《应用密码学：协议、算法与C源程序（浴

图书基本信息

书名：《应用密码学：协议、算法与C源程序（原书第2版）》

13位ISBN编号：9787111445333

10位ISBN编号：7111445333

出版时间：2014-1

出版社：机械工业出版社

作者：（美）Bruce Schneier

译者：吴世忠,祝世雄,张文政 等

《应用密码学：协议、算法与C源程序（浴

内容概要

.....我所读过的关于密码学最好的书.....该书是美国国家安全局最不愿意见到出版的书.....
——《Wired》
.....不朽的.....令人着迷的.....计算机程序员必读的密码学上决定性的著作.....
——《Dr.Dobb's Journal》
.....该领域勿庸置疑的一本权威之作。
——《PC Magazine》
.....编码高手的圣经。
—— The Millennium Whole Earth Catalog
密码学的应用领域远远不只是编码和解码信息，要了解有关密码学技术的数字签名的知识，本书是必读之作。本书介绍了密码学协议的通用类型、特定技术，详细介绍了现实世界密码学算法的内部机制，包括DES和RSA公开密钥加密系统。书中提供了源代码列表和大量密码学应用方面的实践活动，如产 生真正的随机数和保持密钥安全的重要性。
全书共分四个部分，定义了密码学的多个术语，介绍了密码学的发展及背景，描述了密码学从简单到复杂的各种协议，详细讨论了密码技术。并在此基础上列举了如DES、IDEA、RSA、DSA等十多个算法以及多个应用实例，并提供了算法的源代码清单。
全书内容广博权威，具有极大的实用价值，是致力于密码学研究的专业及非专业人员一本难得的好书。

《应用密码学：协议、算法与C源程序（浴

作者简介

Bruce Schneier　是国际知名的安全技术专家，被《经济学家》（The Economist）杂志称为“安全大师”（security guru）。他是12本安全方面技术图书的作者，还是数百篇文章、杂文和学术论文的作者。他的有影响力的通讯“Crypto-Gram”和博客“Schneier on Security”有超过25万的读者和浏览者。他曾在国会作证，还经常做客电视台和广播电台，并在几个政府委员会供职。他是哈佛大学法学院伯克曼互联网和社会中心的fellow, 新美国基金会开放科技中心的program fellow, 电子前哨基金会的董事会成员，电子隐私信息中心的咨询委员会成员，以及BT（原英国电信）的安全未来学家。

《应用密码学：协议、算法与C源程序（浴

书籍目录

《应用密码学：协议、算法与C源程序（浴

精彩短评

1、密码学领域经典，讲的很详细，虽然很多地方看不懂，但还是能感觉到作者写这本书的时候很用心，非常值得多读几遍，哈哈哈！
2、虐成狗。硬着头皮前后大概用了4个月左右读完。后面算法实现，数论一下子不熟且跪。等功力高一点再来精读
3、我感觉这本书全而可读性差，如果当做入门书籍的话，比较晦涩，一些细节需要自己看
4、讲了很多密码算法与思想，后续不知有没有机会再看一遍。
5、不确定看过的是不是这本，先标记一下。详细说明了密码学的各种使用场景，这个对入门是最重要的。
6、密码学领域必看书籍

精彩书评

1、内容旧了，脱离当前的密码学实用现状，对椭圆曲线ECC一笔带过，对AES完全没有涉及，GCM模式也没有，AEAD也没有，OTR也没有。基本上是上个世纪的密码学历史故事集。翻译自：http://blog.cryptographyengineering.com/2011/11/in-defense-of-applied-cryptography.html"此书误导了一些读者，让一些读者误以为自己已经能够专业地实现密码学算法了，导致他们的商业产品充满了可怕，滑稽，破损的密码学算法。例如一个 Diebold voting machine, circa 2003，其中的码农可悲地用了lcg作为PRNG""Unfortunately, some readers, abetted by Bruce's detailed explanations and convenient source code examples, felt that they were now ready to implement crypto professionally. Inevitably their code made its way into commercial products, which shipped full of horribly ridiculous, broken crypto implementations. This is the part that was not so good. We're probably still dealing with the blowback today.Just for one modest example, take this fragment of code spotted in a Diebold voting machine, circa 2003:// LCG - Linear Conguential Generator - used to generate ballot serial numbers // A psuedo-random-sequence generator // (per Applied Cryptography, by Bruce Schneier, Wiley, 1996) #define LCG_MULTIPLIER 1366 #define LCG_INCREMENTOR 150889 ...Thanks to Applied Cryptography, the Diebold coders were able to write a perfectly functional Linear Congruential Generator in no time at all. You certainly can't blame Bruce for anything here -- the LCG code is fine. It's certainly not his fault that Diebold missed the part where he warned never to use LCGs for security applications. Whoops!Although it's all said with love, some people really do blame Applied Cryptography for this sort of thing. Even Bruce has at various points himself apologized for this aspect of the book.(Not coincidentally, you'll notice that his more recent books are nowhere near as brazenly useful as AC. Where Practical Cryptography is all crapped up with grave warnings about the dangers of rolling your own crypto implementations, Applied Cryptography just laid it all out there sans apology, like a copy of the Anarchist Cookbook left open in a middle school library.)""What's magical about Applied Cryptography is really two things. First of all, it's an incredible historical document. If there's a cipher that was used in the period 1970-1996, you'll read about it in Applied Cryptography. Even if the cipher was based on the cryptographic equivalent of an abacus, even if it was broken in the same conference in which it was published, Bruce will still give you a full design description and the address of the guy who owns the patent."

《应用密码学：协议、算法与C源程序（浴

版权说明