Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 46 (2000)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Kapitel: Information,communication ,circuits

Information, communication, circuits

Johannes BUCHMANN, Tom HØHOLDT, Henning STICHTENOTH, Horacio TAPIA-RECILLAS, (Editors). — **Coding theory, cryptography and related areas.** — Proceedings of an International Conference on Coding Theory, Cryptography and Related Areas, held in Guanajuato, Mexico, in April 1998. — Un vol. broché, 15,5×23,5, de VIII, 259 p. — ISBN 3-540-66248-0. — Prix: DM 129.00. — Springer, Berlin, 2000.

This book contains 23 contributions presented at the "International Conference on Coding Theory, Cryptography and Related Areas (ICCC)", held in Guanajuato, Mexico, in April 1998. It comprises a series of research papers on various aspects of coding theory (geometric-algebraic, decoding, exponential sums, etc.) and cryptography (discrete logarithm problem, public key cryptosystems, primitives, etc.), as well as in other research areas, such as codes over finite rings and some aspects of function fields and algebraic geometry over finite fields. The book contains new results on the subject, never published in any other form.

David JOYNER, (Editor). — **Coding theory and cryptography: from Enigma and Geheimschreiber to quantum theory.** — Un vol. broché, 15,5×23,5, de VI, 256 p. — ISBN 3-540-66336-3. — Prix: DM 129.00. — Springer, Berlin, 2000.

These are the proceedings of the Conference on Coding Theory, Cryptography, and Number Theory held at the U.S. Naval Academy during October 25-26, 1998. The emphasis is on geometric Goppa codes, but there is also a paper on codes arising from combinatorial constructions. There are both historical and mathematical papers on cryptography. Several of the contributions on cryptography describe the work done by the British and their allies during World War II to crack the German and Japanese ciphers. Some mathematical aspects of the Enigma rotor machine and more recent research on quantum cryptography are described. Moreover, there are two papers concerned with the RSA cryptosystem and related number-theoretic issues.

Gilbert G. WALTER, Martha CONTRERAS. — **Compartmental modeling with networks.** — Modeling and simulation in science, engineering and technology. — Un vol. relié, 16×24, de XVIII, 250 p. — ISBN 0-8176-4019-3. — Prix: SFr. 108.00. — Birkhäuser, Basel, 1999.

In order to provide a complete and balanced presentation, the book is organized in four parts. Part 1 is devoted to the theory of digraphs; Part 2 addresses Markov chains; Part 3 discusses differential equations; and Part 4 presents the theory of compartmental models, addressing the relations between dynamics of the solution and structure of the model. Key applications discussed include ecosystem models, fluid transfer, competition models, tracer kinetic experiments, and network flows. Essential topics and methods are presented in an accessible style with many examples: directed graphs, differential equations, Markov chains, and compartmental model construction.