La Steganografia Da Erodoto A Bin Laden: Viaggio Attraverso Le Tecniche Elusive Della Comunicazione

Mai, come oggi, lo sviluppo tecnologico è stato così rapido e pervasivo. L'uso del pc e di internet condiziona in modo pregnante le abitudini, le idee, le tendenze e le prospettive degli utenti che si confrontano quotidianamente con gli stessi. La questione non è tuttavia se bisogna o meno essere digitali, ma piuttosto come dobbiamo esserlo: in quale forma e con quali garanzie per la nostra tranquillità e sicurezza. Di qui, la necessità di sviluppare una sensibilità al digitale in grado di assicurare la progressiva costruzione di un senso critico nei confronti del fenomeno digitale nel suo complesso: capirne gli impatti, i vantaggi e, soprattutto, i pericoli. È questo l'obiettivo del presente volume, dedicato al tema della sicurezza informatica nella gestione sia dei documenti telematici sia dei rapporti sociali, al fine di offrire al lettore una nuova chiave di lettura nella comprensione dei meccanismi e delle vulnerabilità degli strumenti informatici, nonché nella predisposizione delle misure di sicurezza idonee a proteggere la propria riservatezza da possibili attacchi informatici.
This book constitutes the refereed contest reports of the 1st International Workshop, VAAM 2014, held in Stockholm, Sweden, in August 2014. The 10 revised full papers presented were carefully reviewed and selected from 13 submissions. The aim of this workshop is to provide an overview of state of the art methods for audience measurements in retail and Digital Signage, end-users attraction, and stimulate the creation of appropriate benchmark dataset to be used as reference for the development of novel audience measurement algorithms. Papers are invited under the following topics: demographics and modeling consumer behaviour.
"Fascinating and insightful. . . . I cannot recall a book that has made me think more about the nature of thinking." -- Richard C. Lewontin Harvard University Everyone knows that optical illusions trick us because of the way we see. Now scientists have discovered that cognitive illusions, a set of biases deeply embedded in the human mind, can actually distort the way we think. In Inevitable Illusions, distinguished cognitive researcher Massimo Piattelli-Palmarini takes us on a provocative, challenging, and thoroughly entertaining exploration of the games our minds play. He opens the doors onto the newly charted realm of the cognitive unconscious to reveal the full range of illusions, showing how they inhibit our ability to reason--no matter what our educational background or IQ. Inevitable Illusions is stimulating, eye-opening food for thought.
I Greci: Una storia greca. Pt. 1. Formazione (fino al VI secolo a.C.) Pt. 2. Definizione (VI-IV secolo a.C.) Pt. 3. Transformazioni (IV secolo a. C.-II secolo d.C.)
Introduction to Cryptography
Inevitable Illusions
A Concept in Art Theory
The Changing Energy Landscape in the Gulf
INTERNET E LE SUE INSICUREZZE
Principles and Applications

This book covers key concepts of cryptography, from encryption and digital signatures to cryptographic protocols, presenting techniques and protocols for key exchange, user ID, electronic elections and digital cash. Advanced topics include bit security of one-way functions and computationally perfect pseudorandom bit generators. Assuming no special background in mathematics, it includes chapter-ending exercises and the necessary algebra, number theory and probability theory in the appendix. This edition offers new material including a complete description of the AES, a section on cryptographic hash functions, new

material on random oracle proofs, and a new section on public-key encryption schemes that are provably secure against adaptively-chosen-ciphertext attacks.
First published in 1997, this is the comprehensive and irrefutable proof of the flesh-and-blood gods who created us genetically in their own image. This interventionist solution identifies them as the builders of the Pyramids, Sphinx and other ancient sites. Up-to-date evidence is that the gods were real and came from within the Solar System.
Roma. Per il giovane avvocato Jonathan Marcus è quasi un ritorno a casa. È ancora vivo in lui il ricordo del periodo trascorso in Italia per completare una ricerca sulla controversa figura di Flavio Giuseppe, lo storico ebreo che, durante le guerre giudaiche, si era alleato con Tito, tradendo il suo stesso popolo. Adesso Jonathan è in città per difendere un cliente dall'accusa di aver illegalmente acquistato due frammenti della Forma Urbis - un'enorme mappa in marmo della Roma imperiale - raffiguranti una sezione del Colosseo. E, con sua grande sorpresa, in quei reperti Jonathan individua un riferimento proprio a Flavio Giuseppe e all'«errore» di Tito... Ostia. Dopo aver ricevuto una soffiata, il capitano dei carabinieri Jacopo Profeta perquisisce un magazzino abbandonato e, all'interno di una colonna romana, scopre il corpo imbalsamato di una donna. Sulla pelle è tatuata una frase enigmatica - La vittoria nell'ombelico del mondo - e tutt'intorno sono sparse varie pagine manoscritte di un'opera di Flavio Giuseppe. Profeta intuisce di essere caduto in una trappola e, pochi secondi prima che il magazzino venga distrutto da un'esplosione, riesce a fuggire, portando in salvo alcune pergamene... Gerusalemme. Sal?h al-D?n, nipote del Gran Muft?, sta clandestinamente scavando sotto la Cupola della Roccia. Il suo obiettivo è localizzare la camera segreta dove Flavio Giuseppe ha nascosto una reliquia leggendaria. Il Monte del Tempio, infatti, è l'ombelico del mondo... Tre uomini, un segreto, una missione: trovare la Menorah.
Idea of the Temple of Painting
The Science of Secrecy from Ancient Egypt to Quantum Cryptography
Judicial Applications of Artificial Intelligence
Versteckte Botschaften (TELEPOLIS)
The Resistible Rise of Anarcho-Capitalism
In Praise of Scribes
La mente, il corpo e i loro enigmi

If you've ever made a secure purchase with your credit card over the Internet, then you have seen cryptography, or "crypto", in action. From Stephen Levy—the author who made "hackers" a household word—comes this account of a revolution that is already affecting every citizen in the twenty-first century. Crypto tells the inside story of how a group of "crypto rebels"—nerds and visionaries turned freedom fighters—teamed up with corporate interests to beat Big Brother and ensure our privacy on the Internet. Levy's history of one of the most controversial and important topics of the digital age reads like the best futuristic fiction.
Hacklog, Volume 1: Anonimato è il primo dei nostri corsi pensati per l'apprendimento della Sicurezza Informatica ed Ethical Hacking. È stato ideato per far in modo che tutti, sia i professionisti che i principianti, riescano ad apprendere i meccanismi e i metodi che

stanno alla base dell'Anonimato. Abbiamo scelto di iniziare con l'Anonimato appunto perché è un tema molto attuale ed applicabile da chiunque, che non richiede particolari abilità e che si può applicare in ogni realtà, sia privata che aziendale. Attenzione: il corso Hacklog, Volume 1: Anonimato prevede l'uso del Sistema Operativo Debian GNU/Linux. Se non hai mai utilizzato questo Sistema Operativo, ti consigliamo caldamente di seguire il breve corso introduttivo che lo riguarda. Gratuito, ovviamente. Nel corso imparerai a utilizzare metodi di anonimato semplici e complessi, a cifrare le tue informazioni in rete e i tuoi dati nel computer, a navigare nel Deep Web in maniera sicura e a riconoscere i rischi che si corrono navigando in Internet. Conoscerai metodi reali, applicati sia dai professionisti che dai malavitosi, per nascondere le tracce in rete; lo scopo finale di questo corso è quello di fare chiarezza sugli strumenti a disposizione di tutti, liberamente in rete. Con il percorso che ti consigliamo, sarai in grado anche di comandare un intero Sistema Operativo a base GNU/Linux tramite una distribuzione Debian, attualmente la più popolare nei computer ad uso casalingo e server. Ciò aiuterà a formarti in vista dei prossimi volumi e anche nella vita professionale di un esperto del settore Informatico.

This book, speaks loud and clear about the meaning of American Patriotism. It is my sincere belief, that if we are to remain a free, and strong democracy, as one Nation under God, we must without the slightest doubt, "Pledge Allegiance to America." We must stand united, determined to identify and expose the "Anti-Americans" within our country, who have total disregard for the labors of Our Founding. Fathers. The enemy exists within our society as both, individuals and as well funded organizations, constantly "chipping away" at our Declaration of Independence and Constitution, with fierce determination to change our form of government. They are intent on eliminating any reference to GOD, regardless of how, when and where, knowing that the majority of our citizens are of the Judeo/Christian belief. We are Christians and Jews, and people of every faith, who believe in God, who will unite to resist the "enemies," whose purpose it is, to deny us of our freedom and strip us of our freedom to worship God as we desire. As united believers in God, we must make certain that our lawmakers do not succumb to the demands of the "enemy within" and their constant "rabble-rousing" methods, aimed at the destruction of Our Heritage, Our Culture and Our Form of Government.

Storie delle guerre nascoste

I Greci: Una storia greca (3 v.)

Cryptology and Computational Number Theory

La battaglia di Platea
How the Code Rebels Beat the Government--Saving Privacy in the Digital Age
Decrypted Secrets

In-depth study of the culture, history and art of Ancient Greece with particular emphasis on its influence on today's society.

In today's extensively wired world, cryptology is vital for guarding communication channels, databases, and software from intruders. Increased processing and communications speed, rapidly broadening access and multiplying storage capacity tend to make systems less secure over time, and security becomes a race against the relentless creativity of the unscrupulous. The revised and extended third edition of this classic reference work on cryptology offers a wealth of new technical and biographical details. The book presupposes only elementary mathematical knowledge. Spiced with exciting, amusing, and sometimes personal accounts from the history of cryptology, it will interest general a broad readership.

This work has been selected by scholars as being culturally important, and is part of the knowledge base of civilization as we know it. This work was reproduced from the original artifact, and remains as true to the original work as possible. Therefore, you will see the original copyright references, library stamps (as most of these works have been housed in our most important libraries around the world), and other notations in the work. This work is in the public domain in the United States of America, and possibly other nations. Within the United States, you may freely copy and distribute this work, as no entity (individual or corporate) has a copyright on the body of the work. As a reproduction of a historical artifact, this work may contain missing or blurred pages, poor pictures, errant marks, etc. Scholars believe, and we concur, that this work is important enough to be preserved, reproduced, and made generally available to the public. We appreciate your support of the preservation process, and thank you for being an important part of keeping this knowledge alive and relevant.

La Steganografia Da Erodoto a Bin Laden: Viaggio Attraverso Le Tecniche Elusive Della Comunicazione

Quaderni del Bobbio n. 4 anno 2012-2013

Hacklog Volume 1 Anonimato

First International Workshop, VAAM 2014, Stockholm, Sweden, August 24, 2014. Revised Selected Papers

Sistemi di cifratura. Storia, principi, algoritmi e tecniche di crittografia

Strategic Implications

I Greci

"An English translation of the Renaissance treatise on painting by the Milanese artist Giovan Paolo Lomazzo (1538-1592). Drawing on a wide range of influences, including Leonardo's legacy, Neoplatonic cosmology, and the occult, Lomazzo affirms the development of every

artist's unique, expressive style or maniera"--Provided by publisher.
La Steganografia Da Erodoto a Bin Laden: Viaggio Attraverso Le Tecniche Elusive Della ComunicazioneIndependently Published
L'alchimista Thomas Vaughan rimane misteriosamente ucciso in un incidente nel suo laboratorio di Albury. Sarà compito del giovane Ulysses Unt sbrogliare l'intricata matassa della sua morte per conto della Royal Society.
I Delitti della Royal Society
Methods and Maxims of Cryptology
Crypto
Underwater Dogs
I servizi segreti di Venezia
Rivista di approfondimento culturale dell'IIS "Bobbio" di Carignano
The Code Book

Extreme fluctuations in oil prices (such as the dramatic fall from mid-2014 into 2015) raise important strategic questions for both importers and exporters. In this volume, specialists from the US, the Middle East, Europe and Asia examine the rapidly evolving dynamic in the energy landscape, including renewable and nuclear power, challenges to producers including the shale revolution, and legal issues. Each chapter provides in-depth analysis and clear policy recommendations.

In their new work research collective Ippolita provides a critical investigation of the inner workings of Facebook as a model for all commercial social networks. Facebook is an extraordinary platform that can generate large profit from the daily activities of its users. Facebook may appear to be a form of free entertainment and self-promotion but in reality its users are working for the development of a new type of market where they trade relationships. As users of social media we have willingly submitted to a vast social, economic and cultural experiment. By critically examining the theories of Californian right-libertarians, Ippolita show the thread con- necting Facebook to the European Pirate Parties, WikiLeaks and beyond. An important task today is to reverse the logic of radical transparency and apply it to the technologies we use on a daily basis.

Spie, spionaggio e operazioni sotto copertura dall'Antica Grecia alla Guerra fredda di Michael Rank Spie e reti spionistiche nella storia Dal premiato autore de I dieci grandi generali della storia, ecco un nuovo ed eccitante libro riguardante le più grandi spie della storia e come le loro azioni di spionaggio sotto copertura abbiano modificato il costo della storia. Che si sia trattato di Enea il Tattico che diede vita alla scienza militare occidentale, o di Francis Walsingham, capo dello spionaggio della Regina Elisabetta I che sventò numerosi tentativi di assassinio e mise in piedi una rete spionistica internazionale all'alba del colonialismo europeo, o di Richard Sorge, l'ubriacona spia tedesca per conto dei russi, la cui intercettazione di informazioni militari dell'Asse impedì la sconfitta dell'esercito russo durante la Seconda Guerra Mondiale, ognuna di queste spie ha rivestito un ruolo fondamentale nella società moderna. Questo libro prenderà in esame la vita e il periodo in cui vissero le dieci più grandi spie, o reti spionistiche, della storia. Alcune di esse godono di fama leggendaria come Mata Hari, l'esotica ballerina e cortigiana vissuta durante la Prima Guerra Mondiale che frequentò così tante camere da letto assieme a ufficiali francesi e tedeschi che non potè non diventare un'agente

segreto doppiogiochista. Altre spie agirono per puri motivi ideologici come George Koval, la spia nata nello Iowa e che fornì segreti nucleari americani all'Unione Sovietica, accelerando in questo modo di anni il programma nucleare russo e rendendo possibile la corsa agli armamenti durante la Guerra fredda. Altre hanno stimolato livelli di quasi adorazione pseudoreligiosa come Nathan Hale, la spia della Guerra di indipendenza americana, che ebbe una carriera molto breve, ma diventò il primo martire americano e simbolo nazionale molto sentito. Qualunque siano state le motivazioni per condurre az

I sette fuochi del tempio

Die faszinierende Geschichte der Steganografie

In the Facebook Aquarium

Strumenti, soggetti e contesti

Il Caso Vaughan

Teoria, algoritmi e protocolli

Manuale sulla Sicurezza Informatica e Hacking Etico

L'intento di questo libro è quello di fornire delle solide basi di studio della steganografia. Esso rappresenta un robusto punto di partenza a livello conoscitivo, che offre una visione globale della steganografia antica e moderna, fornendo chiare e semplici spiegazioni delle tecniche steganografiche utilizzate al giorno d'oggi con relativi esempi di applicazione pratica. Un libro, insomma, che si propone di essere letto da una vasta ed eterogenea utenza e non esclusivamente da lettori di nicchia esperti del settore. Ma che cos'è la steganografia? La steganografia è una tecnica elusiva della comunicazione che consente a due o più individui di comunicare tra loro senza che una terza persona si avveda del fatto che una qualsiasi comunicazione stia avvenendo. Nel passato, sono state utilizzare innumerevoli tecniche, dall'inchiostro invisibile, alle tavolette di cera, al metodo acrostico, per arrivare a veri e propri tatuaggi nascosti sotto i capelli. Oggi la steganografia consente di nascondere all'interno di file digitali, immagini o suoni che siano, ogni tipo di file o di messaggio segreto. Perché proprio in questo consiste la tecnica moderna: si prende un'immagine o un file audio e si estraggono alcune unità grafiche minime che la compongono, ossia alcuni pixel nel caso delle immagini digitali, e le si sostituiscono con dei dati, in genere lettere di testo, che comporranno il messaggio che si vuol far passare. Dal momento che certe immagini sono composte da milioni di pixel, la sostituzione di soltanto alcuni di essi non sarà apprezzabile ad occhio nudo ma, per leggere il messaggio, servirà uno dei tanti programmi reperibili online. Il risultato è stupefacente: l'immagine originale e quella in cui è stato iniettato un altro file contenente un messaggio di testo, messe a confronto, sono perfettamente identiche, sia in termini di risoluzione grafica sia per quello che concerne il peso, ossia lo spazio occupato sulla memoria di massa.

This edition contains an introduction giving the necessary background and setting Book III in the context of the Iliad as a whole, the Greek text, explanatory notes and a vocabulary.

The judiciary is in the early stages of a transformation in which AI (Artificial Intelligence) technology will help to make the judicial process faster, cheaper, and more predictable without compromising the integrity of judges' discretionary reasoning. Judicial decision-making is an area of daunting complexity, where highly sophisticated legal expertise merges with cognitive and emotional competence. How can AI contribute to a process that encompasses such a wide range of knowledge, judgment, and experience? Rather than aiming at the impossible dream (or nightmare) of building an automatic judge, AI research has had two more practical goals: producing tools to support judicial activities, including programs for intelligent document assembly, case retrieval, and support for discretionary decision-making; and developing new analytical tools for understanding and modeling the judicial process, such as case-based reasoning and formal models of dialectics, argumentation, and negotiation. Judges, squeezed between tightening budgets and increasing demands for justice, are desperately trying to maintain the quality of their decision-making process while coping with time and resource limitations. Flexible AI tools for decision support may promote uniformity and efficiency in judicial practice, while supporting rational judicial discretion. Similarly, AI may promote flexibility, efficiency and accuracy in other judicial tasks, such as drafting various judicial documents. The contributions in this volume exemplify some of the directions that the AI transformation of the judiciary will take.

On Education and Non-Education of Early Modern Artists

The Mathematical Theory of Communication

Scientific Investment Analysis

Gods of the New Millenium

What America Means to Me

Storie di spie, spionaggio e operazioni sotto copertura dall'antica Grecia alla Guerra fredda

storia, cultura, arte, società

A state-of-the art treatment offering scientific procedures that require no special scientific expertise, Murphy's unusual new book provides a unified framework for the evaluation of investment assets and strategies--a particularly useful way to conduct security analysis, portfolio management, and trading, and for other general investment applications. Murphy covers practical methods for credit analysis and demonstrates ways to value equities using a pro forma model that integrates forecasting with the detailed use of financial statements and footnotes. He also explains international portfolio management within the context of a changed trading, tax, and regulatory environment. This is an important resource for investment analysts, researchers, advisers, and brokers, and an excellent

text for students in certain advanced university courses.
Die Fantasie der Menschen beim Schmuggeln geheimer Daten ist nahezu grenzenlos: Ein im Schuhabsatz versteckter Mikrofilm, das Tarnen einer Spionagenachricht als Zigarrenbestellung, das Schreiben mit Geheimtinte, das Verbergen von Daten in harmlosen Bildern und Zinken- Codes – dies sind nur einige von unzähligen Beispielen für versteckte Botschaften. Fachleute bezeichnen dieses Verbergen und Schmuggeln von Nachrichten als "Steganografie". Die Steganografie hat eine faszinierende Geschichte. Bevor die Verschlüsselungstechnik Ende des 19. Jahrhunderts deutliche Fortschritte machte, war das Verstecken einer Nachricht oft wirkungsvoller als das Verschlüsseln. Auch heute noch wendet nahezu jeder Mensch steganografische Techniken an – meist ohne es zu wissen. Nach dem großen Erfolg der ersten Auflage erzählt Klaus Schmeh in seiner überarbeiteten Neuausgabe die faszinierende Geschichte dieser versteckten Botschaften, die von den alten Griechen und ihren Wachstafeln über Geheimoperationen im Kalten Krieg bis zu den Computerhackern der Gegenwart reicht. Er nimmt den Leser mit auf eine furiose Reise durch eine Kulturgeschichte voller Intrigen, Verbrechen und Kriege, in der jedoch auch die Falschspielerei oder der Betrug in der Klassenarbeit eine wichtige Rolle spielen. Die Telepolis-Bücher basieren auf dem Themenkreis des Online-Magazins Telepolis. Die Reihe schaut wie das Online-Magazin über den Tellerrand eingefahrener Abgrenzungen hinaus und erörtert Phänomene der digitalen Kultur und der Wissensgesellschaft. Telepolis finden Sie unter www.telepolis.de
The exuberant, exhilarating photographs of dogs underwater that have become a sensation From the water's surface, it's a simple exercise: a dog's leap, a splash, and then a wet head surfacing with a ball, triumphant. But beneath the water is a chaotic ballet of bared teeth and bubbles, paddling paws, fur and ears billowing in the currents. From leaping Lab to diving Dachshund, the water is where a dog's distinct personality shines through; some lounge in the current, paddling slowly, but others arch their bodies to cut through the water with the focus and determination of a shark. In more than eighty portraits, award-winning pet photographer and animal rights activist Seth Casteel captures new sides of our old friends with vibrant underwater photography that makes it impossible to look away. Each image bubbles with exuberance and life, a striking reminder that even in the most loveable and domesticated dog, there are more primal forces at work. In Underwater Dogs, Seth Casteel gives playful and energetic testament to the rough-and-tumble joy that our dogs bring into our lives.
Video Analytics for Audience Measurement

Idea
Kos
saggi di filosofia
Homer: Iliad III
Scientific Proof of Flesh and Blood Gods
Non solo enigma

La Seconda guerra mondiale si è combattuta anche su un fronte più nascosto, tra coloro che volevano rendere illeggibili al nemico i propri messaggi e coloro che cercavano in ogni modo di svelarli. La storia è rimasta segreta per quasi trent'anni dalla fine del conflitto e una grande mole di informazioni è stata resa disponibile soltanto negli anni '90 del Novecento grazie alle leggi sulla trasparenza entrate in vigore negli Stati Uniti e nel Regno Unito, i Freedom of Information Act. I crittologi non furono alle prese solo con Enigma, la macchina cifrante tedesca, che Alan Turing contribuì a decriptare. La storia è costellata di sconfitte e trionfi, dei contributi di decine di menti geniali e del duro lavoro di un esercito di collaboratori, in gran parte donne. L'uso estensivo di macchine per cifrare e per decifrare è stato uno degli elementi decisivi per la nascita dell'informatica moderna.

Fin dall'antichità si sono ideati metodi sempre più sicuri per occultare il reale significato di determinati segni e rendere un messaggio offuscato, in modo che non sia comprensibile a persone non autorizzate a leggerlo. Obiettivo di questo volume è presentare il linguaggio della crittografia moderna e dei vari aspetti collegati. Dopo un'introduzione storica che consente di acquisire dimestichezza con la terminologia e i problemi della disciplina, il testo tratta alcuni sistemi crittografici simmetrici (DES, AES) e asimmetrici. In particolare sono descritti gli algoritmi necessari per comprendere e implementare i crittosistemi e alcuni dei protocolli crittografici oggi più utilizzati. Vengono inoltre illustrati gli aspetti fondamentali della crittografia probabilistica. La completezza della trattazione che illustra tutti gli aspetti coinvolti (storia, matematica, algoritmi, applicazioni, complessità computazionale) rende questo volume adatto non solo agli studenti universitari di Informatica, Matematica e Ingegneria informatica, ma anche a chiunque sia interessato a conoscere il linguaggio della crittografia moderna. L'intero testo è integrato da numerosi esempi, diagrammi e figure, mentre materiali di complemento, tra cui diversi esempi "pratici" (svolti utilizzando il software Pari/Gp) sono disponibili online all'indirizzo www.hoeplieditore.it/66902.

Scientific knowledge grows at a phenomenal pace--but few books have had as lasting an impact or played as important a role in our modern world as The Mathematical Theory of Communication, published originally as a paper on communication theory more than fifty years ago. Republished in book form shortly thereafter, it has since gone through four hardcover and sixteen paperback printings. It is a revolutionary work, astounding in its foresight and contemporaneity. The University of Illinois Press is pleased and honored to issue this commemorative reprinting of a classic.

Manuale di crittografia

How Mistakes of Reason Rule Our Minds

rivista di cultura e storia delle scienze mediche, naturali e umane diretta da Massimo Piattelli Palmarini

I servizi segreti di Venezia. Spionaggio e controspionaggio ai tempi della Serenissima

The Artist as Reader

De Incertitudine Et Vanitate Scientiarum Liber

Based on the history of knowledge, the contributions to this volume elucidate various

aspects of how, in the early modern period, artists ' education, knowledge, reading and libraries were related to the ways in which they presented themselves

In his first book since the bestselling Fermat's Enigma, Simon Singh offers the first sweeping history of encryption, tracing its evolution and revealing the dramatic effects codes have had on wars, nations, and individual lives. From Mary, Queen of Scots, trapped by her own code, to the Navajo Code Talkers who helped the Allies win World War II, to the incredible (and incredibly simple) logisitical breakthrough that made Internet commerce secure, The Code Book tells the story of the most powerful intellectual weapon ever known: secrecy. Throughout the text are clear technical and mathematical explanations, and portraits of the remarkable personalities who wrote and broke the world's most difficult codes. Accessible, compelling, and remarkably far-reaching, this book will forever alter your view of history and what drives it. It will also make you wonder how private that e-mail you just sent really is.

In the past dozen or so years, cryptology and computational number theory have become increasingly intertwined. Because the primary cryptologic application of number theory is the apparent intractability of certain computations, these two fields could part in the future and again go their separate ways. But for now, their union is continuing to bring ferment and rapid change in both subjects. This book contains the proceedings of an AMS Short Course in Cryptology and Computational Number Theory, held in August 1989 during the Joint Mathematics Meetings in Boulder, Colorado. These eight papers by six of the top experts in the field will provide readers with a thorough introduction to some of the principal advances in cryptology and computational number theory over the past fifteen years. In addition to an extensive introductory article, the book contains articles on primality testing, discrete logarithms, integer factoring, knapsack cryptosystems, pseudorandom number generators, the theoretical underpinnings of cryptology, and other number theory-based cryptosystems. Requiring only background in elementary number theory, this book is aimed at nonexperts, including graduate students and advanced undergraduates in mathematics and computer science.