Foundations Of Cryptography: Volume 1, Basic Tools

Focuses on the basic mathematical tools needed for cryptographic design: computational difficulty (one-way functions), pseudorandomness and zero-knowledge proofs.Cryptography is concerned with the conceptualization, definition and construction of computing systems that address security concerns. The design of cryptographic systems must be based on firm foundations. 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. The emphasis is on the clarification of fundamental concepts and on demonstrating the feasibility of solving cryptographic problems, rather than on describing ad-hoc approaches. The book is suitable for use in a graduate course on cryptography and as a reference book for experts. The author assumes basic familiarity with the design and analysis of algorithms, some knowledge of complexity theory and probability is also useful. EAN/ISBN : 9780511031601 Publisher(s): Cambridge University Press Format: ePub/PDF Author(s): Goldreich, Oded

DOWNLOAD HERE