1.

Record Nr.	UNINA9910254244603321
Autore	Ahlswede Rudolf
Titolo	Hiding Data - Selected Topics : Rudolf Ahlswede’s Lectures on Information Theory 3 / / by Rudolf Ahlswede ; edited by Alexander Ahlswede, Ingo Althöfer, Christian Deppe, Ulrich Tamm
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-31515-3
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (367 p.)
Collana	Foundations in Signal Processing, Communications and Networking, , 1863-8546 ; ; 12
Disciplina	001.539
Soggetti	Computer science - Mathematics Mathematical Applications in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Chapter I A Short Course on Cryptography -- Chapter II Authentication and Secret-Key Cryptology -- Chapter III The Mathematical Background of the Advanced Encryption Standard -- Chapter IV Elliptic Curve Cryptosystems -- Chapter V Founding Cryptography on Oblivious Transfer -- Supplement.
Sommario/riassunto	Devoted to information security, this volume begins with a short course on cryptography, mainly based on lectures given by Rudolf Ahlswede at the University of Bielefeld in the mid 1990s. It was the second of his cycle of lectures on information theory which opened with an introductory course on basic coding theorems, as covered in Volume 1 of this series. In this third volume, Shannon’s historical work on secrecy systems is detailed, followed by an introduction to an information-theoretic model of wiretap channels, and such important concepts as homophonic coding and authentication. Once the theoretical arguments have been presented, comprehensive technical details of AES are given. Furthermore, a short introduction to the history of public-key cryptology, RSA and El Gamal cryptosystems is provided, followed by a look at the basic theory of elliptic curves, and algorithms for efficient addition in elliptic curves. Lastly, the important topic of

“oblivious transfer” is discussed, which is strongly connected to the privacy problem in communication. Today, the importance of this problem is rapidly increasing, and further research and practical realizations are greatly anticipated. This is the third of several volumes serving as the collected documentation of Rudolf Ahlswede’s lectures on information theory. Each volume includes comments from an invited well-known expert. In the supplement to the present volume, Rüdiger Reischuk contributes his insights. Classical information processing concerns the main tasks of gaining knowledge and the storage, transmission and hiding of data. The first task is the prime goal of Statistics. For transmission and hiding data, Shannon developed an impressive mathematical theory called Information Theory, which he based on probabilistic models. The theory largely involves the concept of codes with small error probabilities in spite of noise in the transmission, which is modeled by channels. The lectures presentedin this work are suitable for graduate students in Mathematics, and also for those working in Theoretical Computer Science, Physics, and Electrical Engineering with a background in basic Mathematics. The lectures can be used as the basis for courses or to supplement courses in many ways. Ph.D. students will also find research problems, often with conjectures, that offer potential subjects for a thesis. More advanced researchers may find questions which form the basis of entire research programs.