



Cryptography Made Simple: 2016

By Nigel P. Smart

Springer International Publishing AG. Hardback. Book Condition: new. BRAND NEW, Cryptography Made Simple: 2016, Nigel P. Smart, In this introductory textbook the author explains the key topics in cryptography. He takes a modern approach, where defining what is meant by "secure" is as important as creating something that achieves that goal, and security definitions are central to the discussion throughout. The chapters in Part 1 offer a brief introduction to the mathematical foundations: modular arithmetic, groups, finite fields, and probability; primality testing and factoring; discrete logarithms; elliptic curves; and lattices. Part 2 of the book shows how historical ciphers were broken, thus motivating the design of modern cryptosystems since the 1960s; this part also includes a chapter on information-theoretic security. Part 3 covers the core aspects of modern cryptography: the definition of security; modern stream ciphers; block ciphers and modes of operation; hash functions, message authentication codes, and key derivation functions; the "naive" RSA algorithm; public key encryption and signature algorithms; cryptography based on computational complexity; and certificates, key transport and key agreement. Finally, Part 4 addresses advanced protocols, where the parties may have different or even conflicting security goals: secret sharing schemes; commitments and oblivious transfer; zero-knowledge proofs;...



READ ONLINE
[7.43 MB]

Reviews

This publication will be worth purchasing. This is for all those who statte there was not a worthy of reading through. I discovered this publication from my dad and i suggested this pdf to find out.

-- **Macey Cummerata**

The publication is straightforward in study safer to recognize. It is writter in straightforward words and never hard to understand. Its been printed in an extremely straightforward way and it is just after i finished reading this book through which basically modified me, affect the way i think.

-- **Percy Bernhard**