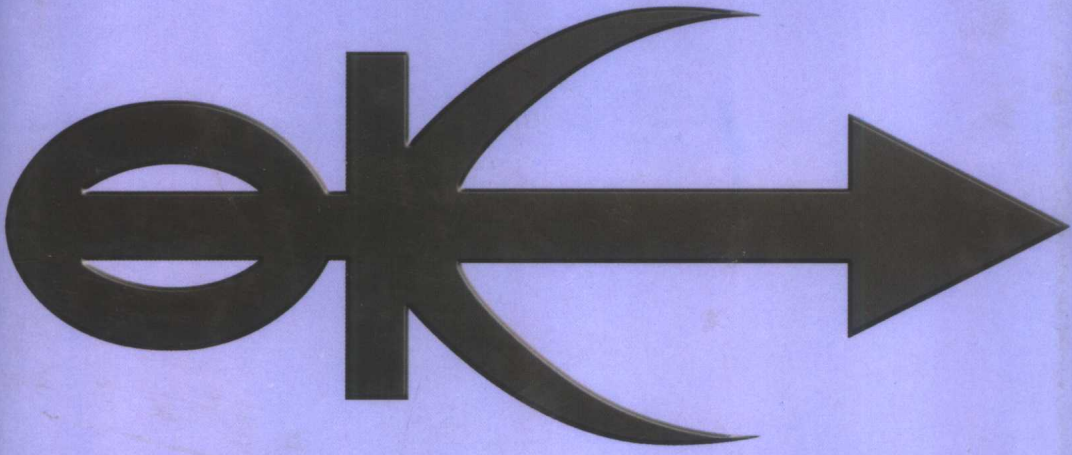
周玉洁 冯登国 编著

公开密钥密码算法及其快速实现

Public Key Cryptographic Algorithms and Its Fast Implementation



国防工业出版社

公开密钥密码算法及其快速实现

Public Key Cryptographic Algorithms and Its Fast Implementation

周玉洁　冯登国　编著

国防工业出版社

·北京·

图书在版编目(CIP)数据

公开密钥密码算法及其快速实现/周玉洁,冯登国编著. -北京:国防工业出版社,2002.9

ISBN 7-118-02749-9

Ⅰ.公… Ⅱ.①周…②冯… Ⅲ.密码-算法 Ⅳ.TN918.2

中国版本图书馆 CIP 数据核字(2001)第 097347 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)

北京奥隆印刷厂印刷

新华书店经售

*

开本 850×1168 1/32 印张 5⅛ 123 千字

2002 年 9 月第 1 版 2002 年 9 月北京第 1 次印刷

印数:1—3000 册 定价:16.00 元

致　读　者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分,又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展,加强社会主义物质文明和精神文明建设,培养优秀科技人才,确保国防科技优秀图书的出版,原国防科工委于1988年初决定每年拨出专款,设立国防科技图书出版基金,成立评审委员会,扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是:

1. 在国防科学技术领域中,学术水平高,内容有创见,在学科上居领先地位的基础科学理论图书;在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖,内容具体、实用,对国防科技和武器装备发展具有较大推动作用的专著;密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值,密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作,负责掌握出版基金的使用方向,评审受理的图书选题,决定资助的图书选题和资助金额,以及决定中断或取消资助等。经评审给予资助的图书,由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承

担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金

评审委员会

国防科技图书出版基金
第三届评审委员会组成人员

名誉主任委员	怀国模
主任委员	黄　宁
副主任委员	殷鹤龄　高景德　陈芳允　曾　铎
秘书长	崔士义
委员 （以姓氏笔画为序）	于景元　王小谟　尤子平　冯允成 刘　仁　朱森元　朵英贤　宋家树 杨星豪　吴有生　何庆芝　何国伟 何新贵　张立同　张汝果　张均武 张涵信　陈火旺　范学虹　柯有安 侯正明　莫梧生　崔尔杰

前　言

公开密钥密码(简称公钥密码,又称非对称公钥密码)是现代密码学中最重要的研究内容之一。密码学,其一般理解就是保护信息传递的机密性,但这仅仅是密码学研究的一个方面。对信息发送人的身份的认证以及信息的完整性的检验是密码学研究的另一个方面。公钥密码很好地解决了这两方面的问题,并正在产生许多新的思想和方案。与公钥密码相对应的是传统密码(又称对称密钥密码)。在传统密码中,用于加密的密钥与用于解密的密钥完全相同。因此,通常使用的加密算法比较简便、高效,密钥简短,安全性高。但是传送和保管密钥是一个严峻的问题。

公钥密码的观点是由 Diffie 和 Hellman 于 1976 年在他们的论文"密码学的新方向"一文中首次提出的,它使密码学发生了一场变革。Diffie 和 Hellman 为解决密钥管理问题,提出了一种密钥交换协议,允许在不安全的媒体上通信双方交换信息,安全地达成一致的密钥。在此新思想的基础上,很快出现了公钥密码。在公钥密码中,加密密钥不同于解密密钥,加密密钥公之于众,谁都可以使用。解密密钥只有解密人自己知道,分别称为公开密钥(简称公钥)和秘密密钥(简称私钥)。在至今为止的所有公钥密码中,最著名的是由 R.Rivest,A.Shamir 和 L.Adleman 三位教授于 1977 年提出的 RSA(RSA 的取名就是来自于这三位发明者的姓的第一个字母)。RSA 之所以具有安全性,是基于数论中的一个事实:将两个大的素数合成一个大数很容易,而相反过程则非常困难。由此可见,RSA 的安全性依赖于作为公钥的大数 n 的位数长度。

公钥密码与传统密码相比,有其不可取代的优势。然而它的运算量却十分浩大。因此,在网络上全都用公钥密码来传送机密

信息是没有必要的，也是不现实的。在传送机密信息的网络用户双方，最好的办法是使用某个传统密码（例如高级加密标准（AES））来加密需传递的机要信息，而同时使用 RSA 等公钥密码来传送 AES 的密钥。这样就可以综合发挥两种密码的优势，即 AES 高速、简便性和 RSA 密钥管理的方便、安全性。

公钥密码的思想与单向函数的概念密切相关。单向函数是这样一个函数，计算起来相对容易，但反过来，即求逆却很困难。也就是说，已知 x 计算函数 $f(x)$ 的值很容易，但已知 $f(x)$，却难于计算出 x。

把一只表拆开是单向函数很好的例子，把表拆成数百个碎片是很容易的事情，然而，要把这些碎片再拼成为功能完好的表，却是非常困难的。

上述单向函数不能用做加密，因为用这种单向函数加密的信息毫无用处，无人能解开它。对加密，我们需要一种所谓的单向陷门函数。

单向陷门函数是有一个秘密陷门的一类特殊单向函数。它的一个方向易于计算而反方向却难于计算。但是，如果你知道那个秘密陷门，就很容易反方向计算这个函数。也就是说，已知 x，易于计算 $f(x)$，已知 $f(x)$ 却难于计算 x。然而，有一些秘密信息 y，一旦给出 $f(x)$ 和 y，就很容易计算出 x。

邮箱是单向陷门函数的一个很好的例子。任何人都能容易地把邮件放进邮箱，只要打开口子投进去就行了。把邮件放进邮箱是一件公开的事情，但打开邮箱却不是，它是难的，你需要吹焊器或其他工具。然而，如果持有秘密信息（钥匙或组合密码），就很容易打开邮箱了。

公钥密码的原理就是基于单向陷门函数，加密是容易的方向，加密指令是公开密钥，任何人都能加密信息。而解密是难的方向，它设计得非常困难，以致于若没有秘密信息，使用最快的计算机用几百万年的时间都不能解开加密信息。秘密信息即陷门就是私钥。

假设 A 和 B 是通信的双方，E 是窃听者，以下是 A 使用公钥密码发送信息给 B 的过程。

(1)A 和 B 选用一个公钥密码系统。

(2)B 将他的公钥传送给 A。

(3)A 用 B 的公钥加密她的信息，然后传送给 B。

(4)B 用他的私钥解密 A 的信息。

可以看出公钥密码是通过密钥分配来解决传统密码的主要问题。对于传统密码，A 和 B 不得不选取同一密钥。A 可能随机选取一个，但她不得不把选取的密钥告诉 B。她可能事先交给 B，但那样做需要有先见之明。她也可能通过挂号信将它寄给 B，但那样做要花费时间。对公钥密码则没有这个问题，不用事先安排，A 就能把信息安全地发送给 B。在整个交换中一直在窃听的 E，虽有 B 的公钥和用公钥加密的信息，但却恢复不出 B 的私钥或者是传送的信息。

更一般地，网络中的用户约定公钥密码，每一用户有自己的公钥和私钥，并且在其他地方的数据库都是公开的，这样一来使用就更容易：

(1)A 从数据库中得到 B 的公钥；

(2)A 用 B 的公钥加密信息，然后传给 B；

(3)B 用自己的私钥解密 A 发送的信息。

自从 1976 年 Diffie 和 Hellman 提出公钥密码的观点之后，大量的公钥密码被陆续提出来，如 RSA 公钥密码、Merke-Hellman 背包公钥密码、McEliece 公钥密码、ElGamal 公钥密码和椭圆曲线(EC)公钥密码等，所有这些公钥密码的安全性都依赖于数学问题的难解性。

当寻找公钥密码所基于的数学问题时，密码学家需要寻找的是用最快算法所需要指数时间的问题。粗略地讲，计算一个问题的最快算法所需的时间越长，基于该问题的公钥密码越安全。20 多年来，许多曾经提出的公钥密码已经被攻破了(也即被证明是基于一个比原先所想像的要容易的问题)，也有很多被证明是不

实用的。迄今为止,比较流行的和被人们认可的公钥密码主要有两类:

(1)基于大整数因子分解问题,其中最典型的代表是 RSA 公钥密码;

(2)基于离散对数问题,比如 EIGamal 公钥密码和影响比较大的椭圆曲线公钥密码。

由于分解大整数的能力日益增强,对 RSA 公钥密码的安全带来了一定的威胁,512bit 模长的 RSA 公钥密码已经不安全,人们建议使用 1024bit 模长,要保证 20 年的安全就要选择 1280bit 模长,但是增大模长带来了实现上的难度。而基于离散对数问题的公钥密码在目前技术下有 512bit 模长就能够保证其安全性。特别是椭圆曲线上的离散对数的计算要比有限域上的离散对数的计算更困难,能设计出密钥更短的公钥密码,因而受到了国际上广泛的关注,RSA 公司等已经开发出符合 IEEE P1363 标准的椭圆曲线公钥密码。

西方一些国家目前正在倡导和实施建设公钥基础设施(PKI)的计划,他们认为,信息技术应使得政府的服务具有更多的可访问性,并且更容易使用,但需要保护系统和这些系统的信息处理的隐私和安全。电子商务、电子函件和其他应用是在政府内部、政府和私人之间以及政府和政府之间。这些应用中都有使用密码技术来提供完整性、不可否认性、保密性和认证服务的可能。使得这些普遍的安全服务成为可能的技术是公钥密码,将它组合在公钥基础设施中,使得在大范围内进行这些服务成为可能。可见,公钥密码的研究和使用将对解决现实生活中所遇到的安全问题起着极其重要的作用。

本书是根据作者多年的科研成果和教学实践,并结合国内外大量文献编著的。该书对现有的公钥密码做了全面系统的介绍,并对它们的安全性做了详尽分析,特别是给出了各种公钥密码的快速实现方法,依照本书的算法,可以方便、快速地实现所需的公钥密码。

本书反映了当今公钥密码的研究现状，并力图使之成为一本高起点的、实用的密码学专著。我们期望这本书对我国保密通信的实际应用工作者和应用理论研究工作者有所帮助。

全书共分5章。第1章介绍了公钥密码的数学基础，特别给出了域表示理论。第2章讨论了RSA的安全性及其典型攻击方法，给出了素性检测方法及因子分解算法，特别给出了快速模算术运算方法，进而给出了RSA的快速实现方法。第3章介绍了ElGamal公钥密码，该章还给出了离散对数算法。第4章介绍了椭圆曲线公钥密码，该章讨论了椭圆曲线离散对数问题，给出了计算椭圆曲线倍点的各种方法，进而给出了椭圆曲线公钥密码的快速实现方法。第5章介绍了背包算法和其他公钥密码算法。

作者对信息安全国家重点实验室的裴定一教授、戴宗铎教授在本书的编写过程中给予的支持深表感谢。感谢欧海文博士在文献资料上提供的帮助。感谢张玉峰硕士、董军武硕士在本书的编排中付出的努力。对解放军信息工程大学的吴益清高工、戚建平教授给予的帮助表示感谢。

本书中的部分研究内容得到了国家重点基础研究发展规划项目(项目编号为G1999035802)、国家杰出青年科学基金项目(项目编号为60025205)、国家"九五"密码发展基金项目、信息安全国家重点实验室开放基金项目的支持，在此表示感谢。

最后，我们在此特别感谢国防科技图书出版基金评审委员会以及国防工业出版社的专家教授，本书的出版与他们的大力支持是分不开的。

作　者

目　录

Contents