Applied Algebra Codes Ciphers And Discrete Algorithms Second Edition Discrete Mathematics And Its Applications

With a substantial amount of new material, the Handbook of Linear Algebra, Second Edition provides comprehensive coverage of linear algebra concepts, applications, and computational software packages in an easy-to-use format. It guides you from the very elementary aspects of the subject to the frontiers of current research. Along with revisions and updates throughout, the second edition of this bestseller includes 20 new chapters. New to the Second Edition Separate chapters on Schur complements, additional types of canonical forms, tensors, matrix polynomials, matrix equations, special types of matrices, generalized inverses, matrices over finite fields, invariant subspaces, representations of quivers, and spectral sets New chapters on combinatorial matrix theory topics, such as tournaments, the minimum rank problem, and spectral graph theory, as well as numerical linear algebra topics, including algorithms for structured matrix computations, stability of structured matrix computations, and nonlinear eigenvalue problems More chapters on applications of linear algebra, including epidemiology and quantum error correction New chapter on using the free and open source software system Sage for linear algebra Additional sections in the chapters on sign pattern matrices and applications to geometry Conjectures and open problems in most chapters on advanced topics Highly praised as a valuable resource for anyone who uses linear algebra, the first edition covered virtually all aspects of linear algebra and its applications. This edition continues to encompass the fundamentals of linear algebra, combinatorial and numerical linear algebra, and applications of linear algebra to various disciplines while also covering up-to-date software packages for linear algebra computations.

On the surface, matrix theory and graph theory seem like very different branches of mathematics. However, adjacency, Laplacian, and incidence matrices are commonly used to represent graphs, and many properties of matrices can give us useful information about the structure of graphs.Applications of Combinatorial Matrix Theory to Laplacian Matrices o

These are the proceedings of the 8th AAECC conference, held in Tokyo in August 1990. Researchers from around the world present new results of recent theoretical and application-oriented research on applied algebra, algebraic algorithms and error-correcting codes.

Using mathematical tools from number theory and finite fields, Applied Algebra: Codes, Ciphers, and Discrete Algorithms, Second Edition presents practical methods for solving problems in data security and data integrity. It is designed for an applied algebra course for students who have had prior classes in abstract or linear algebra. While the content has been reworked and improved, this edition continues to cover many algorithms that arise in cryptography and error-control codes. New to the Second Edition A CD-ROM containing an interactive version of the book that is powered by Scientific Notebook®, a mathematical word processor and easy-to-use computer algebra system New appendix that reviews prerequisite topics in algebra and number theory Double the number of exercises Instead of a general study on finite groups, the book considers finite groups of permutations and develops just enough of the theory of finite fields to facilitate construction of the fields used for error-control codes and the

Advanced Encryption Standard. It also deals with integers and polynomials. Explaining the mathematics as needed, this text thoroughly explores how mathematical techniques can be used to solve practical problems. About the Authors Darel W. Hardy is Professor Emeritus in the Department of Mathematics at Colorado State University. His research interests include applied algebra and semigroups. Fred Richman is a professor in the Department of Mathematical Sciences at Florida Atlantic University. His research interests include Abelian group theory and constructive mathematics. Carol L. Walker is Associate Dean Emeritus in the Department of Mathematical Sciences at New Mexico State University. Her research interests include Abelian group theory, applications of homological algebra and category theory, and the mathematics of fuzzy sets and fuzzy logic. What Is Combinatorics Anyway? Broadly speaking, combinatorics is the branch of mathematics dealing with different ways of selecting objects from a set or arranging objects. It tries to answer two major kinds of questions, namely, counting questions: how many ways can a selection or arrangement be chosen with a particular set of properties; and structural questions: does there exist a selection or arrangement of objects with a particular set of properties? The authors have presented a text for students at all levels of preparation. For some, this will be the first course where the students see several real proofs. Others will have a good background in linear algebra, will have completed the calculus stream, and will have started abstract algebra. The text starts by briefly discussing several examples of typical combinatorial problems to give the reader a better idea of what the subject covers. The next chapters explore enumerative ideas and also probability. It then moves on to enumerative functions and the relations between them, and generating functions and recurrences., Important families of functions, or numbers and then theorems are presented. Brief introductions to computer algebra and group theory come next. Structures of particular interest in combinatorics: posets, graphs, codes, Latin squares, and experimental designs follow. The authors conclude with further discussion of the interaction between linear algebra and combinatorics. Features Two new chapters on probability and posets. Numerous new illustrations, exercises, and problems. More examples on current technology use A thorough focus on accuracy Three appendices: sets, induction and proof techniques, vectors and matrices, and biographies with historical notes, Flexible use of MapleTM and MathematicaTM

The first book devoted exclusively to quantitative graph theory, Quantitative Graph Theory: Mathematical Foundations and Applications presents and demonstrates existing and novel methods for analyzing graphs quantitatively. Incorporating interdisciplinary knowledge from graph theory, information theory, measurement theory, and statistical techniques, this book covers a wide range of quantitative-graph theoretical concepts and methods, including those pertaining to real and random graphs such as: Comparative approaches (graph similarity or distance) Graph measures to characterize graphs quantitatively Applications of graph measures in social network analysis and other disciplines Metrical properties of graphs and measures Mathematical properties of quantitative methods or measures in graph theory Network complexity measures and other topological indices Quantitative approaches to graphs using machine learning (e.g., clustering) Graph measures and statistics Information-theoretic methods to analyze graphs quantitatively (e.g., entropy) Through its broad coverage, Quantitative Graph Theory: Mathematical Foundations and Applications fills a gap in the contemporary literature of discrete and applied mathematics, computer science, systems biology, and related disciplines. It is intended for researchers as well as graduate and advanced undergraduate students in the fields of mathematics, computer science, mathematical chemistry, cheminformatics, physics, bioinformatics, and systems biology.

From the exciting history of its development in ancient times to the present day, Introduction to Cryptography with Mathematical Foundations and Computer Implementations provides a focused tour of the central concepts of cryptography. Rather than present an encyclopedic treatment of topics in cryptography, it delineates cryptographic concepts in chronological order, developing the mathematics as needed. Written in an engaging yet rigorous style, each chapter introduces important concepts with clear definitions and theorems. Numerous examples explain key points while figures and tables help illustrate more difficult or subtle concepts. Each chapter is punctuated with "Exercises for the Reader;" complete solutions for these are included in an appendix. Carefully crafted exercise sets are also provided at the end of each chapter, and detailed solutions to most odd-numbered exercises can be found in a designated appendix. The computer implementation section at the end of every chapter guides students through the process of writing their own programs. A supporting website provides an extensive set of sample programs as well as downloadable platform-independent applet pages for some core programs and algorithms. As the reliance on cryptography by business, government, and industry continues and new technologies for transferring data become available, cryptography plays a permanent, important role in day-to-day operations. This self-contained sophomore-level text traces the evolution of the field, from its origins through present-day cryptosystems, including public key cryptography and elliptic curve cryptography.

Combinatory logic is one of the most versatile areas within logic that is tied to parts of philosophical, mathematical, and computational logic. Functioning as a comprehensive source for current developments of combinatory logic, this book is the only one of its kind to cover results of the last four decades. Using a reader-friendly style, the author presents the most up-to-date research studies. She includes an introduction to combinatory logic before progressing to its central theorems and proofs. The text makes intelligent and well-researched connections between combinatory logic and lambda calculi and presents models and applications to illustrate these connections.

Linear algebra forms the basis for much of modern mathematics—theoretical, applied, and computational. Finite-Dimensional Linear Algebra provides a solid foundation for the study of advanced mathematics and discusses applications of linear algebra to such diverse areas as combinatorics, differential equations, optimization, and approximation. The author begins with an overview of the essential themes of the book: linear equations, best approximation, and diagonalization. He then takes students through an axiomatic development of vector spaces, linear operators, eigenvalues, norms, and inner products. In addition to discussing the special properties of symmetric matrices, he covers the Jordan canonical form, an important theoretical tool, and the singular value decomposition, a powerful tool for computation. The final chapters present introductions to numerical linear algebra and analysis in vector spaces, including a brief introduction to functional analysis (infinite-dimensional linear algebra). Drawing on material from the author's own course, this textbook gives students a strong theoretical understanding of linear algebra. It offers many illustrations of how linear algebra is used throughout mathematics.

The AAECC symposia serieswas started in 1983by Alain Poli (Toulouse), who, together with R. Desq, D. Lazardand P. Camion, organizedthe ?rst conference. OriginallytheacronymAAECCstoodfor"AppliedAlgebraandError-Correcting Codes."Overtheyearsitsmeaninghasshiftedto"AppliedAlgebra, Algebraic- gorithmsandError-CorrectingCodes,"re?ectingthegrowingimportanceofc- plexity, particularlyfor decoding algorithms.During the AAECC-12 symposium the ConferenceCommitteedecidedtoenforcethe theoryandpracticeofthe c- ing side as well as the cryptographic aspects. Algebra was conserved, as in the past, but slightly more oriented to algebraic geometry codes, ?nite ?elds, c- plexity, polynomials, andgraphs. The main topics for AAECC-18 were algebra, algebraiccomputation, codes and algebra, codes and combinatorics, modulation and codes, sequences, and cryptography. TheinvitedspeakersofthiseditionwereIwanDuursma, HenningStichtenoth, and Fernando Torres. We would like to express our deep regret for the loss of Professor Ralf Kotter,] who recently passed away and could not be our fourth invited speaker. Except for AAECC-1 (Discrete Mathematics 56, 1985) and AAECC-7 (D- crete Applied Mathematics 33, 1991), the proceedings of all the symposia have been published in Springer'sLecture Notes in Computer Science (Vols. 228,229, 307, 356, 357, 508, 539, 673, 948, 1255, 1719, 2227, 2643, 3857, 4851). Itis apolicy ofAAECCto maintaina highscienti?c standard, comparableto that of a journal. This was made possible thanks to the many referees involved. Each submitted paper was evaluated by at least two international researchers. AAECC-18 received and refereed 50 submissions. Of these, 22 were selected for publication in these proceedings as regular papers and 7 were selected as extended abstracts. Commutation Relations, Normal Ordering, and Stirling Numbers provides an introduction to the combinatorial aspects of normal ordering in the Weyl algebra and some of its close relatives. The Weyl algebra is the algebra generated by two letters U and V subject to the commutation relation UV ? VU = I. It is a classical result that normal ordering powers of VU involve the Stirling numbers. The book is a one-stop reference on the research activities and known results of normal ordering and Stirling numbers. It discusses the Stirling numbers, closely related generalizations, and their role as normal ordering coefficients in the Weyl algebra. The book also considers several relatives of this algebra, all of which are special cases of the algebra in which UV ? qVU = hVs holds true. The authors describe combinatorial aspects of these algebras and the normal ordering process in them. In particular, they define associated generalized Stirling numbers as normal ordering coefficients in analogy to the classical Stirling numbers. In addition to the combinatorial aspects, the book presents the relation to operational calculus, describes the physical motivation for ordering words in the Weyl algebra arising from quantum theory, and covers some physical applications.

RC4 Stream Cipher and Its Variants is the first book to fully cover the popular software stream cipher RC4. With extensive expertise in stream cipher cryptanalysis and RC4 research, the authors focus on the analysis and design issues of RC4. They also explore variants of RC4 and the eSTREAM finalist HC-128. After an introduction to the vast field of cryptology, the book reviews hardware and software stream ciphers and describes RC4. It presents a theoretical analysis of RC4 KSA, discussing biases of the permutation bytes toward secret key bytes and absolute values. The text explains how to reconstruct the secret key from known state information and analyzes the RC4 PRGA in detail, including a sketch of state recovery attacks. The book then describes three popular attacks on RC4: distinguishing attacks, Wired Equivalent Privacy

(WEP) protocol attacks, and fault attacks. The authors also compare the advantages and disadvantages of several variants of RC4 and examine stream cipher HC-128, which is the next level of evolution after RC4 in the software stream cipher paradigm. The final chapter emphasizes the safe use of RC4. With open research problems in each chapter, this book offers a complete account of the most current research on RC4.

This book constitutes the refereed proceedings of the 16th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-16, held in Las Vegas, NV, USA in February 2006. The 25 revised full papers presented together with 7 invited papers were carefully reviewed and selected from 32 submissions. Among the subjects addressed are block codes; algebra and codes: rings, fields, and AG codes; cryptography; sequences; decoding algorithms; and algebra: constructions in algebra, Galois groups, differential algebra, and polynomials.

Applicable to any problem that requires a finite number of solutions, finite state-based models (also called finite state machines or finite state automata) have found wide use in various areas of computer science and engineering. Handbook of Finite State Based Models and Applications provides a complete collection of introductory materials on fini

Focusing on a very active area of mathematical research in the last decade, Combinatorics of Set Partitions presents methods used in the combinatorics of pattern avoidance and pattern enumeration in set partitions. Designed for students and researchers in discrete mathematics, the book is a one-stop reference on the results and research activities of set partitions from 1500 A.D. to today. Each chapter gives historical perspectives and contrasts different approaches, including generating functions, kernel method, block decomposition method, generating tree, and Wilf equivalences. Methods and definitions are illustrated with worked examples and MapleTM code. End-of-chapter problems often draw on data from published papers and the author's extensive research in this field. The text also explores research directions that extend the results discussed. C++ programs and output tables are listed in the appendices and available for download on the author's web page.

Get an In-Depth Understanding of Graph Drawing Techniques, Algorithms, Software, and ApplicationsThe Handbook of Graph Drawing and Visualization provides a broad, up-to-date survey of the field of graph drawing. It covers topological and geometric foundations, algorithms, software systems, and visualization applications in business, education, scie

The reach of algebraic curves in cryptography goes far beyond elliptic curve or public key cryptography yet these other application areas have not been systematically covered in the literature. Addressing this gap, Algebraic Curves in Cryptography explores the rich uses of algebraic curves in a range of cryptographic applications, such as secret sh Easily Accessible to Students with Nontechnical Backgrounds In a clear, nontechnical manner, Cryptology: Classical and Modern with Maplets explains how fundamental mathematical concepts are the bases of cryptographic algorithms. Designed for students with no background in college-level mathematics, the book assumes minimal mathematical prerequisites and incorporates student-friendly Maplets throughout that provide practical examples of the techniques used. Technology Resource By using the Maplets, students can complete complicated tasks with relative ease. They can encrypt, decrypt, and cryptanalyze messages without the burden of understanding programming or computer syntax. The authors explain topics in detail first before introducing one or more Maplets. All Maplet material and exercises are given in separate, clearly labeled sections. Instructors can omit the Maplet sections without any loss of continuity and non-Maplet examples and exercises can be completed with, at most, a simple hand-held calculator. The Maplets are available for download at www.radford.edu/~npsigmon/cryptobook.html. A Gentle, Hands-On Introduction to Cryptology After introducing elementary methods and techniques, the text fully develops the Enigma cipher machine and Navajo code used during World War II, both of which are rarely found in cryptology textbooks. The authors then demonstrate mathematics in cryptology through monoalphabetic, polyalphabetic, and block ciphers. With a focus on public-key cryptography, the book describes RSA ciphers, the Diffie–Hellman key exchange, and ElGamal ciphers. It also explores current U.S. federal cryptographic standards, such as the AES, and explains how to authenticate messages via digital signatures, hash functions, and certificates.

Representation Theory of Symmetric Groups is the most up-to-date abstract algebra book on the subject of symmetric groups and representation theory. Utilizing new research and results, this book can be studied from a combinatorial, algorithmic or algebraic viewpoint. This book is an excellent way of introducing today’s students to representation theory of the symmetric groups, namely classical theory. From there, the book explains how the theory can be extended to other related combinatorial algebras like the Iwahori-Hecke algebra. In a clear and concise manner, the author presents the case that most calculations on symmetric group can be performed by utilizing appropriate algebras of functions. Thus, the book explains how some Hopf algebras (symmetric functions and generalizations) can be used to encode most of the combinatorial properties of the representations of symmetric groups. Overall, the book is an innovative introduction to representation theory of symmetric groups for graduate students and researchers seeking new ways of thought.

In the ten years since the publication of the best-selling first edition, more than 1,000 graph theory papers have been published each year. Reflecting these advances, Handbook of Graph Theory, Second Edition provides comprehensive coverage of the main topics in pure and applied graph theory. This second edition—over 400 pages longer than its predecessor—incorporates 14 new sections. Each chapter includes lists of essential definitions and facts, accompanied by examples, tables, remarks, and, in some cases, conjectures and open problems. A bibliography at the end of each chapter provides an extensive guide to the research literature and pointers to monographs. In addition, a glossary is included in each chapter as well as at the end of each section. This edition also contains notes regarding terminology and notation. With 34 new contributors, this handbook is the most comprehensive single-source guide to graph theory. It emphasizes quick accessibility to topics for non-experts and enables easy cross-referencing among chapters.

This book constitutes the refereed proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-18, held in Tarragona, Spain, in June 2009. The 22 revised full papers presented together with 7 extended absstracts were carefully reviewed and selected from 50 submissions. Among the subjects addressed are block codes, including list-decoding algorithms; algebra and codes: rings, fields, algebraic geometry codes; algebra: rings and fields, polynomials, permutations, lattices; cryptography: cryptanalysis and complexity; computational algebra: algebraic algorithms and transforms; sequences and boolean functions.

This book covers both theoretical and practical results for graph polynomials. Graph polynomials have been developed for measuring combinatorial graph invariants and for characterizing graphs. Various problems in pure and applied graph theory or discrete mathematics can be treated and solved efficiently by using graph polynomials. Graph polynomials have been proven useful areas such as discrete mathematics, engineering, information sciences, mathematical chemistry and related disciplines.

This two-volume set on Mathematical Principles of the Internet provides a comprehensive overview of the mathematical principles of Internet engineering. The books do not aim to provide all of the mathematical foundations upon which the Internet is based. Instead, these cover only a partial panorama and the key principles. Volume 1 explores Internet engineering, while the supporting mathematics is covered in Volume 2. The chapters on mathematics complement those on the engineering episodes, and an effort has been made to make this work succinct, yet self-contained. Elements of information theory, algebraic coding theory, cryptography, Internet traffic, dynamics and control of Internet congestion, and queueing theory are discussed. In addition, stochastic networks, graph-theoretic algorithms, application of game theory to the Internet, Internet economics, data mining and knowledge discovery, and quantum computation, communication, and cryptography are also discussed. In order to study the structure and function of the Internet, only a basic knowledge of number theory, abstract algebra, matrices and determinants, graph theory, geometry, analysis, optimization theory, probability theory, and stochastic processes, is required. These mathematical disciplines are defined and developed in the books to the extent that is needed to develop and justify their application to Internet engineering. This book constitutes the refereed proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-17, held in Bangalore, India, in December 2007. The 33 revised full papers presented together with 8 invited papers were carefully reviewed and selected from 61 submissions. Among the subjects addressed are block codes, including list-decoding algorithms; algebra and codes: rings, fields, algebraic geometry codes; algebra: rings and fields, polynomials, permutations, lattices; cryptography: cryptanalysis and complexity; computational algebra: algebraic algorithms and transforms; sequences and boolean functions.

By combining algebraic and graphical approaches with practical business and personal finance applications, South-Western's FINANCIAL ALGEBRA, motivates high school students to explore algebraic thinking patterns and functions in a financial context. FINANCIAL ALGEBRA will help your students achieve success by offering an applications based learning approach incorporating Algebra I, Algebra II, and Geometry topics. Authors Gerver and Sgroi have spent more than 25 years working with students of all ability levels and they have found the most success when connecting math to the real world. FINANCIAL ALGEBRA encourages students to be actively involved in applying mathematical ideas to their everyday lives. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Algebraic Cryptanalysis bridges the gap between a course in cryptography, and being able to read the cryptanalytic literature. This book is divided into three parts: Part One covers the process of turning a cipher into a system of equations; Part Two covers finite field linear algebra; Part Three covers the solution of Polynomial Systems of Equations, with a survey of the methods used in practice, including SAT-solvers and the methods of Nicolas Courtois. Topics include: Analytic Combinatorics, and its application to cryptanalysis The equicomplexity of linear algebra operations Graph coloring Factoring integers via the quadratic sieve, with its applications to the cryptanalysis of RSA Algebraic Cryptanalysis is designed for advanced-level students in computer science and mathematics as a secondary text or reference book for self-guided study. This book is suitable for researchers in Applied Abstract Algebra or Algebraic Geometry who wish to find more applied topics or practitioners working for security and communications companies.

Bringing the material up to date to reflect modern applications, Algebraic Number Theory, Second Edition has been completely rewritten and reorganized to incorporate a new style, methodology, and presentation. This edition focuses on integral domains, ideals, and unique factorization in the first chapter; field extensions in the second chapter; and

With most services and products now being offered through digital communications, new challenges have emerged for information security specialists. A Multidisciplinary Introduction to Information Security presents a range of topics on the security, privacy, and safety of information and communication technology. It brings together methods in pure mathematics, computer and telecommunication sciences, and social sciences. The book begins with the cryptographic algorithms of the

Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA). It explains the mathematical reasoning behind public key cryptography and the properties of a cryptographic hash function before presenting the principles and examples of quantum cryptography. The text also describes the use of cryptographic primitives in the communication process, explains how a public key infrastructure can mitigate the problem of crypto-key distribution, and discusses the security problems of wireless network access. After examining past and present protection mechanisms in the global mobile telecommunication system, the book proposes a software engineering practice that prevents attacks and misuse of software. It then presents an evaluation method for ensuring security requirements of products and systems, covers methods and tools of digital forensics and computational forensics, and describes risk assessment as part of the larger activity of risk management. The final chapter focuses on information security from an organizational and people point of view. As our ways of communicating and doing business continue to shift, information security professionals must find answers to evolving issues. Offering a starting point for more advanced work in the field, this volume addresses various security and privacy problems and solutions related to the latest information and communication technology.

Applied AlgebraCodes, Ciphers and Discrete Algorithms, Second EditionCRC Press

Presenting the state of the art, the Handbook of Enumerative Combinatorics brings together the work of today's most prominent researchers. The contributors survey the methods of combinatorial enumeration along with the most frequent applications of these methods. This important new work is edited by Miklós Bóna of the University of Florida where he is a member of the Academy of Distinguished Teaching Scholars. He received his Ph.D. in mathematics at Massachusetts Institute of Technology in 1997. Miklós is the author of four books and more than 65 research articles, including the award-winning Combinatorics of Permutations. Miklós Bóna is an editor-in-chief for the Electronic Journal of Combinatorics and Series Editor of the Discrete Mathematics and Its Applications Series for CRC Press/Chapman and Hall. The first two chapters provide a comprehensive overview of the most frequently used methods in combinatorial enumeration, including algebraic, geometric, and analytic methods. These chapters survey generating functions, methods from linear algebra, partially ordered sets, polytopes, hyperplane arrangements, and matroids. Subsequent chapters illustrate applications of these methods for counting a wide array of objects. The contributors for this book represent an international spectrum of researchers with strong histories of results. The chapters are organized so readers advance from the more general ones, namely enumeration methods, towards the more specialized ones. Topics include coverage of asymptotic normality in enumeration, planar maps, graph enumeration, Young tableaux, unimodality, log-concavity, real zeros, asymptotic normality, trees, generalized Catalan paths, computerized enumeration schemes, enumeration of various graph classes, words, tilings, pattern avoidance, computer algebra, and parking functions. This book will be beneficial to a wide audience. It will appeal to experts on the topic interested in learning more about the finer points, readers interested in a systematic and organized treatment of the topic, and novices who are new to the field.

Discover the first unified treatment of today's most essentialinformation technologies— Compressing, Encrypting, andEncoding With identity theft, cybercrime, and digital file sharingproliferating in today's wired world, providing safe and accurateinformation transfers has become a paramount concern. The issuesand problems raised in this endeavor are encompassed within threedisciplines: cryptography, information theory, anderror-correction. As technology continues to develop, these fieldshave converged at a practical level, increasing the need for aunified treatment of these three cornerstones of the informationage. Stressing the interconnections of the disciplines, Cryptography,Information Theory, and Error-Correction offers a complete, yetaccessible account of the technologies shaping the 21st century.This book contains the most up-to-date, detailed, and balancedtreatment available on these subjects. The authors draw on theirexperience both in the classroom and in industry, giving the book'smaterial and presentation a unique real-world orientation. With its reader-friendly style and interdisciplinary emphasis,Cryptography, Information Theory, and Error-Correction serves asboth an admirable teaching text and a tool for self-learning. Thechapter structure allows for anyone with a high school mathematicseducation to gain a strong conceptual understanding, and provideshigher-level students with more mathematically advanced topics. Theauthors clearly map out paths through the book for readers of alllevels to maximize their learning. This book: Is suitable for courses in cryptography, information theory, ororror-correction as well as courses discussing all three areas Provides over 300 example problems with solutions Presents new and exciting algorithms adopted by industry Discusses potential applications in cell biology Details a new characterization of perfect secrecy Features in-depth coverage of linear feedback shift registers(LFSR), a staple of modern computing Follows a layered approach to facilitate discussion, withsummaries followed by more detailed explanations Provides a new perspective on the RSA algorithm Cryptography, Information Theory, and Error-Correction is anexcellent in-depth text for both graduate and undergraduatestudents of mathematics, computer science, and engineering. It isalso an authoritative overview for IT professionals, statisticians,mathematicians, computer scientists, electrical engineers,entrepreneurs, and the generally curious.

A Unified Account of Permutations in Modern CombinatoricsA 2006 CHOICE Outstanding Academic Title, the first edition of this bestseller was lauded for its detailed yet engaging treatment of permutations. Providing more than enough material for a one-semester course, Combinatorics of Permutations, Second Edition continues to clearly show the usefuln

This two-volume set on Mathematical Principles of the Internet provides a comprehensive overview of the mathematical principles of Internet engineering. The books do not aim to provide all of the mathematical foundations upon which the Internet is based. Instead, they cover a partial panorama and the key principles. Volume 1 explores Internet engineering, while the supporting mathematics is covered in Volume 2. The chapters on mathematics complement those on the engineering episodes, and an effort has been made to make this work succinct, yet self-contained. Elements of information theory, algebraic coding theory, cryptography, Internet traffic, dynamics and control of Internet congestion, and queueing theory are discussed. In addition, stochastic networks, graph-theoretic algorithms, application of game theory to the Internet, Internet economics, data mining and knowledge discovery, and quantum computation, communication, and cryptography are also discussed. In order to study the structure and function of the Internet, only a basic knowledge of number theory, abstract algebra, matrices and determinants, graph theory, geometry, analysis, optimization theory, probability theory, and stochastic processes, is required. These mathematical disciplines are defined and developed in the books to the extent that is needed to develop and justify their application to Internet engineering.

Poised to become the leading reference in the field, the Handbook of Finite Fields is exclusively devoted to the theory and applications of finite fields. More than 80 international contributors compile state-of-the-art research in this definitive handbook. Edited by two renowned researchers, the book uses a uniform style and format throughout and

Discover the Connections between Different Structures and FieldsDiscrete Structures and Their Interactions highlights the connections among various discrete structures, including graphs, directed graphs, hypergraphs, partial orders, finite topologies, and simplicial complexes. It also explores their relationships to classical areas of mathematics,

Winner of an Outstanding Academic Title Award from CHOICE Magazine Most available cryptology books primarily focus on either mathematics or history. Breaking this mold, Secret History: The Story of Cryptology gives a thorough yet accessible treatment of both the mathematics and history of cryptology. Requiring minimal mathematical prerequisites, the book presents the mathematics in sufficient detail and weaves the history throughout the chapters. In addition to the fascinating historical and political sides of cryptology, the author—a former Scholar-in-Residence at the U.S. National Security Agency (NSA) Center for Cryptologic History—includes interesting instances of codes and ciphers in crime, literature, music, and art. Following a mainly chronological development of concepts, the book focuses on classical cryptology in the first part. It covers Greek and Viking cryptography, the Vigenère cipher, the one-time pad, transposition ciphers, Jefferson's cipher wheel, the Playfair cipher, ADFGX, matrix encryption, World War II cipher systems (including a detailed examination of Enigma), and many other classical methods introduced before World War II. The second part of the book examines modern cryptology. The author looks at the work of Claude Shannon and the origin and current status of the NSA, including some of its Suite B algorithms such as elliptic curve cryptography and the Advanced Encryption Standard. He also details the controversy that surrounded the Data Encryption Standard and the early years of public key cryptography. The book not only provides the how-to of the Diffie-Hellman key exchange and RSA algorithm, but also covers many attacks on the latter. Additionally, it discusses Elgamal, digital signatures, PGP, and stream ciphers and explores future directions such as quantum cryptography and DNA computing. With numerous real-world examples and extensive references, this book skillfully balances the historical aspects of cryptology with its mathematical details. It provides readers with a sound foundation in this dynamic field.

From officially sanctioned, high-tech operations to budget spy cameras and cell phone video, this updated and expanded edition of a bestselling handbook reflects the rapid and significant growth of the surveillance industry. The Handbook of Surveillance Technologies, Third Edition is the only comprehensive work to chronicle the background and curre

This book constitutes the refereed proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-15, held in Toulouse, France, in May 2003. The 25 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 40 submissions. Among the subjects addressed are block codes; algebra and codes: rings, fields, and AG codes; cryptography; sequences; decoding algorithms; and algebra: constructions in algebra, Galois groups, differential algebra, and polynomials.

Developed from the author's popular graduate-level course, Computational Number Theory presents a complete treatment of number-theoretic algorithms. Avoiding advanced algebra, this self-contained text is designed for advanced undergraduate and beginning graduate students in engineering. It is also suitable for researchers new to the field and pract