Cryptanalysis Of Number Theoretic Ciphers Computational Mathematics By Samuel S Wagstaff Jr 2002 12 10

Cryptanalytic Attacks on RSA
Mathematics of Public Key Cryptography
Quantum Computational Number Theory
Algorithms and Theory of Computation Handbook, Second Edition, Volume 2
Cryptography and Computational Number Theory
Special Topics and Techniques
Stream Ciphers and Number Theory
A Course in Cryptography
Number Theory and Cryptography
A Course in Mathematical Cryptography
An Introduction to Mathematical Cryptography
Mathematical Principles of the Internet, Volume 1
The Guide to Secrecy From Ancient to Modern Times

Computational Cryptography
Number Theory and Cryptography
Engineering
Elliptic Curves
The Little Book of Bigger Primes
Cybercryptography: Applicable Cryptography for Cyberspace Security
Elementary Number Theory, Cryptography and Codes
Introduction to Cryptography with Open-Source Software
Number Theory and Cryptography, Second Edition
Algorithmic Cryptanalysis
Mathematical Principles of the Internet, Two Volume Set
Introduction to Modern Cryptography, Second Edition
Proceedings of the International Conference organized by the Stefan Banach International Mathematical Center Warsaw, Poland, September 11-15, 2000
The Mathematics of Ciphers
Computational Number Theory
A Handbook for the 21st Century
Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday
Techniques for Advanced Code Breaking
Modern Cryptanalysis
Public-Key Cryptography and Computational Number Theory
Handbook of Surveillance Technologies

Algorithms and Theory of Computation Handbook, Second Edition, Volume 1
General Concepts and Techniques
Stream Ciphers and Number Theory
American Mathematical Society Short Course, January 13-14, 2003, Baltimore, Maryland
Cryptanalysis of Number Theoretic Ciphers

AMIR JERAMIAH

Cryptanalytic Attacks on RSA Springer
Cryptography is ubiquitous and plays a key role in ensuring data secrecy and integrity as well as in securing computer systems more broadly. Introduction to Modern Cryptography provides a rigorous yet accessible treatment of this fascinating subject. The authors introduce the core principles of modern cryptography, with an emphasis on formal definitions, clear assumptions, and rigorous proofs of security. The book begins by focusing on private-key cryptography, including an extensive treatment of private-key encryption, message authentication codes, and hash functions. The authors also present design principles for widely used stream ciphers and block ciphers including RC4, DES, and AES, plus provide provable constructions

of stream ciphers and block ciphers from lower-level primitives. The second half of the book covers public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, and El Gamal cryptosystems (and others), followed by a thorough treatment of several standardized public-key encryption and digital signature schemes. Integrating a more practical perspective without sacrificing rigor, this widely anticipated Second Edition offers improved treatment of: Stream ciphers and block ciphers, including modes of operation and design principles Authenticated encryption and secure communication sessions Hash functions, including hash-function applications and design principles Attacks on poorly implemented cryptography, including attacks on chained-CBC encryption, padding-oracle attacks, and timing attacks The random-oracle model and its application to several standardized, widely used public-key encryption and signature schemes Elliptic-curve cryptography and associated standards such as DSA/ECDSA and DHIES/ECIES Containing updated exercises and worked examples, Introduction to Modern Cryptography, Second Edition can serve as a textbook for undergraduate- or graduate-level courses

in cryptography, a valuable reference for researchers and practitioners, or a general introduction suitable for self-study.
Mathematics of Public Key Cryptography
Springer Science & Business Media
This book is about the theory and practice of integer factorisation presented in a historic perspective. It describes about twenty algorithms for factoring and a dozen other number theory algorithms that support the factoring algorithms. Most algorithms are described both in words and in pseudocode to satisfy both number theorists and computer scientists. Each of the ten chapters begins with a concise summary of its contents. The book starts with a general explanation of why factoring integers is important. The next two chapters present number theory results that are relevant to factoring. Further on there is a chapter discussing, in particular, mechanical and electronic devices for factoring, as well as factoring using quantum physics and DNA molecules. Another chapter applies factoring to breaking certain cryptographic algorithms. Yet another chapter is devoted to practical vs. theoretical aspects of factoring. The book contains more than 100 examples illustrating various algorithms and theorems. It also contains more than 100 interesting

exercises to test the reader's understanding. Hints or answers are given for about a third of the exercises. The book concludes with a dozen suggestions of possible new methods for factoring integers. This book is written for readers who want to learn more about the best methods of factoring integers, many reasons for factoring, and some history of this fascinating subject. It can be read by anyone who has taken a first course in number theory.

Quantum Computational Number Theory John Wiley & Sons

Johannes Buchmann is internationally recognized as one of the leading figures in areas of computational number theory, cryptography and information security. He has published numerous scientific papers and books spanning a very wide spectrum of interests; besides R&D he also fulfilled lots of administrative tasks for instance building up and directing his research group CDC at Darmstadt, but he also served as the Dean of the Department of Computer Science at TU Darmstadt and then went on to become Vice President of the university for six years (2001-2007). This festschrift, published in honor of Johannes Buchmann on the occasion of his 60th birthday, contains contributions by some of his colleagues, former students and friends. The papers

give an overview of Johannes Buchmann's research interests, ranging from computational number theory and the hardness of cryptographic assumptions to more application-oriented topics such as privacy and hardware security. With this book we celebrate Johannes Buchmann's vision and achievements.
Algorithms and Theory of Computation Handbook, Second Edition, Volume 2 American Mathematical Soc.
This book provides a good introduction to the classical elementary number theory and the modern algorithmic number theory, and their applications in computing and information technology, including computer systems design, cryptography and network security. In this second edition proofs of many theorems have been provided, further additions and corrections were made.
Cryptography and Computational Number Theory Springer Science & Business Media
This book provides a comprehensive introduction to advanced topics in the computational and algorithmic aspects of number theory, focusing on applications in cryptography. Readers will learn to develop fast algorithms, including quantum algorithms, to solve various classic and modern number theoretic problems.

Key problems include prime number generation, primality testing, integer factorization, discrete logarithms, elliptic curve arithmetic, conjecture and numerical verification. The author discusses quantum algorithms for solving the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP), and the Elliptic Curve Discrete Logarithm Problem (ECDLP) and for attacking IFP, DLP and ECDLP based cryptographic systems. Chapters also cover various other quantum algorithms for Pell's equation, principal ideal, unit group, class group, Gauss sums, prime counting function, Riemann's hypothesis and the BSD conjecture. Quantum Computational Number Theory is self-contained and intended to be used either as a graduate text in computing, communications and mathematics, or as a basic reference in the related fields. Number theorists, cryptographers and professionals working in quantum computing, cryptography and network security will find this book a valuable asset.

Special Topics and Techniques Springer Science & Business Media

In this volume one finds basic techniques from algebra and number theory (e.g. congruences, unique factorization domains, finite fields, quadratic residues, primality tests, continued

fractions, etc.) which in recent years have proven to be extremely useful for applications to cryptography and coding theory. Both cryptography and codes have crucial applications in our daily lives, and they are described here, while the complexity problems that arise in implementing the related numerical algorithms are also taken into due account. Cryptography has been developed in great detail, both in its classical and more recent aspects. In particular public key cryptography is extensively discussed, the use of algebraic geometry, specifically of elliptic curves over finite fields, is illustrated, and a final chapter is devoted to quantum cryptography, which is the new frontier of the field. Coding theory is not discussed in full; however a chapter, sufficient for a good introduction to the subject, has been devoted to linear codes. Each chapter ends with several complements and with an extensive list of exercises, the solutions to most of which are included in the last chapter. Though the book contains advanced material, such as cryptography on elliptic curves, Goppa codes using algebraic curves over finite fields, and the recent AKS polynomial primality test, the authors' objective has been to keep the exposition as self-contained and elementary as possible. Therefore the

book will be useful to students and researchers, both in theoretical (e.g. mathematicians) and in applied sciences (e.g. physicists, engineers, computer scientists, etc.) seeking a friendly introduction to the important subjects treated here. The book will also be useful for teachers who intend to give courses on these topics.

Stream Ciphers and Number Theory

Walter de Gruyter GmbH & Co KG

This volume contains the refereed proceedings of the Workshop on Cryptography and Computational Number Theory, CCNT'99, which has been held in Singapore during the week of November 22-26, 1999. The workshop was organized by the Centre for Systems Security of the Na tional University of Singapore. We gratefully acknowledge the financial support from the Singapore National Science and Technology Board under the grant num ber RP960668/M. The idea for this workshop grew out of the recognition of the recent, rapid development in various areas of cryptography and computational number the ory. The event followed the concept of the research programs at such well-known research institutions as the Newton Institute (UK), Oberwolfach and Dagstuhl (Germany), and Luminy (France). Accordingly, there were only invited lectures at the

workshop with plenty of time for informal discussions. It was hoped and successfully achieved that the meeting would encourage and stimulate further research in information and computer security as well as in the design and implementation of number theoretic cryptosystems and other related areas. Another goal of the meeting was to stimulate collaboration and more active interaction between mathematicians, computer scientists, practical cryptographers and engineers in academia, industry and government.

A Course in Cryptography CRC Press

Like its bestselling predecessor, Elliptic Curves: Number Theory and Cryptography, Second Edition develops the theory of elliptic curves to provide a basis for both number theoretic and cryptographic applications. With additional exercises, this edition offers more comprehensive coverage of the fundamental theory, techniques, and applications of elliptic curves. New to the Second Edition Chapters on isogenies and hyperelliptic curves A discussion of alternative coordinate systems, such as projective, Jacobian, and Edwards coordinates, along with related computational issues A more complete treatment of the Weil and Tate–Lichtenbaum pairings Doud’s

analytic method for computing torsion on elliptic curves over Q An explanation of how to perform calculations with elliptic curves in several popular computer algebra systems Taking a basic approach to elliptic curves, this accessible book prepares readers to tackle more advanced problems in the field. It introduces elliptic curves over finite fields early in the text, before moving on to interesting applications, such as cryptography, factoring, and primality testing. The book also discusses the use of elliptic curves in Fermat's Last Theorem. Relevant abstract algebra material on group theory and fields can be found in the appendices.

Number Theory and Cryptography CRC Press
Papers presented by prominent contributors at a workshop on Number Theory and Cryptography, and the annual meeting of the Australian Mathematical Society.
A Course in Mathematical Cryptography Springer
This book provides a compact course in modern cryptography. The mathematical foundations in algebra, number theory and probability are presented with a focus on their cryptographic applications. The text provides rigorous definitions and follows the provable security approach. The most relevant cryptographic schemes are covered, including block ciphers, stream ciphers, hash

functions, message authentication codes, public-key encryption, key establishment, digital signatures and elliptic curves. The current developments in post-quantum cryptography are also explored, with separate chapters on quantum computing, lattice-based and code-based cryptosystems. Many examples, figures and exercises, as well as SageMath (Python) computer code, help the reader to understand the concepts and applications of modern cryptography. A special focus is on algebraic structures, which are used in many cryptographic constructions and also in post-quantum systems. The essential mathematics and the modern approach to cryptography and security prepare the reader for more advanced studies. The text requires only a first-year course in mathematics (calculus and linear algebra) and is also accessible to computer scientists and engineers. This book is suitable as a textbook for undergraduate and graduate courses in cryptography as well as for self-study.
An Introduction to Mathematical Cryptography Springer Science & Business Media
Algorithms and Theory of Computation Handbook, Second Edition: Special Topics and Techniques provides an up-to-date compendium of fundamental computer science topics and techniques. It also

illustrates how the topics and techniques come together to deliver efficient solutions to important practical problems. Along with updating and revising many of the existing chapters, this second edition contains more than 15 new chapters. This edition now covers self-stabilizing and pricing algorithms as well as the theories of privacy and anonymity, databases, computational games, and communication networks. It also discusses computational topology, natural language processing, and grid computing and explores applications in intensity-modulated radiation therapy, voting, DNA research, systems biology, and financial derivatives. This best-selling handbook continues to help computer professionals and engineers find significant information on various algorithmic topics. The expert contributors clearly define the terminology, present basic results and techniques, and offer a number of current references to the in-depth literature. They also provide a glimpse of the major research issues concerning the relevant topics.

Mathematical Principles of the Internet, Volume 1 CRC Press

The Proceedings contain twenty selected, refereed contributions arising from the International Conference on Public-Key Cryptography and

Computational Number Theory held in Warsaw, Poland, on September 11-15, 2000. The conference, attended by eightyfive mathematicians from eleven countries, was organized by the Stefan Banach International Mathematical Center. This volume contains articles from leading experts in the world on cryptography and computational number theory, providing an account of the state of research in a wide variety of topics related to the conference theme. It is dedicated to the memory of the Polish mathematicians Marian Rejewski (1905-1980), Jerzy Róøycki (1909-1942) and Henryk Zygalski (1907-1978), who deciphered the military version of the famous Enigma in December 1932 – January 1933. A noteworthy feature of the volume is a foreword written by Andrew Odlyzko on the progress in cryptography from Enigma time until now.
The Guide to Secrecy From Ancient to Modern Times CRC Press
Primality Testing and Integer Factorization in Public-Key Cryptography introduces various algorithms for primality testing and integer factorization, with their applications in public-key cryptography and information security. More specifically, this book explores basic concepts and results in number theory in Chapter 1. Chapter 2 discusses various algorithms for primality

testing and prime number generation, with an emphasis on the Miller-Rabin probabilistic test, the Goldwasser-Kilian and Atkin-Morain elliptic curve tests, and the Agrawal-Kayal-Saxena deterministic test for primality. Chapter 3 introduces various algorithms, particularly the Elliptic Curve Method (ECM), the Quadratic Sieve (QS) and the Number Field Sieve (NFS) for integer factorization. This chapter also discusses some other computational problems that are related to factoring, such as the square root problem, the discrete logarithm problem and the quadratic residuosity problem.
Computational Cryptography CRC Press
Group theoretic problems have propelled scientific achievements across a wide range of fields, including mathematics, physics, chemistry, and the life sciences. Many cryptographic constructions exploit the computational hardness of group theoretical problems, and the area is viewed as a potential source of quantum-resilient cryptographic primitives
Number Theory and Cryptography Cambridge University Press
This introduction to cryptography employs a programming-oriented approach to study the most important cryptographic schemes in current use and the main cryptanalytic attacks against them.

Discussion of the theoretical aspects, emphasizing precise security definitions based on methodological tools such as complexity and randomness, and of the mathematical aspects, with emphasis on number-theoretic algorithms and their applications to cryptography and cryptanalysis, is integrated with the programming approach, thus providing implementations of the algorithms and schemes as well as examples of realistic size. A distinctive feature of the author's approach is the use of Maple as a programming environment in which not just the cryptographic primitives but also the most important cryptographic schemes are implemented following the recommendations of standards bodies such as NIST, with many of the known cryptanalytic attacks implemented as well. The purpose of the Maple implementations is to let the reader experiment and learn, and for this reason the author includes numerous examples. The book discusses important recent subjects such as homomorphic encryption, identity-based cryptography and elliptic curve cryptography. The algorithms and schemes which are treated in detail and implemented in Maple include AES and modes of operation, CMAC, GCM/GMAC, SHA-256,

HMAC, RSA, Rabin, Elgamal, Paillier, Cocks IBE, DSA and ECDSA. In addition, some recently introduced schemes enjoying strong security properties, such as RSA-OAEP, Rabin-SAEP, Cramer--Shoup, and PSS, are also discussed and implemented. On the cryptanalysis side, Maple implementations and examples are used to discuss many important algorithms, including birthday and man-in-the-middle attacks, integer factorization algorithms such as Pollard's rho and the quadratic sieve, and discrete log algorithms such as baby-step giant-step, Pollard's rho, Pohlig--Hellman and the index calculus method. This textbook is suitable for advanced undergraduate and graduate students of computer science, engineering and mathematics, satisfying the requirements of various types of courses: a basic introductory course; a theoretically oriented course whose focus is on the precise definition of security concepts and on cryptographic schemes with reductionist security proofs; a practice-oriented course requiring little mathematical background and with an emphasis on applications; or a mathematically advanced course addressed to students with a stronger mathematical background. The main prerequisite is a basic knowledge of linear

algebra and elementary calculus, and while some knowledge of probability and abstract algebra would be helpful, it is not essential because the book includes the necessary background from these subjects and, furthermore, explores the number-theoretic material in detail. The book is also a comprehensive reference and is suitable for self-study by practitioners and programmers.

Engineering John Wiley & Sons

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

Elliptic Curves Birkhäuser

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

The Little Book of Bigger Primes Cambridge University Press

This is the unique book on cross-fertilisations between stream ciphers and number theory. It systematically and comprehensively covers known connections between the two areas that are available only in research papers. Some parts of this book consist of new research results that are not available elsewhere. In addition to exercises, over thirty research problems are presented in this book. In this revised edition almost every chapter was updated, and some chapters were completely rewritten. It is useful as a textbook for a graduate course on the subject, as well as a reference book for researchers in related fields. · Unique book on interactions of stream ciphers and number theory. · Research monograph with many results not available elsewhere. · A revised edition with the most recent advances in this subject. · Over thirty research problems for stimulating interactions between the two areas. · Written by leading researchers in stream ciphers and number theory.

Cybercryptography: Applicable Cryptography for Cyberspace Security

Erman Yılmaz

This book is almost entirely concerned with stream ciphers, concentrating on a particular mathematical model for such ciphers which are called additive natural stream ciphers. These ciphers use a natural sequence generator to produce a

periodic keystream. Full definitions of these concepts are given in Chapter 2. This book focuses on keystream sequences which can be analysed using number theory. It turns out that a great deal of information can be deducted about the cryptographic properties of many classes of sequences by applying the terminology and theorems of number theory. These connections can be explicitly made by describing three kinds of bridges between stream ciphering problems and number theory problems. A detailed summary of these ideas is given in the introductory Chapter 1. Many results in the book are new, and over seventy percent of these results described in this book are based on recent research results.

Elementary Number Theory, Cryptography and Codes Elsevier

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.