公钥密码学

PUBLIC – KEY CRYPTOGRAPHY

(芬兰)Arto Salomaa 著　丁存生 单炳娟 译

公钥密码学

Public-Key Cryptography

(芬兰)Arto Salomaa 著

丁存生 单炜娟，译

国防工业出版社

·北京·

著作权合同登记　图字:军-1996-010号

D920/50-23

图书在版编目(CIP)数据

公钥密码学/丁存生,单炜娟译.—北京:国防工业出版社,1998.1

书名原文:Public-Key Cryptography

ISBN 7-118-01777-9

Ⅰ.公… Ⅱ.①丁… ②单… Ⅲ.保密通信-密码术 Ⅳ.TN918

中国版本图书馆 CIP 数据核字(97)第 12302 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 100044)

国防工业出版社印刷厂印刷

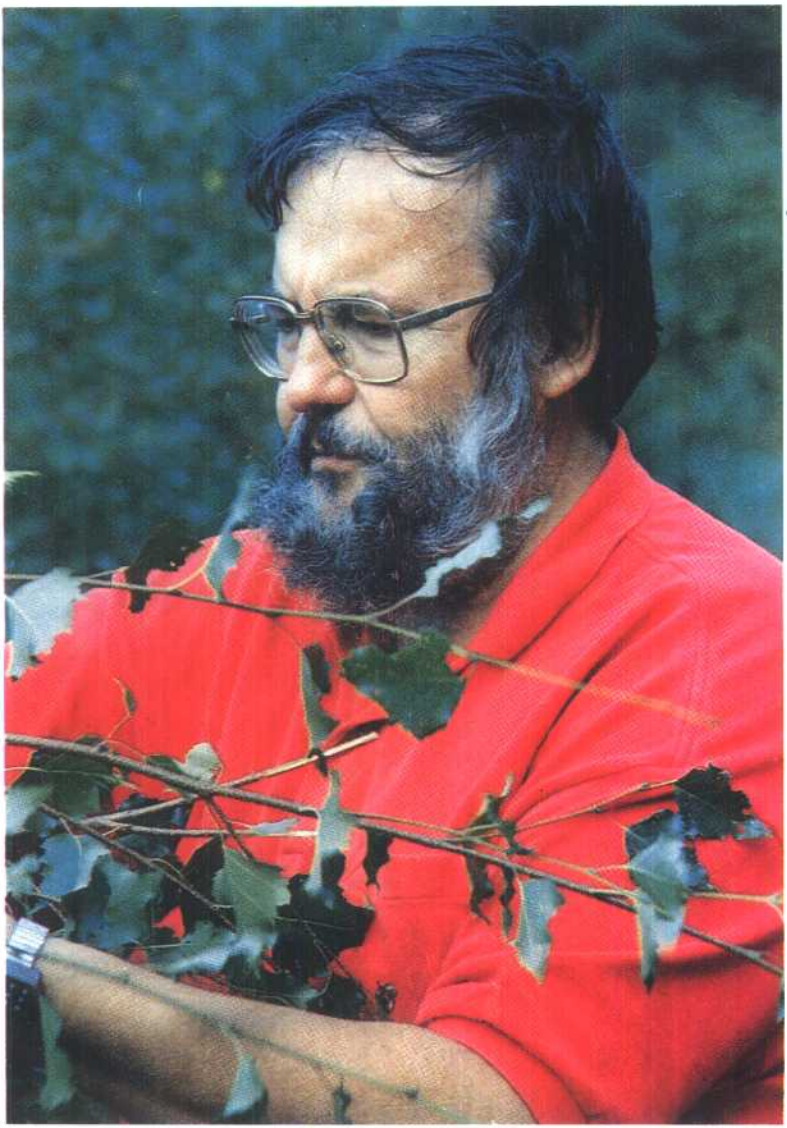
新华书店经售

*

开本 850×1168 1/32 印张 9⅛ 插页 1 237 千字

1998 年 1 月第 1 版 1998 年 1 月北京第 1 次印刷

印数:1—1000 册 定价:25.00 元



Arto Salomaa 教授简介

Salomaa 教授 1934 年 6 月 6 日生于芬兰 Turku 市，受教育于芬兰和美国。1960 年获得 Turku 大学博士学位。他从世界上 6 所大学共获得 6 个荣誉博士学位。1965 年至今为 Turku 大学数学系教授；同时他是芬兰科学院教授。Salomaa 博士曾经是加拿大 Western Ontario 大学计算机系、丹麦 Aarhus 大学计算机系和加拿大 Waterloo 大学计算机系访问教授。Salomaa 教授访问过欧洲、北美洲和亚洲的 150 所大学。

Salomaa 教授在 50 个国际会议上作过特邀报告，是 35 个国际会议的程序委员会委员，包括 4 次国际会议主席。自 1970 年起他是芬兰科学院院士，1980 年起是芬兰瑞典科学院院士，1992 年起是欧洲科学院院士。他是 Nevanlinna 奖评选委员会主席，国际 Godel 奖授奖委员和主席。自 1973 年起他是欧洲理论计算机协会常委委员，1979 年～1985 年为欧洲理论计算机协会主席。

Salomaa 教授著有 400 多种科学出版物，包括 10 本英文专著。他的专著已被翻译成中文、德文、法文、日文、俄文、越南文和罗马尼亚文。他是 8 种国际杂志的编辑，包括北京出版的《计算机科学和技术》杂志。他也是 Springer 出版社理论计算机科学丛书主编。

中 文 版 序

《公钥密码学》中文版的出版对我是一个很大的荣誉，同时也给予了我极大的快乐。我一直非常钦佩中国人和中国文化。童年在芬兰的时候我已经知道中国这个国家，而且大多数东西远在传入欧洲之前已被中国人了解。

这种观点一定同样适合密码学(秘写的理论)中的许多技术。然而，这本书是从西方概念和西方书写格式的角度来讨论密码学的。其中心是70年代中期引入的公钥思想。

我个人一直对密码学感兴趣。事实上，秘写是我最早的智力活动之一。在我家周围的男孩中，我是众所周知的能够破解任何密码的一个！在数学逻辑、自动机理论和形式语言领域从事研究后，我在80年代早期对童年感兴趣的密码学进行了研究。这本书是在我的几个密码学教材基础上发展起来的。

在我的学术生涯中，认识并与几个杰出的中国学者的合作使我受益。我和几个中国科研者合作撰写了一些文章，目前与他们中的两个正在合作写一本书。在家庭方面，我儿子的妻子是一个中国人。

我特别感谢本书的译者丁存生、单炜娟夫妇。当丁存生做我的博士生时，我认识了他们俩，但是这种关系在科研和生活方面发展成了一种真正的友谊。

让我用一个有关语言和密码学的评述来结束该中文版序。一个普通芬兰人(譬如我自己)根本无法读懂中文，因而对于我们而言只要写成中文则不需要任何加密！那么反过来如何？中国读者能读懂我的母语吗？我的土尔库母语与标准芬兰语相当不同，如下是一个测验。如果你能读懂以 F(或 M 或 H)开头的句子，你已经初步(或一般或很好)地掌握了我的母语！

FIINI FRÖÖKYNÄ FRIIAS FRIIPÄIVÄN FÖRIÄIJÄ.

MUINOSTE MAMMA MAKIASOPPA MASSUTETTI, MAROSSI MARRATTI.

HÄPPEVÄINE HURATTANU HUUSSA HURATTI HUUSSI.

Arto Salomaa

土尔库，1996 年 3 月

序

密码学，即秘密书写，很可能与人类文字同样古老。近年来这一学科得到了广泛科学研究。数据安全方面的众多新应用说明了这一科学研究的必要性。密码学得到广泛研究的一个更为重要的原因，也许是公钥密码学这一创造性思想及由此引起的通信新前景。

这本书以经典密码学为起点，对公钥密码学给出了一个新颖阐述，并力图覆盖某些最新研究成果和目前公钥密码学的新特征。本书的明文例子提供了芬兰浴的基础知识。

致谢：Hermann Maurer 在 70 年代后期唤醒了我对密码学的潜在兴趣。1983 年以来我用这本书的某些版本作为 Turku 大学、Leiden 大学和 Wien 技术大学的密码学教材。参加这些课程的听众提供了有益的建议。Juha Honkala，Jarko Kari，Valtteri Niemi，Lila Santean，Mika Niemi 和 Ari Renvall对这本书手稿的不同部分提供了意见，其中前四人也参与了一些讨论。我也与以下同事进行了有益的讨论：Ron Book，Wilfried Brauer，Karel Culik，Ferenc Gecseg，Jozef Gruska，Tero Harju，Iiro Honkala，Helmut Juergensen，Juhani Karhumaki，Werner Kuich，Hannu Nurmi，Kaisa Nyberg，Azaria Paz，Grzegorz Rozenberg，Kai Salomaa，Aimo Tietavainen，Emo Welzl，Derick Wood 及 Sheng Yu。我特别感

谢 Elisa Mikkola 对这本书的出色打印及对许多事情的协助。Anu Heinimaki 为这本书画了图，芬兰科学院为我提供了非常好的工作条件。我同时感谢与芬兰科学院(特别是与 Marjatta Naatanen)的良好合作。科学机构 MATINE 对我的密码学研究给予了资助。最后我感谢 Springer 出版社，特别是 Hans Woessner 博士和 Ingeborg Mayer 女士所给予的良好合作及对本书的及时印刷。

Arto Salomaa

Turku，1990 年 5 月

译者的话

在今天的信息安全中，特别是在数字签名、认证和密钥管理中，公钥密码学是必不可少的。Arto Salomaa 教授的这本书是这方面一本系统且有创新的专著。为使读者掌握公钥思想，作者仔细地准备了大量例子。本书也包含作者在这一领域的许多研究成果。细心的读者也应在本书中学到芬兰浴（桑拿浴）的基础知识（Arto Salomaa 教授也是芬兰浴方面的著名专家，而本书的例子提供了桑拿浴的入门知识）。

据我们所知，该书的英文版已经在世界各地的许多大学作为教材和参考书。另一方面，Arto Salomaa 教授是计算机界和数学界的巨人之一。我们现在非常高兴地看到该书出版了中文版，它将对我国密码学的教育和科研是一个很大的推动。

Arto Salomaa 教授将该书的中文出版权无偿授予了国防工业出版社，我们首先对此表示感谢。其次，我们感谢国防工业出版社对出版该书中译本的大力支持。西安电子科技大学王育民教授、中国科学院卿斯汉教授和陶仁骥教授对该中文版的出版也给予了大力支持，信息安全国家重点实验室冯登国博士后在译稿校正方面付出了辛勤的劳动，我们在此一并表示深深的谢意。

Arto Salomaa 教授也是新书 Chinese Remainder Theo-

rem(中国剩余定理)的作者之一。借此机会,我们感谢他热情地向世人介绍这一中国文化。

就个人而言,我们非常幸运地有机会与 Arto Salomaa 教授在一起工作。我们不仅从他那里学到了许多科研技巧,而且学到了许多科学写作知识。他对我们家庭已经有了很大的影响,将来还会有更多的影响。

丁存生,单炜娟

1996 年 9 月

目　录

第一章　经典双向密码学

§1.1　密码体制与密码分析

密码科学和艺术由两个世界组成。其一是合法通信的世界，例如像合法使用数据库交换信息的用户，这是一个充满阳光的世界。其二是敌方的黑暗世界，敌人设法截获消息、并尽力做各种坏事。合法世界的人希望敌人无法读懂消息，而敌人却想要易懂的消息。

密码学是在这两个世界的斗争中发展的。敌人的成功意味着合法世界的人必须加强他们的加密方法，而加强后的方法将对敌人是一个新的挑战。因而，这种斗争将持续下去。永恒的数学结论可能不实用。

如何在这本书中刻画这两个世界？就过去的事情而言，这并非难事。只要先描述合法世界的一个加密方法，然后叙述敌人是如何破解该方法即可。但谈现在就没那么容易。无论什么时候，只要我们能描述一个有效的攻击方法，我们不得不承认合法世界所采用的相应方法是不安全的。然而，成功不能在两个世界中并存。

我们可以先详细描述合法世界，然后概述一些可能的攻击方法，同时说明这些方法不能奏效的原因。当然，这并不意味着不存在其他破解方法，也许敌人有特别聪明的方法。然而我们将在以下章节中采用这种写作手法。虽然我们无法达到数学上的肯定性，但这些方法的安全性通常是很高的。

值得注意的是，虽然我们将这两个世界分别称为“合法的”和“黑暗的”，但前者有可能由恶魔组成，而后者由“好人”组成。在实际场合中，两者的角色可以互换。譬如，在战争中我们国家设法截获消息，而消息发送者则是我们的敌人。当然正义在我们一方！同

样，一个数据库的合法使用者可能是一个罪犯，而警察正在跟踪他。事实上，我们以后所用的术语是中立的，而不对这两个对立世界做评价。

我们现在介绍密码学中的最基本概念，这些概念将贯穿这本书。值得强调的是，出现在不同密码文献中的术语并非固定不变。介绍本书使用的术语时，我们也将介绍其他作者对同一概念所用的不同术语。我们将自始至终用密码编码学这个术语来表示秘写，它包含这两个世界的活动。有些作者对此使用密码学一词，而用密码编码学表示合法世界的活动。

我们的基本出发点由图 1.1 给出，其中一个消息通过一个信道发送给接收者，这个消息有可能被窃听者所截获。

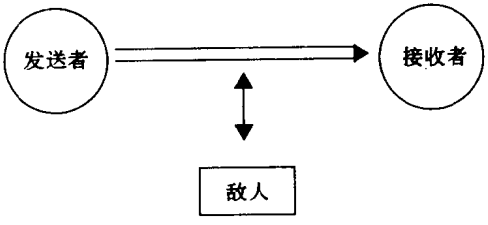


图 1.1

不管我们谈论的是马背信差还是电子邮件，这个图总是一样的。由于我们无法实现信道的安全，消息有可能被截获。敌人的主要目标是破坏通信保密，并从秘密消息中获益。更高的目标可能是：敌人可能想修改消息，以达到用假消息迷惑接收者。这样，接收者在谁是发送者这个问题上也同样受骗。

例如，发送者可能给接收者发送这样的消息："我将不会给绿党帮助"。如果敌人将这条消息改为"我将给绿党 10000 美元"，则接收者不知道这个完全不同的消息是谁发送的。

敌人也有可能就接收者身份问题来欺骗发送者。例如，敌人获取消息后而不将消息传送给接收者。

在所有情况下，如果敌人无法理解所截获的消息，这将对发送者和接收者特别有利。为此，发送者需要某种加密方法。

原来的消息称为明文。因而，发送者对明文进行加密，而所得的东西称为密文。该密文通过不安全信道传送。最后，接收者对密文解密即可得到明文。

因此，发送者的变换工作是：将明文加密成密文。接收者的变换工作是倒过来：将密文解密成明文。

我们可用如下较为简洁的符号表达式：

$$E(pt) = ct, D(ct) = pt$$

文献中常用“原文”和“暗文”或“密码”来分别代替“明文”和“密文”。在这种情况下，变换表示“加密”和“解密”。术语“码”及相应的动词“编码”和“解码”也曾用于文献中，但已不再使用。原因是名词“码”另有含义，即纠错码、理论自动机码等。“码”将在以后的某些特殊场合使用，但不表示一般意义下的“密文”。

我们现在来进一步分析加密和解密。两者都在密码系统框架内工作。一个密码系统的构成如下：

(1) 一个明文空间 PT，即所有可能明文 pt 的集合。

(2) 一个钥空间 K。K 中的每个 k 确定一个加密方法 E_k 和一个解密方法 D_k。如果先将 E_k 作用到一个明文 pt 上，然后再将 D_k 作用到所得的结果上，则得到的仍是 pt。

(3) 一个密文空间 CT，即所有可能密文 ct 的集合。将 PT 的元素用 E_k 加密后得到 CT 的元素，其中 k 遍历 K。

我们需要一些特别基本的语言概念。首先由一个非空有限集合 Σ 开始，这个集合称为**字符集**，而 Σ 的元素称为**字符**。Σ 的有限元素串称为**字**。同一个字符有可能在一个字中出现多次。由零个元素所构成的串也看作是一个字，即**空字** λ。一个字 w 的**长度**是该字中所含字符的个数，其中每个字符出现几次则数几次。我们用 Σ^* 来表示 Σ 上的所有字所组成的集合。Σ^* 的子集被称为 Σ 上的**(形式)语言**。

例如，如果 Σ 是英文字符集{A,B,C,…,Z}，则 ABBA,HORSE

和 KOKOOKOKOONKOKOKOKKO 都是 Σ 上的字(一个字是否有意义并没关系。事实上,第三个字在芬兰语中有意义)。我们也可以将小写字母和日常所需的标点符号及空格加到 Σ 上。如果将莎士比亚的著作连续写在一起,则我们得到这个扩展字符集上的一个字。

现在我们回到密码系统这个概念上来,并进一步分析它所包含的几个要素。明文空间 PT 通常是 Σ^* 或者由一个自然语言中所有有意义的句子所组成。值得强调的是,从多种角度来看,这两种可能性有根本区别。如果明文空间是 Σ^*,则消息中的每个字符都很重要。因而,在加密过程中没什么偏向。另一方面,每个自然语言的多余度都很高。即使改变一个消息中的许多单个字符,人们仍然能正确理解该消息。对窃听者而言,这是一个明显的有利条件,即使在密码分析过程中出了几个错,密码分析者有可能读懂该消息!让我们来进一步说明这一点。

例 1.1 首先假定明文空间由英语所组成。现考虑明文消息 WEMEETTOMORROW(我们去掉了单词之间的空格,以后将继续这样做)。该消息被加密成 UBQBBNNFIVPNFOOB(现在我们不谈所用的加密方法,这是一个令人吃惊的方法)。如果窃听者对密文分析的结果是 WIMIIDTUMAROV,这已经是一个不错的结果,应该是能正确读懂的。

其次,假定明文空间是 Σ^*,其中 $\Sigma=\{0,1\}$ 是二元字符集。进一步假定发送者和接收者关于消息做以下约定。这些消息的长度是 12,给出由 12 个船所组成的船队信息。更具体地来说,早上所发的消息表示哪一个船今天执行任务。例如,消息 010011000001 表示第二、五、六和十二号船在执行任务。这些消息加密后发送,窃听者的密码分析现在必须准确无误地恢复原文。即使一个比特之差也会造成行动上的大错。

当明文是英语时,人们常常先将它进行二元编码,例如,用每个字母在英文字符集中的位置数的二进制表示来代替该字母即可。因为 $2^4<26<2^5$,我们需要长度为 5 的字: