



DOWNLOAD



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
[6.63 MB]

Reviews

It is one of the most popular ebook. It usually fails to price an excessive amount of. It has been printed in an extremely basic way in fact it is merely right after I finished reading through this book in which really altered me, change the way I believe.

-- **Sigrid Brown**

Absolutely one of the best pdf we have ever read. I really could comprehend every little thing using this written ebook. I am easily could get a satisfaction of reading a written publication.

-- **Dr. Odie Hamill**