Cryptography A Very Short Introduction Very Short Introductions

AN UNCONVENTIONAL, FUN WAY TO MASTER THE BASICS OF CRYPTOGRAPHY Cryptography is not just for specialists. Now every wireless message, wireless phone call, online transaction, and email is encrypted at one end and decrypted at the other. “Crypto” is part of the job description for network designers, network engineers, and telecom developers. If you need cryptography basics—but dread the thick tomes that are your only other option—help is at hand. Cryptography Demystified puts the fundamentals into a 35-module, learn-by-doing package that’s actually fun to use. You must read this book if— * You prefer your simplifications from an expert who understands the complexities * 6 years of success as a short course for students and professionals works for you * you enjoy hearing the phrase “nothing to memorize” * ecommerce, email, network security, or wireless communications is part of your bailiwick * cracking cryptography means a jump up the career ladder * the words “public-key cryptography,” “channel-based cryptography,” and “prime numbers” pique your interest * best-practices cryptography is the only secure way for you—and your company—to go One of the most complex subjects in Information Technology, cryptography gets its due in this down-to-earth, self-teaching tutorial—the first to make the basics of the science truly accessible.

This text introduces cryptography, from its earliest roots to cryptosystems used today for secure online communication. Beginning with classical ciphers and their cryptanalysis, this book proceeds to focus on modern public key cryptosystems such as Diffie-Hellman, ElGamal, RSA, and elliptic curve cryptography with an analysis of vulnerabilities of these systems and underlying mathematical issues such as factorization algorithms. Specialized topics such as zero knowledge proofs, cryptographic voting, coding theory, and new research are covered in the final section of this book. Aimed at undergraduate students, this book contains a large selection of problems, ranging from straightforward to difficult, and can be used as a textbook for classes as well as self-study. Requiring only a solid grounding in basic mathematics, this book will also appeal to advanced high school students and amateur mathematicians interested in this fascinating and topical subject.

This Very Short Introduction provides a clear and informative introduction to the science of codebreaking, and its explosive impact on modern society. Taking the reader through the actual processes of developing codes and deciphering them, the book explains what algorithms do, how they are used, the risks associated with using them, and why governments should be concerned. Written in a fluid and lively style to appeal to the non-mathematical reader, this makes for fascinating reading.

The collapse of communism was one of the most defining moments of the twentieth century. This Very Short Introduction examines the history behind the political, economic, and social structures of communism as an ideology.

Over the past sixty years, the spectacular growth of the technologies associated with the computer is visible for all to see and experience. Yet, the science underpinning this technology is less visible and little understood outside the professional computer science community. As a scientific discipline, computer science stands alongside the likes of molecular biology and cognitive science as one of the most significant new sciences of the post Second World War era. In this Very Short Introduction, Subrata Dasgupta sheds light on these lesser known areas and considers the conceptual basis of computer science. Discussing algorithms, programming, and sequential and parallel processing, he considers emerging modern ideas such as biological computing and cognitive modelling, challenging the idea of computer science as a science of the artificial. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

A Comprehensive Introduction

Cryptography For Dummies

Cryptography, Engineering and Economics

Egyptian Myth: A Very Short Introduction

Understanding Bitcoin

Cryptography, in particular public-key cryptography, has emerged in the last 20 years as an important discipline that is not only the subject of an enormous amount of research, but provides the foundation for information security in many applications. Standards are emerging to meet the demands for cryptographic protection in most areas of data communications. Public-key cryptographic techniques are now in widespread use, especially in the financial services industry, in the public sector, and by individuals for their personal privacy, such as in electronic mail. This Handbook will serve as a valuable reference for the novice as well as for the expert who needs a wider scope of coverage within the area of cryptography. It is a necessary and timely guide for professionals who practice the art of cryptography. The Handbook of Applied Cryptography provides a treatment that is multifunctional: It serves as an introduction to the more practical aspects of both conventional and public-key cryptography It is a valuable source of the latest techniques and algorithms for the serious practitioner It provides an integrated treatment of the field, while still presenting each major topic as a self-contained unit It provides a mathematical treatment to accompany practical discussions It contains enough abstraction to be a valuable reference for theoreticians while containing enough detail to actually allow implementation of the algorithms discussed Now in its third printing, this is the definitive cryptography reference that the novice as well as experienced developers, designers, researchers, engineers, computer scientists, and mathematicians alike will use.

"As gripping as a good thriller." --The Washington Post Unpack the science of secrecy and discover the methods behind cryptography--the encoding and decoding of information--in this clear and easy-to-understand young adult adaptation of the national bestseller that's perfect for this age of WikiLeaks, the Sony hack, and other events that reveal the extent to which our technology is never quite as secure as we want to believe. Coders and codebreakers alike will be fascinated by history's most mesmerizing stories of intrigue and cunning--from Julius Caesar and his Caeser cipher to the Allies' use of the Enigma machine to decode German messages during World War II. Accessible, compelling, and timely, The Code Book is sure to make readers see the past--and the future--in a whole new way. "Singh's power of explaining complex ideas is as dazzling as ever." --The Guardian

An authoritative introduction to the exciting new technologies of digital money Bitcoin and Cryptocurrency Technologies

provides a comprehensive introduction to the revolutionary yet often misunderstood new technologies of digital currency. Whether you are a student, software developer, tech entrepreneur, or researcher in computer science, this authoritative and self-contained book tells you everything you need to know about the new global money for the Internet age. How do Bitcoin and its block chain actually work? How secure are your bitcoins? How anonymous are their users? Can cryptocurrencies be regulated? These are some of the many questions this book answers. It begins by tracing the history and development of Bitcoin and cryptocurrencies, and then gives the conceptual and practical foundations you need to engineer secure software that interacts with the Bitcoin network as well as to integrate ideas from Bitcoin into your own projects. Topics include decentralization, mining, the politics of Bitcoin, altcoins and the cryptocurrency ecosystem, the future of Bitcoin, and more. An essential introduction to the new technologies of digital currency Covers the history and mechanics of Bitcoin and the block chain, security, decentralization, anonymity, politics and regulation, altcoins, and much more Features an accompanying website that includes instructional videos for each chapter, homework problems, programming assignments, and lecture slides Also suitable for use with the authors' Coursera online course Electronic solutions manual (available only to professors)

Cipher and decipher codes: transposition and polyalphabetical ciphers, famous codes, typewriter and telephone codes, codes that use playing cards, knots, and swizzle sticks . . . even invisible writing and sending messages through space. 45 diagrams.

Cryptography: A Very Short IntroductionOxford Paperbacks

An Introduction to Cryptography

Cryptography Decrypted

Codes: An Introduction to Information Communication and Cryptography

Preparing for the Day When Quantum Computing Breaks Today's Crypto

Handbook of Applied Cryptography

Many people do not realise that mathematics provides the foundation for the devices we use to handle information in the modern world. Most of those who do know probably think that the parts of mathematics involvedare quite 'cl- sical', such as Fourier analysis and di?erential equations. In fact, a great deal of the mathematical background is part of what used to be called 'pure' ma- ematics, indicating that it was created in order to deal with problems that originated within mathematics itself. It has taken many years for mathema- cians to come to terms with this situation, and some of them are still not entirely happy about it. Thisbookisanintegratedintroductionto Coding.Bythis Imeanreplacing symbolic information, such as a sequence of bits or a message written in a naturallanguage,byanother messageusing (possibly) di?erentsymbols.There are three main reasons for doing this: Economy (data compression), Reliability (correction of errors), and Security (cryptography). I have tried to cover each of these three areas in su?cient depth so that the reader can grasp the basic problems and go on to more advanced study. The mathematical theory is introduced in a way that enables the basic problems to bestatedcarefully,butwithoutunnecessaryabstraction.Theprerequisites(sets andfunctions,matrices,?niteprobability)shouldbefamiliartoanyonewhohas taken a standard course in mathematical methods or discrete mathematics. A course in elementary abstract algebra and/or number theory would be helpful, but the book contains the essential facts, and readers without this background should be able to understand what is going on. vi Thereareafewplaceswherereferenceismadetocomputeralgebrasystems.

Teeth are a vital component of vertebrate anatomy and a fundamental part of the fossil record. It was the evolution of teeth, associated with predation, that drove the evolution of the wide array of fish, amphibians, reptiles, and then mammals. Peter S. Ungar looks at how, without teeth, none of these developments could have occurred.

Number theory is the branch of mathematics primarily concerned with the counting numbers, especially primes. It dates back to the ancient Greeks, but today it has great practical importance in cryptography, from credit card security to national defence. This book introduces the main areas of number theory, and some of its most interesting problems.

Continuing a bestselling tradition, An Introduction to Cryptography, Second Edition provides a solid foundation in cryptographic concepts that features all of the requisite background material on number theory and algorithmic complexity as well as a historical look at the field. With numerous additions and restructured material, this edition

This textbook provides an introduction to the mathematics on which modern cryptology is based. It covers not only public key cryptography, the glamorous component of modern cryptology, but also pays considerable attention to secret key cryptography, its workhorse in practice. Modern cryptology has been described as the science of the integrity of information, covering all aspects like confidentiality, authenticity and non-repudiation and also including the protocols required for achieving these aims. In both theory and practice it requires notions and constructions from three major disciplines: computer science, electronic engineering and mathematics. Within mathematics, group theory, the theory of finite fields, and elementary number theory as well as some topics not normally covered in courses in algebra, such as the theory of Boolean functions and Shannon theory, are involved. Although essentially self-contained, a degree of mathematical maturity on the part of the reader is assumed, corresponding to his or her background in computer science or engineering. Algebra for Cryptologists is a textbook for an introductory course in cryptography or an upper undergraduate course in algebra, or for self-study in preparation for postgraduate study in cryptology.

Communism: A Very Short Introduction

Understanding Cryptography

Introduction to Modern Cryptography

Colonial Latin American Literature: A Very Short Introduction

Algebra for Cryptologists

Modern statistics is very different from the dry and dusty discipline of the popular imagination. In its place is an exciting subject which uses deep theory and powerful software tools to shed light and enable understanding. And it sheds this light on all aspects of our lives, enabling astronomers to explore the origins of the universe, archaeologists to investigate ancient civilisations, governments to understand how to benefit and improve society, and businesses to learn how best to provide goods and services. Aimed at readers with no prior mathematical knowledge, this Very Short Introduction explores and explains how statistics work, and how we can decipher them. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

This Very Short Introduction traces the history and cultural impact of the elements on

humankind, and examines why people have long sought to identify the substances around them. Looking beyond the Periodic Table, the author examines our relationship with matter, from the uncomplicated vision of the Greek philosophers, who believed there were four elements - earth, air, fire, and water - to the work of modern-day scientists in creating elements such as hassium and meitnerium. Packed with anecdotes, The Elements is a highly engaging and entertaining exploration of the fundamental question: what is the world made from? ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

How many possible sudoku puzzles are there? In the lottery, what is the chance that two winning balls have consecutive numbers? Who invented Pascal's triangle? (it was not Pascal) Combinatorics, the branch of mathematics concerned with selecting, arranging, and listing or counting collections of objects, works to answer all these questions. Dating back some 3000 years, and initially consisting mainly of the study of permutations and combinations, its scope has broadened to include topics such as graph theory, partitions of numbers, block designs, design of codes, and latin squares. In this Very Short Introduction Robin Wilson gives an overview of the field and its applications in mathematics and computer theory, considering problems from the shortest routes covering certain stops to the minimum number of colours needed to colour a map with different colours for neighbouring countries. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

Cryptography is the most effective way to achieve data securityand is essential to e-commerce activities such as online shopping,stock trading, and banking This invaluable introduction to the basics of encryption coverseverything from the terminology used in the field to specifictechnologies to the pros and cons of different implementations Discusses specific technologies that incorporate cryptographyin their design, such as authentication methods, wirelessencryption, e-commerce, and smart cards Based entirely on real-world issues and situations, thematerial provides instructions for already available technologiesthat readers can put to work immediately Expert author Chey Cobb is retired from the NRO, where she helda Top Secret security clearance, instructed employees of the CIAand NSA on computer security and helped develop the computersecurity policies used by all U.S. intelligence agencies

Hieroglyphs were far more than a language. They were an omnipresent and all-powerful force in communicating the messages of ancient Egyptian culture for over three thousand years; used as monumental art, as a means of identifying Egyptianness, and for rarefied communication with the gods. In this exciting new study, Penelope Wilson explores the cultural significance of the script with an emphasis on previously neglected areas such as cryptography, the continuing decipherment into modern times, and examines the powerful fascination hieroglyphs still hold for us today. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

Superconductivity: A Very Short Introduction

Cryptography: A Very Short Introduction

Codes, Ciphers and Secret Writing

An Introduction to Mathematical Cryptography

Serious Cryptography

Now the most used texbook for introductory cryptography courses in both mathematics and computer science, the Third Edition builds upon previous editions by offering several new sections, topics, and exercises. The authors present the core principles of modern cryptography, with emphasis on formal definitions, rigorous proofs of security.

The massive disorder and economic ruin following the Second World War inevitably predetermined the scope and intensity of the Cold War. But why did it last so long? And what impact did it have on the United States, the Soviet Union, Europe, and the Third World? Finally, how did it affect the broader history of the second half of the twentieth century - what were the human and financial costs? This Very Short Introduction provides a clear and stimulating interpretive overview of the Cold War, one that will both invite debate and encourage deeper investigation. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-

sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

Lie detection, offender profiling, jury selection, insanity in the law, predicting the risk of re-offending , the minds of serial killers and many other topics that fill news and fiction are all aspects of the rapidly developing area of scientific psychology broadly known as Forensic Psychology. Forensic Psychology: A Very Short Introduction discusses all the aspects of psychology that are relevant to the legal and criminal process as a whole. It includes explanations of criminal behaviour and criminality, including the role of mental disorder in crime, and discusses how forensic psychology contributes to helping investigate the crime and catching the perpetrators. It also explains how psychologists provide guidance to all those involved in civil and criminal court proceedings, including both the police and the accused, and what expert testimony can be provided by a psychologist about the offender at the trial. Finally, David Canter examines how forensic psychology is used, particularly in prisons, to help in the management, treatment and rehabilitation of offenders, once they have been convicted. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

In a startling reinterpretation of the evidence, Stillman Drake advances the hypothesis that Galileo's trial and condemnation by the Inquisition was caused not by his defiance of the Church, but by the hostility of contemporary philosophers. Galileo's own beautifully lucid arguments are used to show how his scientific method was utterly divorced from the Aristotelian approach to physics in that it was based on a search not for causes but for laws. Galileo's method was of overwhelming significance for the development of modern physics, and led to a final parting of the ways between science and philosophy.

ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

A vivid account of the literary culture of the Spanish-speaking Americas from the time of Columbus to Latin American Independence, this Very Short Introduction explores the origins of Latin American literature in Spanish and tells the story of how Spanish literary language developed and flourished in the New World. A leading scholar of colonial Latin American literature, Rolena Adorno examines the writings that debated the justice of the Spanish conquests, described the novelties of New World nature, expressed the creativity of Hispanic baroque culture in epic, lyric, and satirical poetry, and anticipated Latin American Independence. The works of Spanish, creole, and Amerindian authors highlighted here, including Bartolom? de las Casas, Felipe Guaman Poma, Sor Juana In?s de la Cruz, and Andr?s Bello, have been chosen for the merits of their writings, their participation in the larger literary and cultural debates of their times, and their resonance among readers today. About the Series: Combining authority with wit, accessibility, and style, Very Short Introductions offer an introduction to some of life's most interesting topics. Written by experts for the newcomer, they demonstrate the finest contemporary thinking about the central problems and issues in hundreds of key topics, from philosophy to Freud, quantum theory to Islam.

The Cold War: A Very Short Introduction

Theory and Practice, Third Edition

A Very Short Introduction

Making, Breaking Codes

Statistics: A Very Short Introduction

This unique book explains the basic issues of classical and modern cryptography, and provides a self contained essential mathematical background in number theory, abstract algebra, and probability--with surveys of relevant parts of complexity theory and other things. A user-friendly, down-to-earth tone presents concretely motivated introductions to these topics. More detailed chapter topics include simple ciphers; applying ideas from probability; substitutions, transpositions, permutations; modern symmetric ciphers; the integers; prime numbers; powers and roots modulo primes; powers and roots for composite moduli; weakly multiplicative functions; quadratic symbols, quadratic reciprocity; pseudoprimes; groups; sketches of protocols; rings, fields, polynomials; cyclotomic polynomials, primitive roots; pseudo-random number generators; proofs concerning pseudoprimality; factorization attacks finite fields; and elliptic curves. For personnel in computer security, system administration, and information systems.

Superconductivity is one of the most exciting areas of research in physics today. Outlining the history of its discovery, and the race to understand its many mysterious phenomena, this Very Short Introduction also explores the deep implications of the theory, and its potential to revolutionize the physics and technology of the future.

Discover Bitcoin, the cryptocurrency that has the finance worldbuzzing Bitcoin is arguably one of the biggest developments in financesince the advent of fiat currency. With UnderstandingBitcoin, expert author Pedro Franco provides financeprofessionals with a complete technical guide and resource to thecryptography, engineering and economic development of Bitcoin andother cryptocurrencies. This comprehensive, yet accessible workfully explores the supporting economic realities and technologicaladvances of Bitcoin, and presents positive and negative argumentsfrom various economic schools regarding its continuedviability. This authoritative text provides a step-by-step description ofhow Bitcoin works, starting with public key cryptography and movingon to explain transaction processing,

the blockchain and miningtechnologies. This vital resource reviews Bitcoin from the broaderperspective of digital currencies and explores historical attemptsat cryptographic currencies. Bitcoin is, after all, not just adigital currency; it's a modern approach to the secure transfer ofvalue using cryptography. This book is a detailed guide to what itis, how it works, and how it just may jumpstart a change in the waydigital value changes hands. Understand how Bitcoin works, and the technology behind it Delve into the economics of Bitcoin, and its impact on thefinancial industry Discover alt-coins and other available cryptocurrencies Explore the ideas behind Bitcoin 2.0 technologies Learn transaction protocols, micropayment channels, atomiccross-chain trading, and more Bitcoin challenges the basic assumption under which the currentfinancial system rests: that currencies are issued by centralgovernments, and their supply is managed by central banks. To fullyunderstand this revolutionary technology, UnderstandingBitcoin is a uniquely complete, reader-friendly guide.

This practical guide to modern encryption breaks down the fundamental mathematical concepts at the heart of cryptography without shying away from meaty discussions of how they work. You'll learn about authenticated encryption, secure randomness, hash functions, block ciphers, and public-key techniques such as RSA and elliptic curve cryptography. You'll also learn: - Key concepts in cryptography, such as computational security, attacker models, and forward secrecy - The strengths and limitations of the TLS protocol behind HTTPS secure websites - Quantum computation and post-quantum cryptography - About various vulnerabilities by examining numerous code examples and use cases - How to choose the best algorithm or protocol and ask vendors the right questions Each chapter includes a discussion of common implementation mistakes using real-world examples and details what could go wrong and how to avoid these pitfalls. Whether you're a seasoned practitioner or a beginner looking to dive into the field, Serious Cryptography will provide a complete survey of modern encryption and its applications.

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.

Number Theory

The Elements: A Very Short Introduction

A Practical Introduction to Modern Encryption

Introduction to Cryptography with Mathematical Foundations and Computer Implementations

Cryptography is now ubiquitous - moving beyond the traditional environments, such as government communications and banking systems, we see cryptographic techniques realized in Web browsers, e-mail programs, cell phones, manufacturing systems, embedded software, smart buildings, cars, and even medical implants. Today's designers need a comprehensive understanding of applied cryptography. After an introduction to cryptography and data security, the authors explain the main techniques in modern cryptography, with chapters addressing stream ciphers, the Data Encryption Standard (DES) and 3DES, the Advanced Encryption Standard (AES), block ciphers, the RSA cryptosystem, public-key cryptosystems based on the discrete logarithm problem, elliptic-curve cryptography (ECC), digital signatures, hash functions, Message Authentication Codes (MACs), and methods for key establishment, including certificates and public-key infrastructure (PKI). Throughout the book, the authors focus on communicating the essentials and keeping the mathematics to a minimum, and they move quickly from explaining the foundations to describing practical implementations, including recent topics such as lightweight ciphers for RFIDs and mobile devices, and current key-length recommendations. The authors have considerable experience teaching applied cryptography to engineering and computer science students and to professionals, and they make extensive use of examples, problems, and chapter reviews, while the book's website offers slides, projects and links to further resources. This is a suitable textbook for graduate and advanced undergraduate courses and also for self-study by engineers.

THE LEGACY... First introduced in 1995, Cryptography: Theory and Practice garnered enormous praise and popularity, and soon became the standard textbook for cryptography courses around the world. The second edition was equally embraced, and enjoys status as a perennial bestseller. Now in its third edition, this authoritative text continues to provide a solid foundation for future breakthroughs in cryptography. WHY A THIRD EDITION? The art and science of cryptography has been evolving for thousands

of years. Now, with unprecedented amounts of information circling the globe, we must be prepared to face new threats and employ new encryption schemes on an ongoing basis. This edition updates relevant chapters with the latest advances and includes seven additional chapters covering: Pseudorandom bit generation in cryptography Entity authentication, including schemes built from primitives and special purpose "zero-knowledge" schemes Key establishment including key distribution and protocols for key agreement, both with a greater emphasis on security models and proofs Public key infrastructure, including identity-based cryptography Secret sharing schemes Multicast security, including broadcast encryption and copyright protection THE RESULT... Providing mathematical background in a "just-in-time" fashion, informal descriptions of cryptosystems along with more precise pseudocode, and a host of numerical examples and exercises, Cryptography: Theory and Practice, Third Edition offers comprehensive, in-depth treatment of the methods and protocols that are vital to safeguarding the mind-boggling amount of information circulating around the world.

A clear, comprehensible, and practical guide to the essentials of computer cryptography, from Caesar's Cipher through modern-day public key. Cryptographic capabilities like detecting imposters and stopping eavesdropping are thoroughly illustrated with easy-to-understand analogies, visuals, and historical sidebars. The student needs little or no background in cryptography to read Cryptography Decrypted. Nor does it require technical or mathematical expertise. But for those with some understanding of the subject, this book is comprehensive enough to solidify knowledge of computer cryptography and challenge those who wish to explore the high-level math appendix.

Quantum Theory is the most revolutionary discovery in physics since Newton. This book gives a lucid, exciting, and accessible account of the surprising and counterintuitive ideas that shape our understanding of the sub-atomic world. It does not disguise the problems of interpretation that still remain unsettled 75 years after the initial discoveries. The main text makes no use of equations, but there is a Mathematical Appendix for those desiring stronger fare. Uncertainty, probabilistic physics, complementarity, the problematic character of measurement, and decoherence are among the many topics discussed. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

The complex world of Egyptian myth is clearly illuminated in this fascinating new approach to ancient Egypt. Geraldine Pinch explores the cultural and historical background behind a wide variety of sources and objects, from Cleopatra's Needle and Tutankhamun's golden statue, to a story on papyrus of the gods misbehaving. What did they mean, and how have they been interpreted? The reader is taken on an exciting journey through the distant past, and shown how myths of deities such as Isis and Osiris influenced contemporary culture and have become part of our cultural heritage. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

Artificial Intelligence: A Very Short Introduction

A Textbook for Students and Practitioners

Ideology: A Very Short Introduction

The Code Book: The Secrets Behind Codebreaking

Numbers: A Very Short Introduction

In this Very Short Introduction Peter M. Higgins presents an overview of the number types featured in modern science and mathematics. Providing a non-technical account, he explores the evolution of the modern number system, examines the fascinating role of primes, and explains their role in contemporary cryptography.

Ideology is one of the most controversial terms in the political vocabulary, exciting both revulsion and inspiration. This book examines the reasons for those views, and explains why ideologies deserve respect as a major form of political thinking. It investigates the centrality of ideology both as a political phenomenon and as an organizing framework of political thought and action. It explores the changing understandings of ideology as a concept, and the arguments of the main ideologies. By employing the latest insights from a range of disciplines, the reader is introduced to the vitality and force of a crucial resource at the disposal of societies, through which sense and purpose is assigned to the political world. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

The applications of Artificial Intelligence lie all around us; in our homes, schools and offices, in our cinemas, in art galleries and - not least - on the Internet. The results of Artificial Intelligence have been invaluable to biologists, psychologists, and linguists in helping to understand the processes of memory, learning, and language from a fresh angle. As a concept, Artificial Intelligence has fuelled and sharpened the philosophical debates concerning the nature of the mind, intelligence, and the uniqueness of human beings. In this Very Short Introduction , Margaret A. Boden reviews the philosophical and technological challenges raised by Artificial Intelligence, considering whether programs could ever be really intelligent, creative or even conscious, and shows how the pursuit of Artificial Intelligence has helped us to appreciate how human and animal minds are possible. ABOUT THE SERIES: The Very Short Introductions series from Oxford University Press contains hundreds of titles in almost every subject area. These pocket-sized books are the perfect way to get ahead in a new subject quickly. Our expert authors combine facts, analysis, perspective, new ideas, and enthusiasm to make interesting and challenging topics highly readable.

Will your organization be protected the day a quantum computer breaks encryption on the internet?

Computer encryption is vital for protecting users, data, and infrastructure in the digital age. Using traditional computing, even common desktop encryption could take decades for specialized 'crackers' to break and government and infrastructure-grade encryption would take billions of times longer. In light of these facts, it may seem that today's computer cryptography is a rock-solid way to safeguard everything from online passwords to the backbone of the entire internet. Unfortunately, many current cryptographic methods will soon be obsolete. In 2016, the National Institute of Standards and Technology (NIST) predicted that quantum computers will soon be able to break the most popular forms of public key cryptography. The encryption technologies we rely on every day—HTTPS, TLS, WiFi protection, VPNs, cryptocurrencies, PKI, digital certificates, smartcards, and most two-factor authentication—will be virtually useless. . . unless you prepare. Cryptography Apocalypse is a crucial resource for every IT and InfoSec professional for preparing for the coming quantum-computing revolution. Post-quantum crypto algorithms are already a reality, but implementation will take significant time and computing power. This practical guide helps IT leaders and implementers make the appropriate decisions today to meet the challenges of tomorrow. This important book: Gives a simple quantum mechanics primer Explains how quantum computing will break current cryptography Offers practical advice for preparing for a post-quantum world Presents the latest information on new cryptographic methods Describes the appropriate steps leaders must take to implement existing solutions to guard against quantum-computer security threats Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto is a must-have guide for anyone in the InfoSec world who needs to know if their security is ready for the day crypto break and how to fix it.

Discusses the basic components of computers; how increasingly miniature parts have led to products, applications, and networks that solve problems; the issues that increased connectivity has produced; and some of the emerging technologies in the field.

Hieroglyphs: A Very Short Introduction
Cryptography
Quantum Theory: A Very Short Introduction
Forensic Psychology: A Very Short Introduction
Combinatorics

This self-contained introduction to modern cryptography emphasizes the mathematics behind the theory of public key cryptosystems and digital signature schemes. The book focuses on these key topics while developing the mathematical tools needed for the construction and security analysis of diverse cryptosystems. Only basic linear algebra is required of the reader; techniques from algebra, number theory, and probability are introduced and developed as required. This text provides an ideal introduction for mathematics and computer science students to the mathematical foundations of modern cryptography. The book includes an extensive bibliography and index; supplementary materials are available online. The book covers a variety of topics that are considered central to mathematical cryptography. Key topics include: classical cryptographic constructions, such as Diffie Hellmann key exchange, discrete logarithm-based cryptosystems, the RSA cryptosystem, and digital signatures; fundamental mathematical tools for cryptography, including primality testing, factorization algorithms, probability theory, information theory, and collision algorithms; an in-depth treatment of important cryptographic innovations, such as elliptic curves, elliptic curve and pairing-based cryptography, lattices, lattice-based cryptography, and the NTRU cryptosystem. The second edition of An Introduction to Mathematical Cryptography includes a significant revision of the material on digital signatures, including an earlier introduction to RSA, Elgamal, and DSA signatures, and new material on lattice-based signatures and rejection sampling. Many sections have been rewritten or expanded for clarity, especially in the chapters on information theory, elliptic curves, and lattices, and the chapter of additional topics has been expanded to include sections on digital cash and homomorphic encryption. Numerous new exercises have been included.

Cryptography Apocalypse
Teeth: A Very Short Introduction
Computer Science: A Very Short Introduction
Galileo: A Very Short Introduction
Bitcoin and Cryptocurrency Technologies