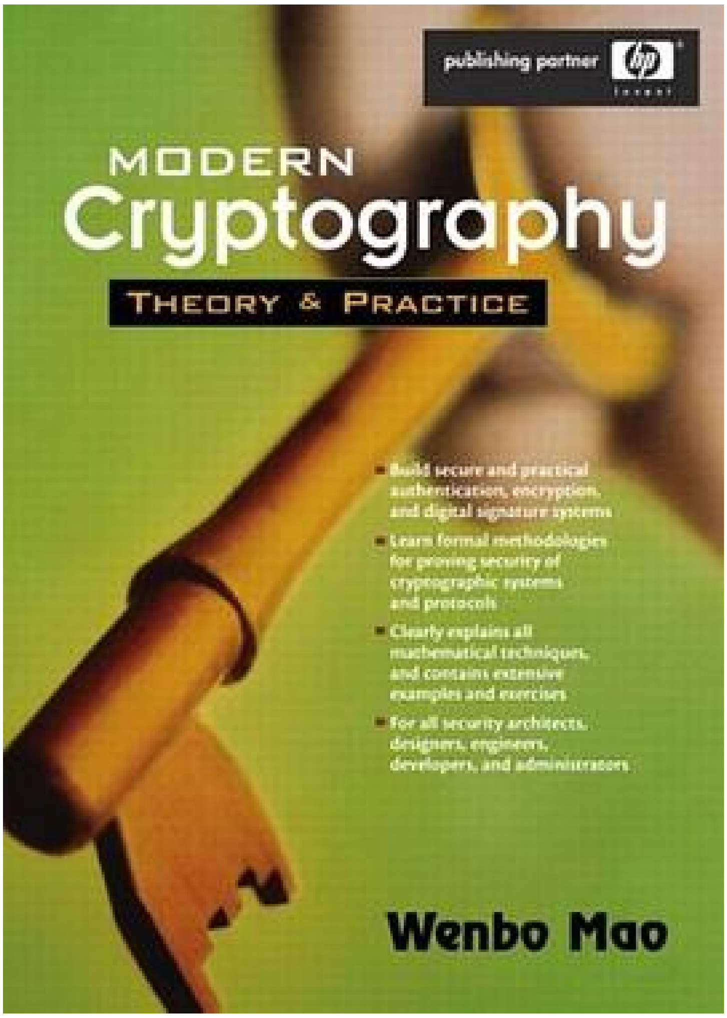
Modern Cryptography



Modern Cryptography_下载链接1_

著者:Wenbo Mao

出版者:Prentice Hall PTR

出版时间:2003-07-25

装帧:Hardcover

isbn:9780130669438

Appropriate for all graduate-level and advanced undergraduate courses in cryptography and related mathematical fields. </P>

Modern Cryptography is an indispensable resource for every advanced student of cryptography who intends to implement strong security in real-world applications. Leading HP security expert Wenbo Mao explains why conventional crypto schemes, protocols, and systems are profoundly vulnerable, introducing both fundamental theory and real-world attacks. Next, he shows how to implement crypto systems that are truly â&#128;&#156;fit for application,â&#128;&#157; and formally demonstrate their fitness. He begins by reviewing the foundations of cryptography: probability, information theory, computational complexity, number theory, algebraic techniques, and more. He presents the â&#128;&#156;idealâ&#128;&#157; principles of authentication, comparing them with real-world implementation. Mao assesses the strength of IPSec, IKE, SSH, SSL, TLS, Kerberos, and other standards, and offers practical guidance on designing stronger crypto schemes and using formal methods to prove their security and efficiency. Finally, he presents an in-depth introduction to zero-knowledge protocols: their characteristics, development, arguments, and proofs. Mao relies on practical examples throughout, and provides all the mathematical background students will need. </P>

作者介绍:

目录:

Modern Cryptography_下载链接1_

标签

Cryptography

计算机

教材

密码学

andTheory

Practice

Modern

Cryptography:

评论

Modern Cryptography_下载链接1_

书评

Modern Cryptography_下载链接1_