1. Record Nr. UNISA996465535303316

Autore	Neuenschwander Daniel
Titolo	Probabilistic and Statistical Methods in Cryptology [[electronic resource]] : An Introduction by Selected Topics / / by Daniel Neuenschwander
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	1-280-30756-0 9786610307562 3-540-25942-2
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (X, 162 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3028
Disciplina	003.54
Soggetti	Computers Data encryption (Computer science) Probabilities Theory of Computation Cryptology Probability Theory and Stochastic Processes
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1 Classical Polyalphabetic Substitution Ciphers -- 2 RSA and Probabilistic Prime Number Tests -- 3 Factorization with Quantum Computers: Shor’s Algorithm -- 4 Physical Random-Number Generators -- 5 Pseudo-random Number Generators -- 6 An Information Theory Primer -- 7 Tests for (Pseudo-)Random Number Generators -- 8 Diffie-Hellman Key Exchange -- 9 Differential Cryptanalysis -- 10 Semantic Security -- 11 *Algorithmic Complexity -- 12 Birthday Paradox and Meet-in-the-Middle Attack -- 13 Quantum Cryptography.
Sommario/riassunto	Cryptology nowadays is one of the most important areas of applied mathematics, building on deep results and methods from various areas of mathematics. This text is devoted to the study of stochastic aspects of cryptology. Besides classical topics from cryptology, the author presents chapters on probabilistic prime number tests, factorization with quantum computers, random-number generators, pseudo-

random-number generators, information theory, and the birthday paradox and meet-in-the-middle attack. In the light of the vast literature on stochastic results relevant for cryptology, this book is intended as an invitation and introduction for students, researchers, and practitioners to probabilistic and statistical issues in cryptology.