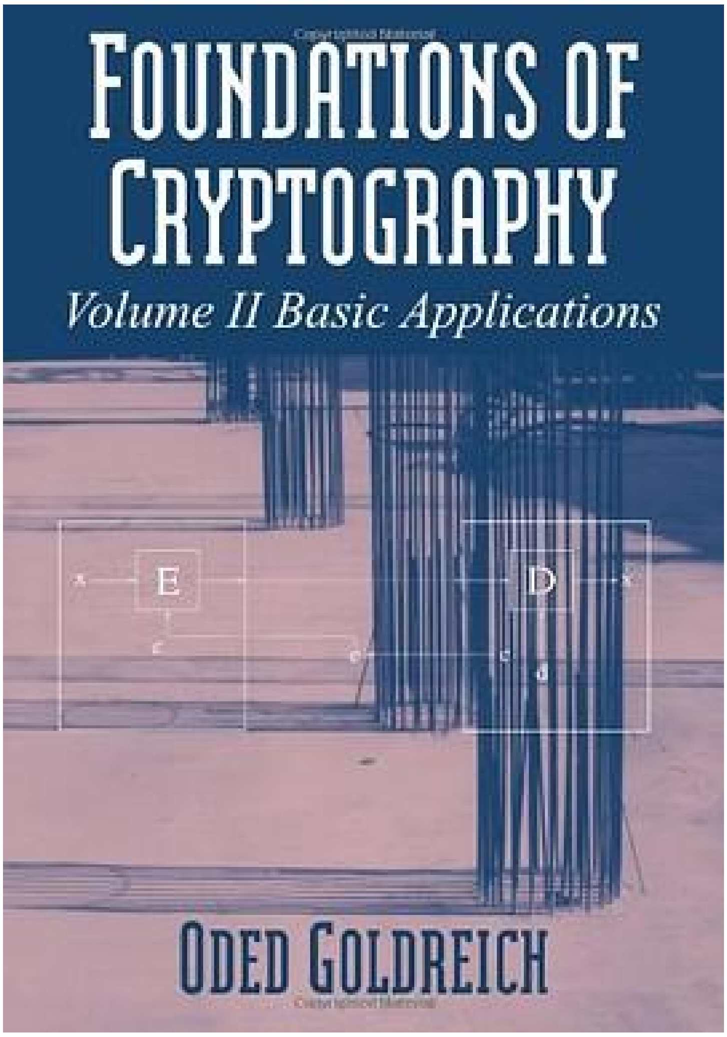
Foundations of Cryptography



Foundations of Cryptography_下载链接1_

著者:Oded Goldreich

出版者:Cambridge University Press

出版时间:2007-01-18

装帧:Paperback

isbn:9780521035361

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.

作者介绍:

目录:

标签

计算机科学

计算机

密码学

cryptography

数学

D

1111

评论

靠着这书可把这学期密码学的试考完了，对密码学又爱又恨喜欢给自己找虐

Foundations of Cryptography_下载链接1_

书评

Goldreich是交互证明系统的创始人之一，很好的写的，而且他偏重于概念性的讲述，把这些概念的关系讲的很清楚。 关于 入门 这两个字的意思
，我想解释一下，因为已经不能改题目了，所以有误导性，如果你没有密码学的基础的话，一定不能用这本书，我的入门的意思是如果你想研究密...

Foundations of Cryptography_下载链接1_