ZMATH 2011a.00745

Klima, Richard E.; Sigmon, Neil P.; Stitzinger, Ernest L.

Applications of abstract algebra with Maple and MATLAB. 2nd ed.

Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC (ISBN 1-58488-610-2/hbk). 505 p. (2007).

This book concentrates on the mathematical softwares `Maple` and `MATLAB` which would certainly help in better understanding of several topics dependent on abstract algebra like block designs, coding theory, combinatorics, cryptography and graph theory, eliminating the need for extensive computations. Beginning with a comprehensive and concise review of all prerequisite advanced mathematics, the authors go on examining block designs, coding theory, cryptography: RSA cryptosystem, digital signatures, primes for security, elliptic curve cryptosystems; finally dealing with counting techniques such as Pólya's, Burnside's theorem, Pólya enumeration theorem, and counting undirected graphs. This (second) edition incorporates some new chapters which are on Vigenère ciphers, Advanced Encryption Standard (AES) and graph theory, also including expanded exercises and additional research exercises. The book provides a variety of codes including Hadamard, Reed-Muller, Hamming, BCH, and Reed-Solomon; exploers shift, affine, Hill, and Vigenère ciphers; describes how elliptic curves can be incorporated into the El-Gamal cryptosystem; presents a thorough treatment of AES. The book intends to give students more exposure to basic algebraic concepts as well as their practical uses. The inclusion of two mathematical software packages available make the book a useful tool for students, mathematicians, and computer scientists. `Maple` and `MATLAB` files and functions are available for download online and from a CD-ROM with all the programs and codes that are used in the book. The book can be used by students having a course on linear and abstract algebra.

Bal Kishan Dass (Delhi)

Classification: H45 K25 R25
Keywords: linear algebra; Maple; MATLAB; designs; coding theory; cryptography; Pólya theory