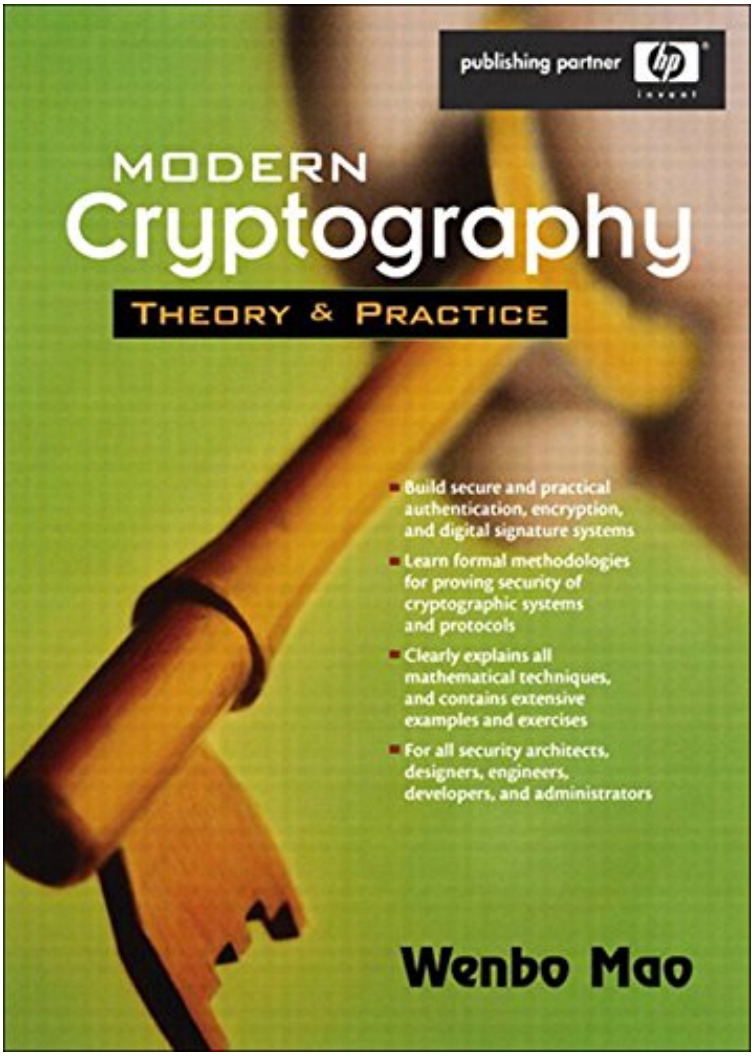
Modern Cryptography: Theory and Practice

Von Wenbo Mao
*DOC | *audiobook | ebooks | Download PDF | ePub*



Produktinformation Verffentlicht am: 2003-07-25Erscheinungsdatum: 2003-07-25File Name: B00T671URA | File size: 25.Mb

Von Wenbo Mao : Modern Cryptography: Theory and Practice before purchasing it in order to gage whether or not it would be worth my time, and all praised Modern Cryptography: Theory and Practice:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. A very good overwiew ...Von Ein KundeThis book gives a very good overview with lots of in-depth information on the common cryptographcal standards and the latest innovations. Heaps of information, well written, good to understand. Go and get it - you'll love it as it offers everything you're looking for if you need to know what's up in cryptography.

Kurzbeschreibung Leading HP security expert Wenbo Mao explains why "textbook" crypto schemes, protocols, and systems are profoundly vulnerable by revealing real-world-scenario attacks. Next, he shows how to realize cryptographic systems and protocols that are truly "fit for application"--and formally demonstrates their fitness. Mao presents practical examples throughout and provides all the mathematical background you'll need. Coverage includes: Crypto foundations: probability, information theory, computational complexity, number theory, algebraic techniques, and more Authentication: basic techniques and principles vs. misconceptions and consequential attacks Evaluating real-world protocol standards including IPSec, IKE, SSH, TLS (SSL), and Kerberos Designing stronger counterparts to vulnerable "textbook" crypto schemes Mao introduces formal and reductionist methodologies to prove the "fit-for-application" security of practical encryption, signature, signcryption, and authentication schemes. He gives detailed explanations for zero-knowledge protocols: definition, zero-knowledge properties, equatability vs. simulatability, argument vs. proof, round-efficiency, and non-interactive versions.