1. Record Nr. UNINA9910484807103321

| | |
|---|---|
| Autore | Mittelbach Arno |
| Titolo | The Theory of Hash Functions and Random Oracles : An Approach to Modern Cryptography / / by Arno Mittelbach, Marc Fischlin |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021 |
| ISBN | 3-030-63287-3 |
| Edizione | [1st ed. 2021.] |
| Descrizione fisica | 1 online resource (XXIII, 788 p. 109 illus.) |
| Collana | Information Security and Cryptography, , 2197-845X |
| Disciplina | 005.82 |
| Soggetti | Data protection<br>Computer security<br>Computer networks - Security measures<br>Data and Information Security<br>Principles and Models of Security<br>Mobile and Network Security |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | Introduction -- Preliminaries: Cryptographic Foundations -- Part I: Foundations -- Computational Security -- Pseudorandomness and Computational Indistinguishability -- Collision Resistance -- Encryption Schemes -- Signature Schemes -- Non-cryptographic Hashing -- Part II: The Random Oracle Methodology -- The Random Oracle Model -- The Full Power of Random Oracles -- Random Oracle Schemes in Practice -- Limitations of Random Oracles -- The Random Oracle Controversy -- Part III: Hash Function Constructions -- Iterated Hash Functions -- Constructing Compression Functions -- Iterated Hash Functions in Practice -- Constructions of Keyed Hash Functions -- Constructing Random Oracles: Indifferentiability -- Constructing Random Oracles: UCEs -- Index. |
| Sommario/riassunto | Hash functions are the cryptographer’s Swiss Army knife. Even though they play an integral part in today’s cryptography, existing textbooks discuss hash functions only in passing and instead often put an emphasis on other primitives like encryption schemes. In this book the authors take a different approach and place hash functions at the |

center. The result is not only an introduction to the theory of hash functions and the random oracle model but a comprehensive introduction to modern cryptography. After motivating their unique approach, in the first chapter the authors introduce the concepts from computability theory, probability theory, information theory, complexity theory, and information-theoretic security that are required to understand the book content. In Part I they introduce the foundations of hash functions and modern cryptography. They cover a number of schemes, concepts, and proof techniques, including computational security, one-way functions, pseudorandomness and pseudorandom functions, game-based proofs, message authentication codes, encryption schemes, signature schemes, and collision-resistant (hash) functions. In Part II the authors explain the random oracle model, proof techniques used with random oracles, random oracle constructions, and examples of real-world random oracle schemes. They also address the limitations of random oracles and the random oracle controversy, the fact that uninstantiable schemes exist which are provably secure in the random oracle model but which become insecure with any real-world hash function. Finally in Part III the authors focus on constructions of hash functions. This includes a treatment of iterative hash functions and generic attacks against hash functions, constructions of hash functions based on block ciphers and number-theoretic assumptions, a discussion of privately keyed hash functions including a full security proof for HMAC, and a presentation of real-world hash functions. The text is supported with exercises, notes, references, and pointers to further reading, and it is a suitable textbook for undergraduate and graduate students, and researchers of cryptology and information security.