敌人就可能获得发布的编码簿,从而破解编码。而对加密计算密钥的改动,则安全得多。发布一个密钥比邮寄一本厚的编码簿更容易,风险也更小。因此,编码法现今使用很少。但这并不意味着管理多密钥的过程就容易。事实上,在加密法中,密钥管理过程是一个很重要的问题。这些内容将在第 9 章中介绍。

除编码法和加密法外,加密信息的另一种方式是**夹带加密法**(steganography)。该方法是将密文进行隐藏的方式来加密信息的。例如,密文可能夹带在一幅图画或其他消息中。使用不可视墨水是夹带加密法的另一种方式。夹带加密法的使用未能推广是因为密钥问题,但是,随着用计算机进行图像处理的现代技术的应用,这种方法又重现光明了。

1.3 加密法的评价

贯穿本书的主题是如何开发一个好的加密法。通过了解 Alice 和 Bob 是如何领先 Eve 一步,你将学习如何开发一个好的加密法。Eve 对 Alice 与 Bob 的成功破解说明了加密法的一个弱点,这将成为加密法质量的一个测试。每章的末尾都有一个小结,从 Alice、Bob 和 Eve 的角度,概述了一个加密法的设计原理。

但是，任何关于加密法的讨论都必须从加密学的通用原理开始，也就是说，必须假定**偷听者具有加密数据所使用的算法知识**。这就意味着，不要以为加密算法是新的或是对外人是未知的，数据永远都是不安全的。只有加密算法的密钥是安全的，数据才是安全的。永远不要指望敌人不明白你的数据的加密原理。应总是假定他们知道加密算法的详细细节。这就叫作 Kerckhoffs 规律，这也是佛兰德的密码员 Auguste Kerckhoffs 在他 19 世纪的著作 *La Crypthographie Militaire* 中所列举的加密系统必具的六条要求之一。这六条要求现在仍认为是所有加密算法的基础：

(1) 加密系统在实际中应是不可破解的，尽管不是理论上不可破解的。

(2) 破解加密系统应不会打扰通信者。

(3) 密钥应无须做记录即可记住，并容易修改。

(4) 密码应能够用电报来传输。

(5) 设备或文档应一个人即可携带或操作。

(6) 系统应很容易操作，无须掌握一长串的规则或进行专门培训。

20 世纪 40 年代，Claude Shannon 提出了一个常用的评估概念。他认为一个好的加密法应具有**模糊性**(confusion)和**扩散性**(diffusion)。模糊性意味着加密法应隐藏所有局部模式，也就是说，语言的任何识别字符都应变模糊。加密法应将可能导致破解密钥的提示性语言特征进行隐藏。扩散性要求加密法将密文的不同部分进行混合，使任何字符都不在其原来的位置。本书前部分将介绍的很多经典加密法，要么不具备其中的某个特性，要么一个特性也不具备。正是由于未能满足这两个 Shannon 条件，所以它们能被破解。

与其他大多数技术一样，加密系统的评估最终也要落到经济因素上来。一个加密法不必光为了安全而“牢不可破”(而且，它未必就是牢不可破的)。如果获得信息的代价比破解加密的代价更小，就可以称该数据是安全的。或者，如果破解加密需要的时间比信息的有用周期更长，该数据也是安全的。因此，任何加密法的最终安全性是基于这样一个原理：付出大于回报。

1.4 密码分析法

在 Alice 和 Bob 面临创建一个安全的加密法的同时，Eve 也不得不紧跟他们的脚步。Eve 利用所有工具和她所收集的辅助信息，来破解所截获的密文。本书将探究 Eve 的破解过程，让你掌握如何发现加密法的弱点，这就是密码分析的目的。但是，有一点很重要，必须明白，那就是密码分析是一把双刃剑。破解知识可用在好的方面，也可用在坏的方面。学习密码分析法的重要原因是：它是评估新的加密法的必需工具，它在保护国家安全上起着至关重要的作用。另一方面，它也可能成为危害他人隐私的工具。Eve 攻击 Alice 与 Bob 之间的通信可以不是为了任何利益，但她毕竟是有害的。你应确保，你学习密码分析法知识是为了保护自己而不是去危害他人。

Eve 攻击 Alice 与 Bob 的加密法的方法有三种。第一种称为**密文**(ciphertext-only)攻击。当 Eve 获得了 Alice 与 Bob 所传输的全部密文后，她将只凭从密文中获得所有信息来

生成明文。第二种称为**已知明文**(known-plaintext)攻击。在这种情况下,Eve 具有密文和全部(或部分)明文。她可能发现 Alice 和 Bob 总是用同样的句子开始或结束他们之间的消息通信。利用这些信息和密文,Eve 就可能发现密钥。知道一组明文—密文集的密钥,有助于她探查 Alice 与 Bob 的其他通信。第三种称为**选取明文**(chosen-plaintext)攻击。在这种情况下,Eve 试图影响 Alice 与 Bob 之间的消息的特性。她可能给 Alice 一些有趣的信息,她知道 Alice 会将这些信息发送给 Bob。她选择这些信息,这样明文和密文就具有一个很重要的特性,从而有利于密钥的发现。Eve 可以利用这些信息,再加上 Alice 的密文,从而尝试和发现 Alice 的密钥。

显然,密文攻击最为困难,而选取明文攻击最为容易。本书将使用这些攻击方法的一种或多种对所介绍的各种加密法进行攻击。当你学会了破解加密后,应遵守道德和伦理规范。虽然前面已经强调过,但由于这一点太重要了,有必要反复重申。使用密码分析技术破解特定明文只有两个好的原因:国家安全的需要或法律实施的需要。尽管这样,也必须得到特定和法律的许可。另一方面,研究加密系统的弱点也是使用密码分析法的一个很好原因:确保用最健壮、最安全的加密法用于保护敏感信息。

1.5　编码与加密法的历史简介

保护信息的过程具有悠久而迷人的历史。关于加密的历史,有几本很好的书,但关于加密法的经典书则要算由 David Kahn 编写的 *The Codebreakers* 一书了。该书不仅介绍了加密法的历史、技术细节及描述,并介绍了实际的应用。作者建议对密码学领域感兴趣的人都应去读读该书。

在古埃及人的坟墓中发现了早期的编码与加密。其实际的使用已经失传了,但据推测,这些"秘密书法"是为了给墓主的生活增加神秘气氛,从而提高他们的声望。希伯来人开发了三种不同的加密法:atbah、atbash 和 albam,它们都是以替换为基本工作原理的。一个字母表的字母与另一个字母表的字母配对。通过用相配对的字母来替换明文的每个字母,从而生成密文。这种配对关系就相当于密钥,每种加密法都有不同的配对方式。atbah 加密法是先用数字按顺序标出希伯来字母表中的每个字母,就像在英语中将"a"标为 1,"b"标为 2,等等。前 9 个希伯来字符进行配对,这样使它们的值之和为 10;其余的再进行配对,其值之和为 28。消息中的每个明文字母都被配对的字母替换。atbash 加密法是把字母表中的最后一个字母与第一个字母配对,倒数第二个字母与第二个字母配对,以此类推。albam 加密法则是把字母表分割为两部分,再使其两两配对。

据说早期的希腊人使用的一种"秘密书写"方法是,先将奴隶的头剃光,然后将消息刺在头上,等头发长好后,再派他上路。这其实就是夹带加密法的一个示例,因为消息并没有编码,只是进行了隐藏而已。

斯巴达克人是最早将加密技术用于军事消息传递的人之一。他们发明了一种称为 skytale 的工具(实际应拼写为 scytail,其发音为 skytale,因而变成了它的名字)。这种工具是一根有固定面的竿。把一块布或羊皮纸缠在该工具上,再在竿上书写消息。当把布解开后,其上的字母顺序就变乱了(这其实就是换位加密法的一个示例)。要还原明文,须将布缠回到类似的 skytale 工具

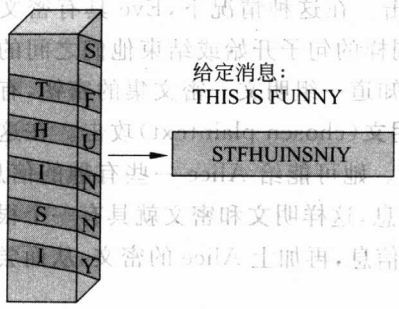


图 1.3 Skytale 加密法

上,如图 1.3 所示。这种对消息的加密方式与希伯来人使用的有着本质的不同。斯巴达克人没有用密文去替换明文,他们只是重新排列了明文字母的顺序。

在 David Kahn 的经典著作 *The Codebreakers* 一书中,他把密码学(即加密与密码分析的组合)归功于阿拉伯人。实际上,也的确是他们创造了"加密法(cipher)"一词。关于密码学的早期主要著作出现在 15 世纪早期由阿拉伯科学家 al-Qalqashandi 完成的百科全书第 14 卷中,它也是介绍密码分析法最早的著作之一。

在欧洲的"黑暗时代",科学艺术,包括密码学,进展甚微。但当欧洲开始从"黑暗时代"中走出来时,编码和加密经历了一个快速发展的阶段。政府成立了大型的间谍网络,并开发了不少加密法以便于他们之间的通信联络,而且这恰好对阅读敌人的加密信息也很有用。因此出现了一个新的政府组织(今天,该组织已成了大多数政府的一个重要部门),称为"保密局(black chamber)"。保密局的任务是截获并解密重要信息。这些组织很成功,并开展了一些很重要的通用解密分析法的初始工作。一个成功的例子是英国的解密部门,在 18 世纪,它的主要工作是阅读美国和欧洲的邮件。

直到 20 世纪美国才设有官方的保密局。这并不意味着美国就不重视加密技术。在 Thomas Jefferson 的很多成就中就有关于功能强大(就当时而言)的加密工具的发明,称为轮加密(wheel cipher)。轮加密使用了一组相互独立的"轮",其上都是以随机顺序刻写的字母表。这些轮可以转动,使明文出现在同一条直线上,而密文则可以从其他任意直线选取,如图 1.4 所示。

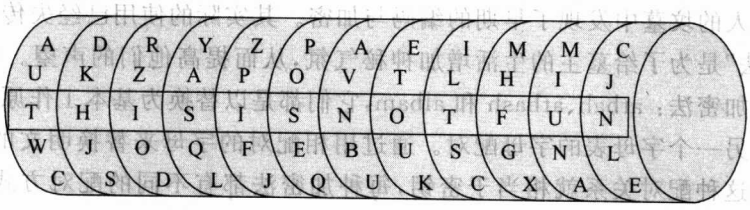


图 1.4 轮加密法示例

第一次世界大战期间,美国终于成立了自己的保密局,称为 MI-8,由 Herbert O. Yardley领导。战争结束后,他继续在纽约市领导该部门。第一次世界大战后,MI-8 非常成功地破获了日本的密码,因此在早期的裁军谈判中,美国处于很有利的位置。所有这些在 1929 年发生了变化,美国的保密局被解散,其任务由陆军和海军承担。

第二次世界大战时期,英国和美国的保密局都成功破获了轴编码法(axis code)。美国政府能阅读日本的大多数密码,而英国(在来自波兰的密码破译家的帮助下)则能阅读德国的密码。不用说,能阅读日本和德国的密码,对联军的胜利起了很大的作用。

今天,美国有了世界上功能最强、最成功的保密局之一,称为美国国家安全局(National Security Agency, NSA),它负责开发新的加密法和对已有加密法的分析。

对于历史上有关加密技术的使用及其影响的真实事件,将在讨论一些经典加密法和现

代加密法的时候介绍。现在，你应该能知道，密码学具有悠久而迷人的历史了吧。

1.6　经典加密法与现代加密法

本书将加密法的内容分为两大类（正如本书的标题所表示的那样）：经典加密法和现代加密法。经典加密法就是以单个字母为作用对象的加密法，而现代加密法则是以明文的二元表示为作用对象。以这种方式描绘其区别，更能清楚地明白经典加密法是有历史（和基础）原因的，而现代加密法更多的是实用。每种类型的加密法又根据生成密文所使用的算法本质，可以进一步细分成如图 1.5 所示。

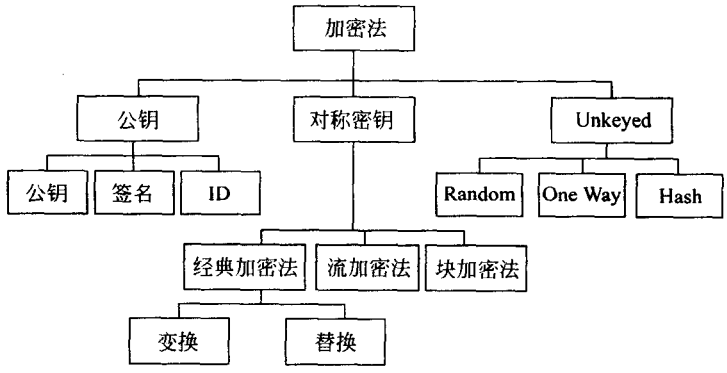


图 1.5　加密法分类

如图 1.5 所示，历史上经典加密法有两种基本类型。一种是替换（substitution）加密法，每个密文字母被其他字母替换，也就是说，每个明文字母“a”可能被密文字母“c”替代。希伯来人所使用的就是这种加密法。另一种是换位（transposition）加密法，明文中的每个字母没有改变，但它们在密文中的位置进行了重新排列（如斯巴达克人使用的 skytale 加密法），也就是说，单词“next”在密文中可能成了“xent”。

图 1.5 没有显示这两种经典加密法的进一步分类，否则将使该图太复杂了。例如，在经典的替换加密法中，又有两种方法。一种称为单码加密法；另一种称为多码加密法。单码加密法的特征是，每个明文的字母正好映射到一个密文字母，这也就是说，一旦明文的字母“a”被密文的字母“n”替代，那它总是被“n”替代。而在多码加密法中，同一个明文字母可能用多个不同的密文字母来替代。例如，明文字母“a”可能用密文字母“n”、“s”或“y”来替换。显然，多码加密法的生成和破解比单码加密法更困难。但后来发现，即便是多码加密法也有其弱点。

1.7　CAP 软件介绍

本书介绍的很多内容都将用一个称为加密分析程序（CAP）来演示说明。CAP 软件可以从 www.tup.com.cn 下载，它运行在基于 Windows 的 PC 机上。随着不同章节的内容介

绍，你将学习如何使用 CAP 软件，但这只是简短的介绍而已。

CAP 软件是一个 Windows 程序，可以生成和破解密码，它包含了本书所讨论的经典加密法和密码分析技术，以及一些现代的加密系统。它还有一个富有挑战性的博弈游戏，你可以用来测试一下你的加密破解技术。该软件还有一个自动密码分析系统，可以一步一步地指导你如何破解一个加密法。

双击 CAP 软件的图标，可以打开 CAP 主窗口，如图 1.6 所示。从该窗口，可以浏览 CAP 软件的各种不同特性。

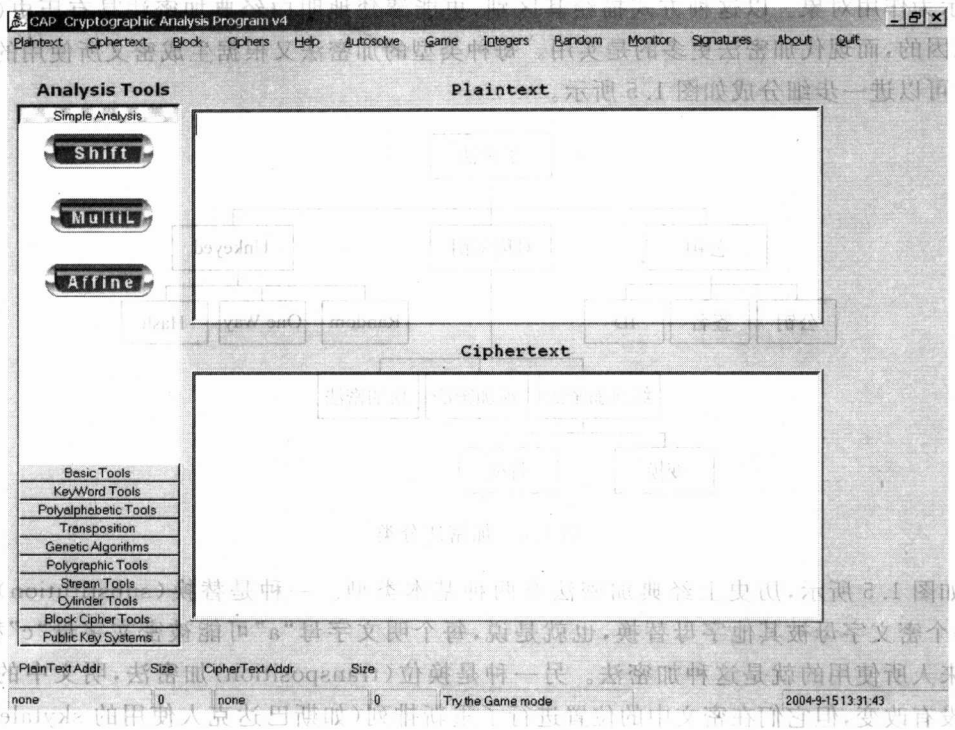


图 1.6 CAP 软件的主窗口

在 CAP 软件的主窗口中，有两个主要区域，分别为 Plaintext 框和 Ciphertext 框。这两个框就像两个小的字处理器，你可以在任意一个中直接输入文字并将它保存，随后还可以在这两个框中将所保存的文件打开。

为了说明 CAP 软件的使用，来看看一个最简单的替换加密法。该加密法称为恺撒加密法，因为朱利叶斯·恺撒使用过它，用来把与高卢进行的战争的消息送回罗马。恺撒使用的密钥是移动 3 位。后来，奥古斯塔斯·恺撒使用的密钥是移动 1 位(即 A 到 B，B 到 C，…，Z 到 A)。首先按顺序写下 26 个字母：ABCDEFGHIJKLMNOPQRSTUVWXYZ。恺撒加密法将把明文中的每个字母用其右边的第 4 个字母替换，也就是说，“a”将被“d”替换，“b”将被“e”替换，以此类推。而后面的字母，如“x”将被“a”替换，“y”将被“b”替换，最后，“z”将被“c”替换。CAP 软件将自动实现这种移位加密。只要在 Plaintext 框中输入明文，从 Cipher 菜单中选取 Simple Shift 菜单项，将出现图 1.7，要求输入移位的个数。恺撒加密法使用的是 3，你也可以选择 1～25 之间的任何数。