“十三五”国家重点出版物出版规划项目

高等教育网络空间安全规划教材

现代密码学

任伟 许瑞 宋军 编著

提供电子课件

http://www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

在线互动交流平台
官 方 微 博：http://weibo.com/cmpjsj
读者教师 QQ 群：158665100
教师服务微信：15910938545

现代密码学

内容简介

本书内容包括密码学概述、古典密码体制、信息理论安全、序列密码、分组密码、Hash 函数和消息鉴别、公钥加密（基础）、公钥加密（扩展）、数字签名、实体认证与身份识别、密码管理。本书的特色是注重介绍密码学方案设计的基本原理和内在规律，展现知识体系之间的内在逻辑性，大量采用类比和比较的方式探究方法论，力图使读者“知其所以然”。在给出方案的同时，解释方案的设计机理和思路，并专门设立“思考”环节，有意识地培养读者的创造性思维能力。

本书读者对象包括高等院校网络空间安全、信息安全、密码学、应用数学、计算机科学、信息与计算科学等专业本科高年级学生，对信息安全领域的研究人员也具有启发作用和参考价值。

为中华崛起传播智慧
封底无防伪标均为盗版
策划编辑◎郝建伟
封面设计◎ 子时文化 ZiShi Culture
机工教育微信服务号
获取更多相关资源及图书信息请关注
上架指导 计算机/信息安全
ISBN 978-7-111-64867-3
ISBN 978-7-111-64867-3
9 787111 648673 >
定价：55.00 元

“十三五”国家重点出版物出版规划项目
高等教育网络空间安全规划教材

现代密码学

任伟　许瑞　宋军　编著

机械工业出版社

本书内容包括密码学概述、古典密码体制、信息理论安全、序列密码、分组密码、Hash 函数和消息鉴别、公钥加密（基础）、公钥加密（扩展）、数字签名、实体认证与身份识别、密码管理。本书的特色是注重介绍密码学方案设计的基本原理和内在规律，展现知识体系之间的内在逻辑性，大量采用类比和比较的方式探究方法论，力图使读者“知其所以然”。在给出方案的同时，解释方案的设计机理和思路，并专门设立“思考”环节，有意识地培养读者的创造性思维能力。

本书读者对象包括高等院校网络空间安全、信息安全、密码学、应用数学、计算机科学、信息与计算科学等专业本科高年级学生。对信息安全领域的研究人员也具有启发作用和参考价值。

本书配有授课电子课件，需要的教师可登录 www.cmpedu.com 免费注册，审核通过后下载，或联系编辑索取。微信：15910938545。电话：010-88379739。

图书在版编目（CIP）数据

现代密码学/任伟，许瑞，宋军编著．—北京：机械工业出版社，2020.8
“十三五”国家重点出版物出版规划项目　高等教育网络空间安全规划教材
ISBN 978-7-111-64867-3

Ⅰ．①现…　Ⅱ．①任…　②许…　③宋…　Ⅲ．①密码-理论-高等学校-教材　Ⅳ．①TN918.1

中国版本图书馆 CIP 数据核字（2020）第 032970 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策划编辑：郝建伟　　责任编辑：郝建伟　陈崇昱　时　静
责任校对：张艳霞　　责任印制：常天培
北京捷迅佳彩印刷有限公司印刷

2020 年 9 月第 1 版 · 第 1 次印刷
184mm×260mm · 15.25 印张 · 376 千字
0001-1500 册
标准书号：ISBN 978-7-111-64867-3
定价：55.00 元

电话服务　　网络服务
客服电话：010-88361066　　机　工　官　网：www.cmpbook.com
　　010-88379833　　机　工　官　博：weibo.com/cmp1952
　　010-68326294　　金　　书　　网：www.golden-book.com
封底无防伪标均为盗版　　机工教育服务网：www.cmpedu.com

高等教育网络空间安全规划教材
编委会成员名单

前　言

目前市场上的密码学书籍依然有值得改进的地方，主要表现在虽然对密码方案过程的讲解较为细致，但是对方案的设计原理、设计原则等内在机制的讲解不够充分，导致读者学习了各种方案后，大多局限于对方案的代码实现和使用，没有深刻理解为什么要这样设计方案，特别是不知道密码学方案是如何想出来的，不知道其来龙去脉，没有理解方案设计中的内在逻辑性，因此，可认为没有“真正学懂”。同时，目前的相关书籍在思维的启发性、学生创造性能力培养方面仍然有待完善。本书力图在这些方面做出新的尝试，有意识地引导学生思考，培养他们的逻辑推理能力、发散性思维能力、知识的归纳能力，以及灵活运用所学知识的能力。

每章内容的组织是从整体全貌到局部细节，从一般模型到具体方案（先讲模型、分类，再介绍具体构造方案）。介绍具体内容时遵照学习规律，从易到难，从简单方案到改进方案，还原历史发展的原貌和变迁，突出来龙去脉（如在介绍公钥方案的提出时，首先介绍 Merkle 谜题，Pohlig-Hellman 对称密钥分组加密，Merkle-Hellman 背包公钥密码方案，然后才介绍 RSA 方案）。讲解内容时深入浅出，简洁直观，使用浅显的语言来表述深奥的内在规律。在介绍完多个具体方案后，再归纳一般规律，从具体方案中提炼出一般规律和原理（如从 ElGamal 签名、DSA 等到一般 ElGamal 签名，从基于身份识别协议到知识签名）。大部分方案都会给出实例进行直观的讲解。本书还大量采用类比法、比较法、归纳法、图示法，试图使读者对所学内容能够反复巩固、前后联系。写作本书时还特别遵循了以下思路：

1）注重启发性。目前大部分教材以罗列密码学方案为主，缺乏对设计原理的分析，以及对设计动机和逻辑性的解释。本书试图改变这一局面。

2）注重知识点的逻辑联系和类比。指出章节间和章节中前后各个分离的知识点间的联系和类比关系，明确给出各知识点间的关联，便于读者体会密码算法或协议设计的奥妙。

3）注重原理的总结和推广。在介绍完具体构造方案后，给出一般性构造方案，或者加以讨论和总结，给出提问思考，有利于知识的理解，起到举一反三的作用。

4）兼具广度和深度。基本原理和基本概念的讲解力求透彻、有深度。通过扩展阅读提高广度，便于读者回顾经典论文或者了解最新的国际国内发展动态。

全书共分 11 章：第 1 章为密码学概论；第 2 章介绍古典密码体制；第 3 章介绍信息理论安全；第 4 章介绍序列密码；第 5 章介绍分组密码；第 6 章介绍 Hash 函数和消息鉴别；第 7 章介绍公钥加密（基础）；第 8 章介绍公钥加密（扩展）；第 9 章介绍数字签名；第 10 章介绍实体认证与身份识别；第 11 章介绍密钥管理。

全书精心安排了示例。为帮助读者进一步对书中的内容进行拓展研究，本书还有针对性地提供了扩展阅读建议，用于开展课外学习和论文研读讨论。每章小结归纳了本章知识点，并指出重点和难点，便于复习。打 * 号的章节可选学。

本书第3章由许瑞编写，11.1节和11.4节由宋军编写，其余章节由任伟编写，全书由任伟负责统稿和定稿。

本书的出版得到了省级教学研究项目（2015146）和本科教学质量工程项目（2016039）的支持，在此表示感谢。同时感谢学生肖睿阳的辅助性工作。由于编者水平有限，在此衷心希望读者批评指正，可将意见和建议反馈至E-mail：weirencs@cug.edu.cn。

编　者

目　录

第1章　密码学概论

本章要点：

- 密码学解决的主要目标问题。
- 从密码学的发展简史体会密码学方案设计的演变。
- 对加密体制的攻击和安全性。

1.1　密码学的目标与知识构成

随着信息社会的发展，信息安全成为一个需要解决的关键问题。针对信息安全的攻击，主要包括主动攻击和被动攻击。

被动攻击主要是信息的截取（Interception），指未经授权窃听传输的信息，企图分析出消息内容或者是通信模式。

主动攻击主要包括：

（1）中断（Interruption），阻止通信设施的正常工作，破坏可用性。

（2）篡改（Modification），更改数据流。

（3）伪造（Fabrication），将一个非法实体伪装成一个合法的实体。

（4）重放（Replay），将一个数据单元截取后进行重传。

思考1.1：能否给出上述攻击的具体表现形式？ □

信息安全的目标是确保信息的安全性。安全目标通常包括：

（1）机密性（Confidentiality）。指保证信息不泄露给非授权的用户或者实体，确保保存的信息和被传输的信息仅能被授权的各方得到，而非授权用户即使得到信息也无法知晓信息的内容。通常通过访问控制机制阻止非授权用户的访问，通过加密机制阻止非授权用户知晓信息的内容。

（2）完整性（Integrity）。指消息未经授权不能进行篡改，要保证消息的一致性，即消息在生成、传输、存储和使用过程中不应发生人为（或无意）的非授权篡改（插入、修改、删除、重排序等）。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检测信息是否被篡改。

（3）认证性（Authentication）。指确保一个消息的来源或者消息本身被正确地标识，同时确保该标识没有被伪造，认证分为消息鉴别和实体认证。消息鉴别是指接收方保证消息确实来自于所声称的源；实体认证指能确保被认证实体是所声称的实体。

（4）不可否认性（Non-repudiation）。指能保证用户无法事后否认曾经对信息进行的生成、签发、接收等行为。当发送一个消息时，接收方能证实该消息确实是由既定的发送方发来的，称为源不可否认性；同样，当接收方收到一个消息时，发送方能够证实该消息确实已经送到了指定的接收方，称为宿不可否认性。一般通过数字签名来提供不可

否认服务。

（5）可用性（Availability）。指保障信息资源随时可提供服务的能力。即授权用户根据需要可以随时访问所需信息，保证合法用户对信息资源的使用不被非法拒绝。典型的对可用性的攻击是拒绝服务攻击。

思考 1.2：你能给出上述目标的具体例子吗？ □

除了以上一些主要目标外，还有隐私性（Privacy）、匿名性（Anonymity）等。

例 1.1 下面给出隐私性的几个例子。

移动互联网中的位置隐私（Location Privacy）：基于位置的服务（Location-based Service）通常需要用户的位置，而用户的位置通常又会泄露用户的隐私，因此，位置隐私需要保护。

大数据公开共享可能会导致用户数据的隐私泄露，因此大数据在公开的时候需要对数据进行处理，目前比较流行的做法是差分隐私方法。

比特币账本中的交易隐私：由于比特币账本是公开的，因此每一个人都可以查找账本和分析账本，于是有些交易可能会定位到某一个人，这个人的所有交易都能够被查找到，他的交易隐私也会因此被泄露。

思考 1.3：攻击和信息安全的目标是什么关系？

在实际中，我们通常先发现一种攻击，然后给出对该种攻击的防御措施。攻击可能针对多个信息安全的目标。每个信息安全的目标可能面临多种具体的攻击方式。将攻击方式的共同目标提炼和抽象出来，可以确定某些信息安全的目标。 □

为达到上述目标，信息安全采用了信息论、计算机科学和密码学等方面的知识，形成了一门综合学科，其主要任务是研究计算机系统和通信网络中信息的保护方法，以及实现系统和网络中信息的机密性、完整性、认证性、不可否认性、可用性等目标，其中密码学是实现信息安全目标的核心技术。

密码学（Cryptology）是研究实现信息安全各目标的相关的数学、方法和技术。密码学不是提供信息安全的唯一方式。其研究的目标是信息安全目标的一个子集，主要包括：机密性、完整性、认证性、不可否认性。（注意，这里没有包括可用性。）为实现上述目标，密码学集数学、计算机科学、电子与通信等诸多学科的方法于一体，是一门交叉学科。从大的方面可分为密码编码学和密码分析学两类，对应于密码方案的设计学科和密码方案的分析学科。

密码学在设计方案的时候，首先需要考虑方案所能达到的安全性。通常，衡量密码体制安全性的基本准则有以下几种：

（1）计算安全（Computational Security）：如果攻破一个密码体制所需要的计算能力和计算时间是现实条件所不具备的，就认为相应的密码体制满足计算安全。

（2）无条件安全（Unconditional Security）：如果假设攻击者在无限计算能力和计算时间的前提下，也无法攻破该体制，则认为相应的密码体制满足无条件安全。

（3）可证明安全（Provable Security）：如果攻破一个密码体制意味着可以解决某一个经过深入研究的数学难题，就认为相应的密码体制满足可证明安全。

思考 1.4：上述 3 个安全性基本准则之间的比较？

计算安全与计算能力和计算时间的假设有关，通常计算安全的安全程度是计算能力和计算时间的函数。例如，即使是当前世界 500 强的计算机也需要计算 100 年。

无条件安全不需要假设计算能力和计算时间。简言之，不定方程解在自变量定义范围内的取值是等可能的。多元线性方程组的个数（即线性方程组的秩）少于自变量的个数时，则线性方程组解在自变量定义范围内的取值是等可能的。即使对非经典的计算机，如量子计算机、DNA 计算机而言，也是安全的（即无法确定自变量的取值）。

可证明安全强调安全的规约，即安全性的缺失将导致某个数学难题的解决，换句话说，因为数学难题被广泛认为是不能解决的，因此安全性是可以保证的。 □

通常现代密码学强调达到可证明安全，这通常是计算安全的。即安全具有一定的等级，这种等级通常通过攻破方案所需要的工作量来衡量。一种衡量安全等级的常见参数就是密钥的长度。

除了安全性外，设计密码方案时还需要考虑如下因素：

（1）功能性。方案能够满足安全需求即可，要避免过于满足安全需求且性能代价过高的方案。也可以理解为“杀鸡不要用牛刀”。

（2）性能。方案的计算、存储、传输等各方面的效率。例如，嵌入式系统、手机系统、智能卡系统等在计算和存储能力上有限，设计安全方案时需要考虑到。

（3）容易实现性。在实际中实施方案的难易程度。包括在软件和硬件环境中实现密码要素的复杂度。

上述方面往往在实际应用中需要权衡，如在一个计算能力有限的环境中，为了使系统在整体上具有良好的性能，可能不得不割舍高级别的安全性。

围绕着密码学要达到的目标，可以将密码学的实现方案分类成各种工具。图 1.1 给出了密码学内容的构成，图 1.2 围绕着安全目标给出了各内容间的联系。

图 1.1 密码学的内容构成

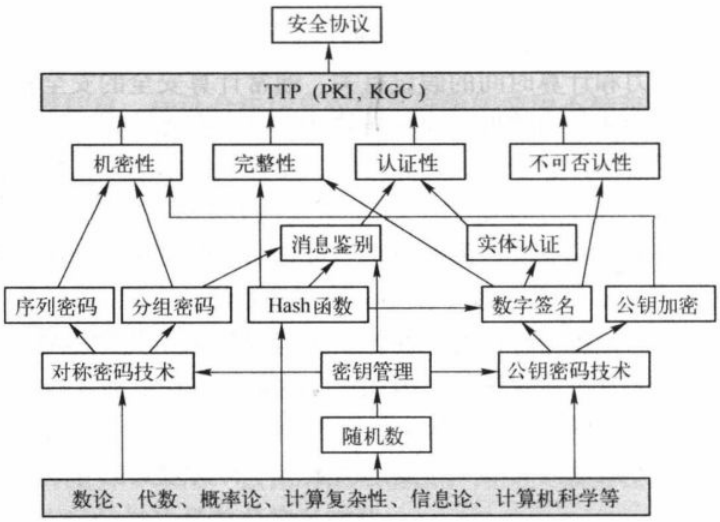

图 1.2　密码学研究内容间的关系

1.2　密码学的发展简史

从整体上来说，密码学经过了古典密码时期（人工密码）、近代密码时期（机械密码）、现代密码时期（电子计算机）这三个发展历程。下面按年代顺序列出密码学发展中的重要事件。

1.2.1　古典密码时期

（1）公元前 1900 年左右，一位佚名的埃及书吏在碑文中使用了非标准的象形文字，这或许是目前已知最早的密码术实例。

（2）公元前 400 多年，古希腊斯巴达军队中使用的 Scytale 密码，是一种置换密码。

（3）公元前 1 世纪，古罗马帝国皇帝凯撒（Caesar）曾经使用有序的单表代换密码，即 Caesar 密码，是单表代换密码的代表。

（4）我国宋代曾公亮、丁度等编撰的《武经总要·字验》中记载，北宋前期，在作战中曾用一首五言律诗的 40 个汉字，分别代表 40 种情况或要求，这种方式已具备了密码本的特点。

（5）欧洲的密码学起源于中世纪。约在 1379 年，欧洲第一本关于密码学的手册由生活在意大利北部城市帕尔玛的 Gabriela de Lavinde 写成，它由几个加密算法组成，且为罗马教皇克莱门特七世服务。

（6）阿拉伯人是第一个清晰地理解密码学原理的人，他们设计并使用代换和换位加密，并且发现了密码分析中的字母频率分布关系。大约在 1412 年，波斯人 al-Qalqashandi 所编的百科全书的第 14 卷中记载了破译简单代换密码的方法。这是密码分析法最早的著作之一。

（7）大约在 1467 年左右，意大利佛罗伦萨的建筑师 Alberti 发明了多字母表替代密码，他设计了一个密码盘，该盘有一个大一些的外轮和一个小一些的内轮，并各自以明文字符和密文字符作为索引。字母的排列确定了一个简单替代，并且可在加密一些字符之后通过转动

盘来修改替代方式。

（8）1508 年，密码学的第一本印刷书籍 Polygraphic 由德国的僧侣 Trithemius 写成，并在 1518 年出版，其中包含了第一个基于 24 个字符的方形表，该表列出了明文字母表字符在一个固定次序下的所有移位替代。

（9）17 世纪，英国著名的哲学家弗朗西斯·培根在他所著的《学问的发展》一书中最早给密码下了定义，他说："所谓密码应具备三个条件，即易于翻译、第三者无法理解、在一定场合下不易引人注意。"

（10）1854 年，Playfair 密码（Playfair Cipher）由 C. Wheatstone 提出，此后由他的朋友 L. Playfair 将该密码公布，所以就称为 Playfair 密码。

（11）1858 年，维吉尼亚密码（Vigenere Cipher）由法国密码学家 B. D. Vigenere 提出。

（12）1860 年，密码系统在外交通信中已得到普遍使用。如在美国南北战争中，联邦军广泛地使用换位加密，主要是使用 Vigenere 密码。

（13）1863 年，Kasiki 测试法于由普鲁士军官 F. Kasiski 提出，用于分析多表代换的周期。

（14）1871 年，上海大北水线电报公司选用 6899 个汉字，代以 4 码数字，成为中国最初的商用明码本，同时也设计了由明码本改编成密码本并进行混淆的方法。

（15）1883 年，A. Kerckhoffs 在《军事密码学》一书中提出了密码系统的安全性的一个基本假设，称为 Kerckhoffs 假设（原则），即密码分析者知道所使用的密码算法。

（16）1917 年，Vernam 密码由美国 AT&T 公司的 G. Vernam 提出，它是为电报通信设计的非常简单方便的密码，奠定了序列密码的基础。

（17）1918 年，W. F. Friedman 的论文《重合指数及其在密码学中的应用》（The Index of Coincidence and Its Applications in Cryptography），给出了多表代换密码的破译方法，它是 1949 年之前最重要的密码文献。

（18）1929 年，Hill 密码（Hill Cipher）由数学家 L. Hill 提出。

古典密码时期的密码技术仅是一门文字变换艺术，其研究和应用远没有形成一门科学，最多只能称其为密码术。

1.2.2 近代密码时期

（1）20 世纪 20 年代，随着机械和机电技术的成熟，以及电报和无线电需求的出现，引起了密码设备方面的一场革命——发明了转轮密码机（Rotor），转轮机的出现是密码学发展的重要标志之一，从此出现了商业密码机的公司和市场。

（2）从 1921 年开始的接下来的十多年里，美国加州奥克兰的一个名叫 Edward Hebern 的工程师构造了一系列改进的转轮机，并投入美国海军的试用评估，他申请了第一台转轮机的专利，这种装置在差不多 50 年内一直被指定为美军的主要密码设备，奠定了第二次世界大战中美国在密码学方面的超级地位。

（3）在美国的 Herbern 发明转轮密码机的同时，欧洲的工程师们如荷兰的 Hugo Koch、德国的 Arthur Scherbius 都独立地提出了转轮机的概念。德国的 Arthur Scherbius 于 1919 年设计出了历史上著名的密码机——ENIGMA 机（意思是"谜"）。1930 年，日本的第一台转轮密码机（美国分析家称之为 RED）开始为外交部门服务。1939 年，日本人引入了一台新的

加密机（美国分析家称之为 PURPLE），其中的转轮机用电话步进交换机取代。

（4）第二次世界大战是人工加密时代转变为机械加密时代的转折点。转轮密码机的大量使用极大地提高了加解密的速度，同时抗攻击性能也有很大的提高，是密码学发展史上的一座里程碑。同时，密码分析最伟大的成功发生在第二次世界大战期间，波兰人和英国人破译了 ENIGMA 密码，美国人攻破了日本的 RED、ORANGE 和 PURPLE 密码，对盟军在第二次世界大战中获胜起到了重要作用。

近代密码时期可以看作是科学密码学的前夜，这个阶段的密码技术可以说是一种艺术，也是一种技巧和经验的综合体，但还不是一种科学，密码专家常常是凭直觉和信念来进行密码设计和分析，而不是推理和证明。因此，也有学者将古典、近代密码时期划分为一个阶段。

1.2.3 现代密码时期

（1）1949 年，Shannon（香农）在 *Bell Systems Technical Journal* 上发表了《保密系统的通信理论》（*Communication Theory of Secrecy Systems*）一文，用概率和统计等科学工具研究加密系统，为密码学奠定了坚实的理论基础，从此密码学从艺术变为科学。

（2）1967 年，Kahn 出版了《破译者》（*The Codebreakers*）一书，对密码学的历史进行了相当完整的记述，使成千上万原本不知道密码学的人了解了密码学。从此，密码学研究引起了民间的兴趣。Kahn 认为是阿拉伯人创造了“加密法（cipher）”一词。

（3）1973 年，美国国家标准局（NBS，现在是美国国家标准技术研究所 NIST）在全世界范围征求国际密码标准方案（DES）。4 年后，发布正式的标准 DES。该方案的公布极大地促进了密码学在民间的研究。

（4）1976 年，W. Diffie 和 M. Hellman 在《密码学的新方向》一文中提出公钥密码体制。这是密码学发展史上最伟大的一次革命，也是现代密码学诞生的标志。

（5）1978 年，Merkle 和 Hellman 提出了第一个公钥密码系统——背包（knapsack）公钥密码系统，安全性基于背包问题（一种 NP 完全问题）。

（6）1978 年，美国麻省理工学院（MIT）的 Rivest、Shamir 和 Adleman 提出 RSA 加密机制，这是第一个实用的公钥方案，开创了密码学的新纪元。

（7）1979 年，MIT 的 M. O. Rabin 提出第一个可证明安全的公钥密码体制。

（8）1979 年，L. Lamport 提出基于任意单向函数的一次签名方案。

（9）1984 年，S. Goldwasser 与 S. Micali 提出了概率公钥密码系统的概念，并提出 Goldwasser-Micali 概率公钥密码系统。

（10）1984 年，IBM 公司的 Benett 和 Montreal 大学的 Brassard 提出第一个量子密码学方案，称为 BB84 协议。它是以量子力学基本理论为基础的量子信息理论领域的第一个应用，并提出了一个量子密钥交换的安全协议，由此迎来了量子密码学的新时期。

（11）1985 年，ElGamal 密码体制由 T. ElGamal 提出，该密码体制基于的困难问题是群中的离散对数问题。

（12）1985 年，T. ElGamal 提出一个基于离散对数问题的数字签名体制，称为 ElGamal 数字签名体制。

（13）1985 年，N. Koblitz 和 V. Miller 提出了椭圆曲线密码系统（Elliptic Curve Cryptog-

raphy，ECC），实现了公钥密码体制在效率上的重大突破。

（14）1987 年，R. Rivest 提出面向软件实现的序列密码 RC4，RC4 是目前公开范围内应用最广泛的序列密码。

（15）1988 年，Matsumoto 和 Imai 提出多变量公钥密码体制，这是第一个使用“小域——大域”的思想来构造域的方法，也是多变量公钥密码体制发展史上的里程碑，还是第一个实用的多变量公钥密码体制。

（16）1989 年，Robert A. J. Matthews 首次将混沌理论用于密码学研究，并提出一种基于变形 Logistic 映射的混沌序列密码方案。从此，混沌密码学作为密码学的一个分支引起了广泛的关注。

（17）1989 年，世界上第一台量子密钥分配原型样机研制成功，它的工作距离仅为 32cm，然而，它却标志着量子密码开始初步走向实用。

（18）1994 年，Peter Shor 发现了一种在量子计算机上多项式时间内运行的大整数因子分解算法，这意味着一旦人们能研制出量子计算机，则 RSA 密码体制将不再安全。

（19）1994 年，Adleman 利用 DNA 计算机解决了一个有向 Hamilton 路径问题，标志着信息时代进入了一个新的阶段。

（20）1996 年，Bellare 等人基于嵌套 MAC 提出 HMAC，并证明了其安全性。

（21）1996 年，在 Crypto 会议上，布朗大学的 Hoffstein、Pipher、Silverman 三位数学家提出了 NTRU（Number Theory Research Unit）公开密钥算法，它是一种基于格的快速公开密钥体制。

（22）1997 年，NIST 发起公开征集高级加密标准（Advanced Encryption Standard，AES）算法的活动。

（23）2000 年 10 月，美国政府在多次评审后宣布，比利时人发明的 Rijndael 算法为最终的 AES 算法。

（24）2001 年 1 月，欧洲委员会在信息社会技术（Information Society Technology，IST）规划中投入巨资，支持一项称为 NESSIE（New European Schemes for Signature，Integrity，and Encryption）的工程，希望通过公开征集和进行公开、透明的测试评估，推出一套安全性高、软硬件实现性能好、能适应不同应用环境的密码算法。该工程于 2003 年 2 月完成，极大地推动了密码学的研究。

（25）2004 年 2 月，欧洲委员会的 IST 基金支持了一个为期 4 年的项目，ECRYPT（European Network of Excellence for Cryptology），目标是促进欧洲信息安全研究人员在密码学和数字水印研究上的交流。2008 年该项目完成评审。

（26）2006 年，国家密码管理局公布了《无线局域网产品使用的 SMS4 密码算法》，该算法是我国自有知识产权的国际无线网络安全标准 WAPI 的一部分。这是我国第一次公布自己的商用密码算法。

（27）密码货币比特币（Bitcoin）的概念最初由中本聪在 2008 年 11 月 1 日提出，并于 2009 年 1 月 3 日正式诞生，从此出现了一门新的分支——密码经济学。

（28）2010 年 2 月，Kleinjung 等在 IACR 的 ePrint 预印版论文服务器上（2010/006）发表了论文 *Factorization of a 768-bit RSA modulus*，这是迄今分解的最大 RSA 模。

（29）2012 年 3 月 21 日，国家密码管理局公布了 6 项密码行业标准，包括：GM/T