Crittografia Nel Paese Delle Meraviglie

The narrator tries to reconstruct the life and death of Krasnov, a Russian anticommunist, and his role in the history of the city of Trieste

This book constitutes the refereed proceedings of the 17th Annual International Cryptology Conference, CRYPTO'97, held in Santa Barbara, California, USA, in August 1997 under the sponsorship of the International Association for Cryptologic Research (IACR). The volume presents 35 revised full papers selected from 160 submissions received. Also included are two invited presentations. The papers are organized in sections on complexity theory, cryptographic primitives, lattice-based cryptography, digital signatures, cryptanalysis of public-key cryptosystems, information theory, elliptic curve implementation, number-theoretic systems, distributed cryptography, hash functions, cryptanalysis of secret-key cryptosystems.

A survey of pseudorandomness, the theory of efficiently generating objects that look random despite being constructed using little or no randomness. This theory has significance for areas in computer science and mathematics, including computational complexity, algorithms, cryptography, combinatorics, communications, and additive number theory.

There's a common belief that cyberspace cannot be regulated-that it is, in its very essence, immune from the government's (or anyone else's) control.Code argues that this belief is wrong. It is not in the nature of cyberspace to be unregulable; cyberspace has no "nature." It only has code-the software and hardware that make cyberspace what it is. That code can create a place of freedom-as the original architecture of the Net did-or a place of exquisitely oppressive control.If we miss this point, then we will miss how cyberspace is changing. Under the influence of commerce, cyberpsace is becoming a highly regulable space, where our behavior is much more tightly controlled than in real space.But that's not inevitable either. We can-we must-choose what kind of cyberspace we want and what freedoms we will guarantee. These choices are all about architecture: about what kind of code will govern cyberspace, and who will control it. In this realm, code is the most significant form of law, and it is up to lawyers, policymakers, and especially citizens to decide what values that code embodies.

Predicated on the notion that mathematics has been a growing source of aesthetic inspiration in culture, this volume celebrates where the two intermesh. It is a meditation on the performances and cultural events, all mathematics-related, performed in Bologna in 2004, is dedicated to all those who are curious about mathematics, but also more generally about theatre, cinema, literature, arts and science. Thanks to the DVD, one can readers can relive various events through the voices and the images of the participants.

In apparenza con Gesù i conti non tornano mai. Dal vignaiolo che dà la stessa paga all'operaio della prima e dell'ultima ora, alla richiesta di perdonare settanta volte sette. Scrive in prefazione il certosino e matematico Dom Jacques Dupont: «Il Dio di Gesù Cristo non sa né addizionare, né sottrarre, tanto meno dividere. Forse, sa soltanto moltiplicare, e sempre per l'infinito».I numeri possono portarci molto lontano. Ma per andare all'essenziale Enzo Romeo ci invita a compitare una tabellina evangelica. Perché i Vangeli sono come i numeri primi in matematica. Capaci di illuminare e dare senso a ogni gesto della vita umana.

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.

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.

This tutorial volume is based on a summer school on cryptology and data security held in Aarhus, Denmark, in July 1998. The ten revised lectures presented are devoted to core topics in modern cryptololgy. In accordance with the educational objectives of the school, elementary introductions are provided to central topics, various examples are given of the problems encountered, and this is supplemented with solutions, open problems, and reference to further reading. The resulting book is ideally suited as an up-to-date introductory text for students and IT professionals interested in modern cryptology.

"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.

As a beginning graduate student, I recall being frustrated by a general lack of acces sible sources from which I could learn about (theoretical) cryptography. I remember wondering: why aren't there more books presenting the basics of cryptography at an introductory level? Jumping ahead almost a decade later, as a faculty member my graduate students now ask me: what is the best resource for learning about (various topics in) cryptography? This monograph is intended to serve as an answer to these 1 questions — at least with regard to digital signature schemes. Given the above motivation, this book has been written with a beginninggraduate student in mind: a student who is potentially interested in doing research in the ?eld of cryptography, and who has taken an introductory course on the subject, but is not sure where to turn next. Though intended primarily for that audience, I hope that advanced graduate students and researchers will ?nd the book useful as well. In addition to covering various constructions of digital signature schemes in a uni?ed framework, this text also serves as a compendium of various "folklore" results that are, perhaps, not as well known as they should be. This book could also serve as a textbook for a graduate seminar on advanced cryptography; in such a class, I expect the entire book could be covered at a leisurely pace in one semester with perhaps some time left over for excursions into related topics.

Originally published in 1985, One Chord Wonders was the first full-length study of the glory years of British punk. The book argues that one of punk's most significant political achievements was to expose the operations of power in the British entertainment industries as they were thrown into confusion by the sound and the fury of musicians and fans. Through a detailed examination of the conditions under which punk emerged and then declined, Dave Laing develops a view of the music as both complex and contradictory. Special attention is paid to the relationship between punk and the music industry of the late 1970s, in particular the political economy of the independent record companies through which much of punk was distributed. Using examples from a wide range of bands, individual chapters use the techniques of semiology to consider the radical approach to naming in punk (from Johnny Rotten to Poly Styrene), the instrumental and vocal sound of the music, and its visual images. The concluding chapter critically examines various theoretical explanations of the punk phenomenon, including the class origins of its protagonists and the influential view that punk represented the latest in a line of British youth “subcultures.” There is also a chronology of the punk era, plus discographies and a bibliography.

Crittografia nel Paese delle MeraviglieSpringer Science & Business Media

Steps forward in mathematics often reverberate in other scientific disciplines, and give rise to innovative conceptual developments or find surprising technological applications. This volume brings to the forefront some of the proponents of the mathematics of the twentieth century, who have put at our disposal new and powerful instruments for investigating the reality around us. The portraits present people who have impressive charisma and wide-ranging cultural interests, who are passionate about defending the importance of their own research, are sensitive to beauty, and attentive to the social and political problems of their times. What we have sought to document is mathematics’ central position in the culture of our day. Space has been made not only for the great mathematicians but also for literary texts, including contributions by two apparent interlopers, Robert Musil and Raymond Queneau, for whom mathematical concepts represented a valuable tool for resolving the struggle between ‘soul and precision.’

The latest Web app attacks and countermeasures from world-renowned practitioners Protect your Web applications from malicious attacks by mastering the weapons and thought processes of today's hacker. Written by recognized security practitioners and thought leaders, Hacking Exposed Web Applications, Third Edition is fully updated to cover new infiltration methods and countermeasures. Find out how to reinforce authentication and authorization, plug holes in Firefox and IE, reinforce against injection attacks, and secure Web 2.0 features. Integrating security into the Web development lifecycle (SDL) and into the broader enterprise information security program is also covered in this comprehensive resource. Get full details on the hacker's footprinting, scanning, and profiling tools, including SHODAN, Maltego, and OWASP DirBuster See new exploits of popular platforms like Sun Java System Web Server and Oracle WebLogic in operation Understand how attackers defeat commonly used Web authentication technologies See how real-world session attacks leak sensitive data and how to fortify your applications Learn the most devastating methods used in today's hacks, including SQL injection, XSS, XSRF, phishing, and XML injection techniques Find and fix vulnerabilities in ASP.NET, PHP, and J2EE execution environments Safety deploy XML, social networking, cloud computing, and Web 2.0 services Defend against RIA, Ajax, UGC, and browser-based, client-side exploits Implement scalable threat modeling, code review, application scanning, fuzzing, and security testing procedures

Not Available

In passato, l’arte della “scrittura nascosta” (meglio nota come crittografia) era per lo più riferita ad un insieme di metodi per nascondere il contenuto di un dato messaggio agli occhi di lettori non autorizzati. Oggi, l’evoluzione dei sistemi digitali ha generato nuovi scenari di comunicazione, richiedendo ai moderni crittografi di progettare crittosistemi che soddisfino requisiti di sicurezza complessi, ben oltre il requisito base di confidenzialità ottenibile attraverso la “scrittura nascosta”. Tuttavia, l’analisi di sicurezza di questi schemi crittografici (fino ai primi anni ‘80) era soprattutto guidata dall’intuito e dall’esperienza. Nuovi schemi venivano ideati e, dopo qualche tempo, inevitabilmente, un nuovo attacco alla sicurezza veniva scoperto. Il paradigma della “sicurezza dimostrabile” ha trasformato la crittografia da arte a scienza, introducendo un paradigma formale per l’analisi di sicurezza dei crittosistemi: in questo modo è possibile fornire una dimostrazione matematica che un dato sistema è sicuro rispetto ad una classe generale di attaccanti. Tanto più vasta e vicina alla realtà è questa classe, tanto più forti sono le garanzie offerte dal crittosistema analizzato. Il libro ha lo scopo di guidare lo studente (oppure il giovane ricercatore) nel mondo crittografico, in modo che acquisisca le metodologie di base, preparandosi alla ricerca nell’area.

Identity Based Encryption (IBE) is a type of public key encryption and has been intensely researched in the past decade. Identity-Based Encryption summarizes the available research for IBE and the main ideas that would enable users to pursue further work in this area. This book will also cover a brief background on Elliptic Curves and Pairings, security against chosen Cipher text

Attacks, standards and more. Advanced-level students in computer science and mathematics who specialize in cryptology, and the general community of researchers in the area of cryptology and data security will find Identity-Based Encryption a useful book. Practitioners and engineers who work with real-world IBE schemes and need a proper understanding of the basic IBE techniques, will also find this book a valuable asset.

The field of cryptography has experienced an unprecedented development in the past decade and the contributors to this book have been in the forefront of these developments. In an information-intensive society, it is essential to devise means to accomplish, with information alone, every function that it has been possible to achieve in the past with documents, personal control, and legal protocols (secrecy, signatures, witnessing, dating, certification of receipt and/or origination). This volume focuses on all these needs, covering all aspects of the science of information integrity, with an emphasis on the cryptographic elements of the subject. In addition to being an introductory guide and survey of all the latest developments, this book provides the engineer and scientist with algorithms, protocols, and applications. Of interest to computer scientists, communications engineers, data management specialists, cryptographers, mathematicians, security specialists, network engineers.

A collection of stories about time, space, and the evolution of the universe in which the author blends mathematics with poetic imagination. “Calvino does what very few writers can do: he describes imaginary worlds with the most extraordinary precision and beauty” (Gore Vidal, New York Review of Books). Translated by William Weaver. A Helen and Kurt Wolff Book

Protocols that remain zero-knowledge when many instances are executed concurrently are called concurrent zero-knowledge, and this book is devoted to their study. The book presents constructions of concurrent zero-knowledge protocols, along with proofs of security. It also shows why "traditional" proof techniques (i.e., black-box simulation) are not suitable for establishing the concurrent zero-knowledge property of "message-efficient" protocols.

Alan Turing is regarded as one of the greatest scientists of the 20th century. But who was Turing, and what did he achieve during his tragically short life of 41 years? Best known as the genius who broke Germany's most secret codes during the war of 1939-45, Turing was also the father of the modern computer. Today, all who 'click-to-open' are familiar with the impact of Turing's ideas. Here, B. Jack Copeland provides an account of Turing's life and work, exploring the key elements of his life-story in tandem with his leading ideas and contributions. The book highlights Turing's contributions to computing and to computer science, including Artificial Intelligence and Artificial Life, and the emphasis throughout is on the relevance of his work to modern developments. The story of his contributions to codebreaking during the Second World War is set in the context of his thinking about machines, as is the account of his work in the foundations of mathematics.

From that long investigation of mine the conclusions that I summarize and explain in this book arose and which, I will say immediately, are the following: It is true that the poetry of the "Fedeli d'Amore", especially that of Dante and his most immediate predecessors, of the his contemporaries and his successors, is written in a secret jargon for which at least thirty words (Rossetti had already pointed out some, deceiving himself about others) constantly have, in addition to the apparent meaning concerning love matter, a second and sometimes also a third conventional meaning, concerning the ideas of an initiatory doctrine and the life of a group of initiates. These words are precisely those that with exasperating monotony fill the lines of these "Faithful", very often presenting nonsense in the literal plane, namely: love, madonna, death, life, women, madness and madness, cold, gaiety, gravity, boredom, nature, weep, stone, rose, flower, source, greeting, wild, shame and others of less frequent use. It is true that all the women of the dolce stil novo are in reality one woman and that is the holy Wisdom, which in the special use of the dolce stil novo conventionally takes a different name for each different lover and is called Beatrice for Dante, Giovanna for Guido Cavalcanti, Lagia for Lapo Gianni, Selvaggia for Cino and so on. And since, as I said above, the doctrine cultivated by a sect and the sect itself are confused under the same designation, these women also serve to designate the sect of the "Fedeli d'Amore". Dante's Vita Nuova is all written in this jargon: it is all symbolic from the first to the last word and concerns the initiatory life of Dante and his relations not with the wife of Simone de 'Bardi, but with the Holy Wisdom and with the group that cultivated it. Therefore the Beatrice of the New Life does not differ substantially from the one who appears triumphant on the chariot of the Church in the apocalyptic vision of the Divine Comedy. The darkest poems of the "Fedeli d'Amore" and especially Dante's obscure songs, over which those who were ignorant of the jargon have struggled in vain, read according to the jargon, melt their clarity, coherence, unsuspected depth. Not only that, but with the knowledge of the secret meaning of these few words of jargon, they clear up in our eyes and completely transform into their spirit, other very obscure works by Dante's contemporaries, such as the Documents of love by Francesco da Barberino, the Intelligence by Dino Compagni, the Acerba by Cecco d'Ascoli, works which, while differing outwardly from the love poetry of the sweet styl novo are informed by the same profound mystical spirit, by the same secret doctrine, they come out, in other words, from the bosom of the same sect. These poems, once translated into their real meaning with the key of jargon, in place of that vague, stylized, monotonous, cold, artificial love, which they almost always show according to the letter, reveal to us an intense and deep life of love. for a mystical idea, considered the true essence of Catholic revelation, of a struggle for it, against the carnal and corrupt Church, conventionally called "Death" or "the Stone" and which is depicted as an opponent of the sect of the "Fedeli d'Amore" and as a concealer of that holy Wisdom that the "Fedeli d'Amore" pursue under the figure of the woman; they reveal to us a series of mystical kidnappings, of cries invoking help against the persecutions and threats of adversaries, of excitements with which the followers comfort each other to remain faithful to the holy idea, and other very high and very deep things, before which the fictitious love poem, which is on the surface, falls, and almost always without our regret, like a very insignificant rind, leaving us astonished that we could have believed that all this was really love poetry.

Valperga, published in 1823, the year after Percy Bysshe Shelley's death is a romance of the 14th century in Italy, during the height of the struggle between the Guelphs and the Ghibellines, when each state and almost each town was at war with the other ; a condition of things which lends itself to romance. Mary Shelley's intimate acquaintance with Italy and Italians gives her the necessary knowledge to write on this subject. Her zealous Italian studies came to her aid, and her love of nature give life and vitality to the scene. Valperga, the ancestral castle home of Euthanasia, a Florentine lady of the Guelph faction, is most picturesquely described, on its ledge of projecting rock, overlooking the plain of Lucca; the dependent peasants around happy under the protection of their good Signora. That this beautiful and high-minded lady should be affianced to a Ghibelline leader is a natural combination ; but when her lover Castruccio, prince of Lucca, carries his political enthusiasm the length of making war on her native city of Florence, whose Republican greatness and love of art are happily described, Euthanasia cannot let love stand in the way of duty and gratitude to all those dearest to her ...

In an age when computers process immense amounts of information by the manipulation of sequences of 1s and 0s, it remains a frustrating mystery how prehistoric Inka recordkeepers encoded a tremendous variety and quantity of data using only knotted and dyed strings. Yet the comparison between computers and khipu may hold an important clue to deciphering the Inka records. In this book, Gary Urton sets forth a pathbreaking theory that the manipulation of fibers in the construction of khipu created physical features that constitute binary-coded sequences which store units of information in a system of binary recordkeeping that was used throughout the Inka empire. Urton begins his theory with the making of khipu, showing how at each step of the process binary, either/or choices were made. He then investigates the symbolic components of the binary coding system, the amount of information that could have been encoded, procedures that may have been used for reading the khipu, the nature of the khipu signs, and, finally, the nature of the khipu recording system itself—emphasizing relations of markedness and semantic coupling. This research constitutes a major step forward in building a unified theory of the khipu system of information storage and communication based on the sum total of construction features making up these extraordinary objects.

The best selling 'Algorithmics' presents the most important, concepts, methods and results that are fundamental to the science of computing. It starts by introducing the basic ideas of algorithms, including their structures and methods of data manipulation. It then goes on to demonstrate how to design accurate and efficient algorithms, and discusses their inherent limitations. As the author himself says in the preface to the book; 'This book attempts to present a readable account of some of the most important and basic topics of computer science, stressing the fundamental and robust nature of the science in a form that is virtually independent of the details of specific computers, languages and formalisms'.

When Celine's first novel, 'Journey to the End of the Night', was first published in 1932, it created an instant scandal. Four years later came its sequel, 'Death on Credit', in which a doctor's recollections introduce the reader to the teeming world of everyday Parisian tragedies, of stupidity, malice, lust and greed."

This book provides students with the rudiments of Linear Algebra, a fundamental subject for students in all areas of science and technology. The book would also be good for statistics students studying linear algebra. It is the translation of a successful textbook currently being used in Italy. The author is a mathematician sensitive to the needs of a general audience. In addition to introducing fundamental ideas in Linear Algebra through a wide variety of interesting examples, the book also discusses topics not usually covered in an elementary text (e.g. the "cost" of operations, generalized inverses, approximate solutions). The challenge is to show why the "everyone" in the title can find Linear Algebra useful and easy to learn. The translation has been prepared by a native English speaking mathematician, Professor Anthony V. Geramita.

Three book editors, jaded by reading far too many crackpot manuscripts on the mystic and the occult, are inspired by an extraordinary conspiracy story told to them by a strange colonel to have some fun. They start feeding random bits of information into a powerful computer capable of inventing connections between the entries, thinking they are creating nothing more than an amusing game, but then their game starts to take over, the deaths start mounting, and they are forced into a frantic search for the truth

Treatment of varicose veins based on hemodynamic considerations and especially the CHIVA concept have influenced phlebology for more than a decade. These ideas are not historical but are also a part of new treatment concepts including sclerotherapy and modified surgical procedures. Pre-treatment duplex investigation has become the gold standard. Today, more than ever before, there is a lively discussion and a lot of controversies on how to treat varicose veins best. In the moment there is no definite answer to this question based on published prospective comparative studies. Many questions still remain open and hopefully may be answered in the near future. In these discussions hemodynamic based treatment is always an issue. The chapters of this book are not only well illustrated with excellent color pictures but also based on the actual literature. This book is a mandatory reading for every phlebologist, may she or he be performing CHIVA treatment or not. It is the basis for a better understanding of this concept and for fruitful discussions on the best way of treating varicose veins in the future.