《Applied Cryptography, Second Edition: Protocols, Algorithms And Source Code In C 9780471117094》

书籍信息

版 次：1
页 数：758
字 数：
印刷时间：1995年10月01日
开 本：大32开
纸 张：胶版纸
包 装：平装
是否套装：否
国际标准书号ISBN：9780471117094

内容简介

"...the best introduction to cryptography I ′ ve ever seen. ... The book the National Security Agency wanted never to bepublished. . . ." – Wired Magazine". . .monumental . . . fascinating. . . comprehensive . . . the definitive work on cryptography forcomputer programmers . . ." – Dr. Dobb ′ s Journal". . .easily ranksas one of the most authoritative in its field." – PC Magazine". ..the bible of code hackers." – The Millennium Whole EarthCatalogThis new edition of the cryptography classic provides youwith a comprehensive survey of modern cryptography. The bookdetails how programmers and electronic communications professionalscan use cryptography – the technique of enciphering and decipheringmessages – to maintain the privacy of computer data. It describesdozens of cryptography algorithms, gives practical advice on how toimplement them into cryptographic software, and shows how they canbe used to solve security problems. Covering the latestdevelopments in practical cryptographic techniques, this newedition shows programmers who design computer applications,networks, and storage systems how they can build security intotheir software and systems.What ′ s new in the Second Edition?? Newinformation on the Clipper Chip, including ways to defeat the keyescrow mechanism? New encryption algorithms, including algorithmsfrom the former Soviet Union and South Africa, and the RC4 streamcipher? The latest protocols for digital signatures,authentication, secure elections, digital cash, and more? Moredetailed information on key management and cryptographicimplementations

显示全部信息

作者简介

BRUCE SCHNEIER is President of Counter-pane Systems, a consulting firm s pecializing in cryptography and computer security. He is a contributing editor to Dr. Dobb's Journal, serves on the board of directors of the Internatio nal Association of Cryptologic Research, and is a member of the Advisory Board for the Electronic Privacy Information Center. He is the author of E -Mail Security (Wiley) and is a frequent lecturer on cryptography, computer security, and privacy.

目录

Partial table of contents:

CRYPTOGRAPHIC PROTOCOLS.
Protocol Building Blocks.
Basic Protocols.
Intermediate Protocols.
Advanced Protocols.
Esoteric Protocols.
CRYPTOGRAPHIC TECHNIQUES.
Key Length.
Key Management.
Algorithm Types and Modes.
Using Algorithms.
CRYPTOGRAPHIC ALGORITHMS.
Data Encryption Standard (DES).

显示全部信息

媒体评论

"Overall, I enjoyed this book and its contribution to the field of transplantation. Many clinicians would find this helpful in their daily practice." (Doody ′ s, 16 December 2011)