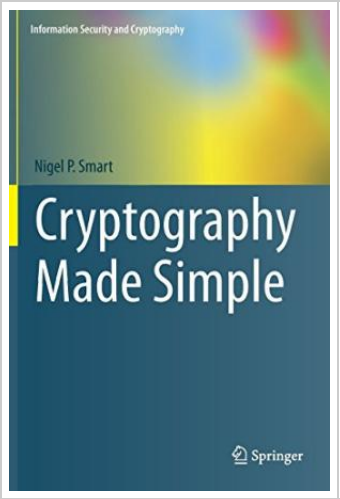

Cryptography Made Simple: 2016

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 prot ocols, where the parties may have different or even conflicting security goals: secret sharing schemes; commitments and oblivious transfer; zero-knowledge proofs;...

Reviews

Comprehensive manual! Its this sort of excellent read through. We have read through and i also am certain that i will going to read through once more again later on. You wont sense monotony at at any time of your time (that's what catalogs are for regarding in the event you question me).

-- ***Prof. Geraldine Monahan***

A must buy book if you need to adding benefit. It can be rally exciting throgh reading time. I am pleased to let you know that this is the greatest publication we have read through during my very own life and may be he best publication for possibly.

-- ***Mr. Kade Rippin***