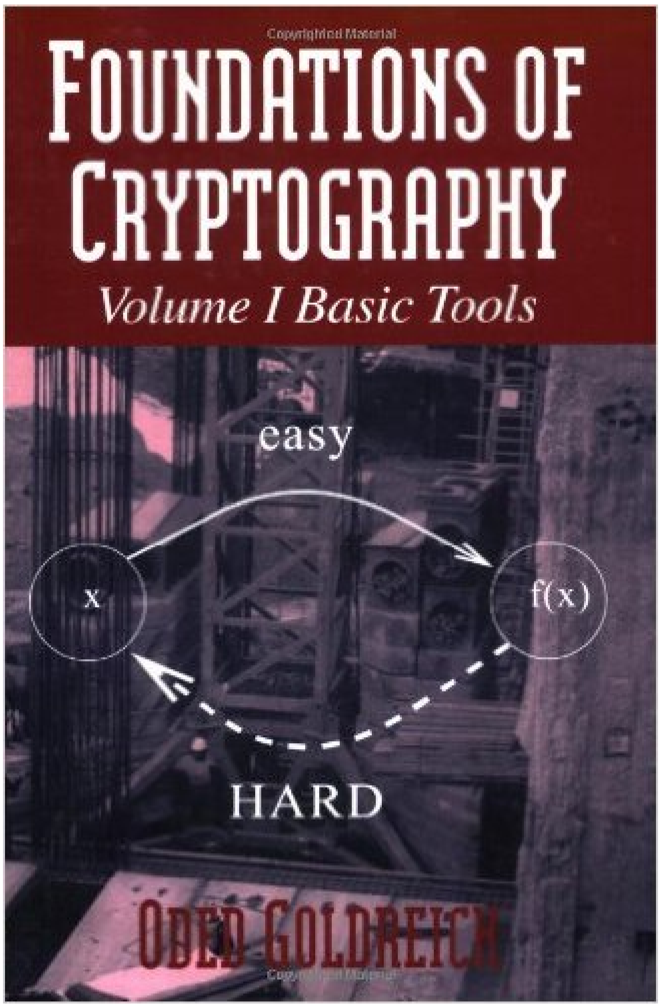
Foundations Of Cryptography: Volume 1, Basic Tools



Synopsis

Cryptography is concerned with the conceptualization, definition and construction of computing systems that address security concerns. This book presents a rigorous and systematic treatment of the foundational issues: defining cryptographic tasks and solving new cryptographic problems using existing tools. It focuses on the basic mathematical tools: computational difficulty (one-way functions), pseudorandomness and zero-knowledge proofs. Rather than describing ad-hoc approaches, this book emphasizes the clarification of fundamental concepts and the demonstration of the feasibility of solving cryptographic problems. It is suitable for use in a graduate course on cryptography and as a reference book for experts.

Book Information

Paperback: 396 pages
Publisher: Cambridge University Press; 1 edition (January 18, 2007)
Language: English
ISBN-10: 0521035368
ISBN-13: 978-0521035361
Product Dimensions: 7 x 0.8 x 10 inches
Shipping Weight: 1.9 pounds (View shipping rates and policies)
Average Customer Review: 4.2 out of 5 starsÂ Â See all reviewsÂ (5 customer reviews)
Best Sellers Rank: #482,991 in Books (See Top 100 in Books) #3 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Coding Theory #121 inÂ Books > Computers & Technology > Security & Encryption > Encryption #132 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

We all know what it means for an algorithm to compute a function, but what does it mean for an encryption scheme to be secure? Traditionally, cryptographic schemes were suggested and attacked based on ad-hoc criterias, for lack of a proper theoretical setting. The last two decades have seen enormous progress in this respect. New notions were devised to harness the computational difficulty of problems in a constructive way to achieve security (in various senses) against all adversaries. This enabled the definition of a host of well-defined cryptographic "objects" and investigation of their existence and relations.The planned 3-volume series aims to provide a thorough presentation of the theory, written by a dominant figure in the field. This first volume introduces the basic notions: one-way functions, pseudorandom generators, various zero-knowledge proof systems and related concepts. Curiously, common cryptographic objects such as encryption schemes and signature schemes are only briefly discussed in an appendix -- the author has chosen to postpone these to the Volume 2 in the interest of in-depth discussion of the simpler objects. Hence this volume does not stand well on its own, and until Volume 2 is published the impatient reader may be disappointed. Fortunately, drafts of Volume 2 are available on-line: [...]The presentation style is a tour de force of didactic sensitivity. The subject material is often problematic, because the mental gymnastics required are not quite like any other field. The author is fully aware of this, and provides ample intuitive discussion and motivation to help the reader through the more technical parts (without compromising rigorousness).

Download to continue reading...

Foundations of Cryptography: Volume 1, Basic Tools Foundations of Cryptography: Volume 1, Basic Tools (Vol 1) Foundations of Cryptography: Volume 2, Basic Applications Foundations of GMAT Math, 5th Edition (Manhattan GMAT Preparation Guide: Foundations of Math) Nutritional Foundations and Clinical Applications: A Nursing Approach, 5e (Foundations and Clinical Applications of Nutrition) Break the Code: Cryptography for Beginners (Dover Children's Activity Books) Introduction to Cryptography with Coding Theory Cryptography and Network Security: Principles and Practice (3rd Edition) An Introduction to Cryptography (Discrete Mathematics and Its Applications) Cryptography and Network Security: Principles and Practice (2nd Edition) RSA and Public-Key Cryptography (Discrete Mathematics and Its Applications) Cryptography and Coding (The Institute of Mathematics and its Applications Conference Series, New Series) Cryptography and Lattices: International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001. Revised Papers (Lecture Notes in Computer Science) An Introduction to Mathematical Cryptography (Undergraduate Texts in Mathematics) The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography Cryptography: A Very Short Introduction Understanding Bitcoin: Cryptography, Engineering and Economics (The Wiley Finance Series) Computer Security and Cryptography Foundations in Comic Book Art: SCAD Creative Essentials (Fundamental Tools and Techniques for Sequential Artists) Six Sigma for Green Belts and Champions: Foundations, DMAIC, Tools, Cases, and Certification