

《计算机密码学资料24本（英文）》(Cryptography)[光盘镜像]



极客

2009-5-3 20:44

3492



下载地址：<http://www.verycd.com/topics/2744748/>

资源简介:

=====

中文名: 计算机密码学资料26本（英文）

英文名: Cryptography

别名: Cryptography

资源格式: 光盘镜像

发行时间: 2008年

地区: 美国

对白语言: 英语

文字语言: 英文

现代密码学

第二次世界大战后计算机与电子学的发展促成了更复杂的密码，而且计算机可以加密任何二进制形式的资料，不再限于书写的文字，以语言学为基础的破密术因此失效。多数计算机加密的特色是在二进制字串上操作，而不像经典密码学那样直接地作用在传统字母数字上。然而，计算机同时也促进了破密分析的发展，抵消了某些加密法的优势。不过，优良的加密法仍保持领先，通常好的加密法都相当有效率（快速且使用少量资源），而破解它需要许多级数以上的资源，使得破密变得不可行。

虽然频率分析是很有效的技巧，实际上加密法通常还是有用的。不使用频率分析来破解一个信息需要知道目前是使用何种加密法，因此才会促成了谍报、贿赂、窃盗或背叛等行为。直到十九世纪学者们才体认到加密法的算法并非理智或实在的防护。实际上，适当的密码学机制（包含加解密法）应该保持安全，即使敌人知道了使用何种算法。对好的加密法来说，钥匙的秘密性理应足以保障资料的机密性。这个原则首先由奥古斯特·柯克霍夫（Auguste Kerckhoffs）提出并被称为柯克霍夫原则（Kerckhoffs' principle）。信息论始祖克劳德·艾尔伍德·香农（Claude Shannon）重述：“敌人知道系统。”

大量的公开学术研究出现，是现代的事，这起源于一九七零年代中期，美国国家标准局（National Bureau of Standards, NBS；现称国家标准技术研究所，National Institute of Standards and Technology, NIST）制定数字加密标准（DES），Diffie和Hellman提出的开创性论文，以及公开释出RSA。从那个时期开始，密码学成为通讯、电脑网络、电脑安全等上的重要工具。许多现代的密码技术的基础依赖于特定基算问题的困难度，例如因子分解问题或是离散对数问题。许多密码技术可被证明为只要特定的计算问题无法被有效的解出，那就安全。除了一个著名的例外：一次垫（one-time pad, OTP），这类证明是偶然的而非决定性的，但是是目前可用的最好的方式。

密码学算法与系统设计者不但要留意密码学历史，而且必须考虑到未来发展。例如，持续增加计算机处理速度会增进暴力攻击法（brute-force attacks）的速度。量子计算的潜在效应已经是部份密码学家的焦点。

二十世纪早期的密码学本质上主要考虑语言学上的模式。从此之后重心转移，现在密码学使用大量的数学，包括信息论、计算复杂性理论、统计学、组合学、抽象代数以及数论。密码学同时也是工程学的分支，但却是与别不同，因为它必须面对有智能且恶意的对手，大部分其他的工程仅需处理无恶意的自然力量。检视密码学问题与量子物理间的关连也是目前热门的研究。

本镜像包括:

- 1.A Classical Introduction to Cryptography Exercise Book.pdf 《经典密码学概论练习本》
- 2.Advances in Elliptic Curve Cryptography.pdf 《高级椭圆曲线密码学》
- 3.Applied Cryptanalysis - Breaking Ciphers in the Real World.pdf 《应用密码分析学》
- 4.Applied Cryptography - Protocols, Algorithms, & Source COde in C, 2nd Ed..chm 《应用密码学》
- 5.Applied Cryptography & Network Security - 2nd International Conference, ACNS 2004.pdf 《应用密码学和网络安全》
- 6.Beginning Cryptography with Java.chm 《Java密码学初步》
- 7.BigNum Math - Implementing Cryptographic Multiple Precision Arithmetic.pdf 《BigNum 数学-实施加密多精度算术》
- 8.Codes - The Guide to Secrecy from Ancient to Modern Times.pdf 《代码-古今保密指南》
- 9.Computer Security & Cryptography.pdf 《电脑安全与密码学》
- 10.Contemporary Cryptography.pdf 《现代密码学》
- 11.Cryptography - A Very Short Introduction.chm 《密码学简介》
- 12.Cryptography & Network Security, 4th Ed..chm 《密码学与网络安全》
- 13.Cryptography & Security Services - Mechanisms & Applications.pdf 《加密与安全服务-机制及应用》
- 14.Cryptography for Developers.pdf 《加密技术的开发》
- 15.Cryptography for Dummies.chm 《密码学傻瓜书》
- 16.Cryptography in C & C++.chm 《C & C++里的密码学》
- 17.Cryptography-Theory_and_practice_3ed.djvu 《密码学—理论与实践》
- 18.Cryptology Unlocked.pdf 《密码解锁》
- 19.Decrypted Secrets - Methods & Maxims of Cryptology, 4th, Revised & Extended Ed..pdf 《解密秘密》
- 20.Encyclopedia of Cryptology.chm 《密码学百科全书》
- 21FOUNDATIONS OF Cryptography - A Primer.pdf 《密码学基础》
- 22FOUNDATIONS OF Cryptography - Vol. 1, Basic Tools.pdf 《密码学基础》
- 23.Fundamentals of Cryptology - A Professional Reference & Interactive Tutorial.pdf 《密码学基础》
- 24.Modern Cryptography - Theory & Practice.pdf 《现代密码学—理论与实践》
- 25.The_CodeBreakers.pdf 《破译者》
- 26.Theory of Cryptography.pdf 《密码学原理》

CTF训练营-Web篇



收藏 · 3



点赞



打赏



分享

最新回复 (9)



极客

kmlch

2009-5-4 09:41

2楼 0

谢谢分享。我能看完一本就不错了。



极客

hjmyx

2009-5-4 10:08

3楼 0

很专业啊,先收藏了,以后会用到的!!!



极客

weinuan

2009-5-4 11:56

4楼 0

太多了！看不完了！

最新回复 (9)



[孤舟蓑笠](#)

2009-5-4 14:49

[5 楼](#) 0

英文的有点复杂。

极客



[kinglord](#)

2009-5-20 19:44

[6 楼](#) 0

要是 有翻译版的就好了

极客



[jingru](#)

2009-5-21 01:06

[7 楼](#) 0

强。收藏。。

极客



[fangawxs](#)

2 2009-5-22 20:38

[8 楼](#) 0

这个不错，谢谢楼主分享

大侠



[wentaoy](#)

2009-5-23 10:46

[9 楼](#) 0

看起来不错，顶一个

极客



[decolor](#)

2009-5-24 10:57

[10 楼](#) 0

英文看起来太费劲了，中文密码学都不好学~~~

极客



游客

[登录](#) | [注册](#) 方可回帖

回帖

表情

[高级回复](#)

返回