Codes, Cryptology and Curves with Computer Algebra

Ruud Pellikaan
Technische Universiteit Eindhoven, The Netherlands

Xin-Wen Wu
Griffith University, Queensland

Stanislav Bulygin
Relinde Jurrius
Université de Neuchatel, Switzerland

This well-balanced text touches on theoretical and applied aspects of protecting digital data. The reader is provided with the basic theory and is then shown deeper fascinating detail, including the current state of the art. Readers will soon become familiar with methods of protecting digital data while it is transmitted, as well as while the data is being stored. Both basic and advanced error-correcting codes are introduced together with numerous results on their parameters and properties. The authors explain how to apply these codes to symmetric and public key cryptosystems and secret sharing. Interesting approaches based on polynomial systems solving are applied to cryptography and decoding codes. Computer algebra systems are also used to provide an understanding of how objects introduced in the book are constructed, and how their properties can be examined. This book is designed for Masters-level students studying mathematics, computer science, electrical engineering or physics.