<<密码协议>>

图书基本信息

书名：<<密码协议>>

13位ISBN编号：9787040313314

10位ISBN编号：7040313316

出版时间：2011-10

出版时间：高等教育出版社

作者：董玲，陈克非 著

页数：373

<<密码协议>>

内容概要

《密码协议：基于可信任新鲜性的安全性分析（英文版）》主要介绍如何利用系统工程思想和可信任新鲜性的方法，分析和设计密码通信协议。
作者基于可信任的新鲜性标识符概念，提出了一个新颖的新鲜性原则。
该原则指出了一种有效的、易用的密码协议安全性分析方法。
使用这种分析方法，可以有效检验协议在实际应用中能否满足安全需要。
此外，书中给出大量的分析实0例，详细说明如何基于概率定义安全性，如何将安全指标定量化，如何针对具体的协议寻找漏洞，如何自动实现协议漏洞的查找，等等。
《密码协议：基于可信任新鲜性的安全性分析（英文版）》总结了作者近年来的研究成果，这些成果的有效性和易用性对从事通信协议安全性研究的人员，特别是工程技术人员，具有很好的参考和实用价值。
董玲网络系统建设和信息安全领域高级工程师，上海交通大学密码与信息安全实验室兼职教授、研究兴趣是信息安全和应用密码学，特别是实际应用的密码通信协议和密码系统的安全性分析。
陈克非上海交通大学计算机科学与工程系教授，长期从事密码与信息安全理论研究。
主要研究兴趣是序列密码、可证明安全、密码协议分析、数据安全。
近年来承担多项国家自然科学基金、国家高技术研究发展计划（863计划），发表学术论文150多篇，编辑出版学术著作7部。

<<密码协议>>

书籍目录

<<密码协议>>

章节摘录

Over the ages，information was typically stored and transmitted on paper，whereas much of it now resides on magnetic media and iS transmitted via computer networks.As we all know.it iS much easier to copy and alterinformation stored and transmitted electronically than that on paper.Infor-mation security intends to provide security services for information in digitalform · Information security objectives include confidentiality，data integrity，authentication，non-repudiation，access control，availability，fairness and SO on · Computer and network security research and development foCUS on thefirst four general security services，from which other security services，such as access control，and fairness can be derived[卜弓|.Many terms and COnceptsin this book are from Ref_[1]which is well addressed.For strict 0r inquisitive readers，please refer to book 11 for detailed information.一Confidentiality is a service used to keep the content of information from aU but those authorized to have it.That is，the information in a computer systern or transmitted information cannot be comprehended by unau- thorized parties · Secrecy IS a term synonymous with confidentiality and privacy. ……

<<密码协议>>

版权说明