The Crypto Controversy A Key Conflict In The Information Society Law And Electronic Commerce By Koops Bert Jaap 1998 Hardcover

BAKER BUCK

The Crypto Controversy Routledge
This double volume constitutes the thoroughly refereed post-conference proceedings of the 25th International Conference on Financial Cryptography and Data Security, FC 2021, held online due to COVID-19, in March 2021. The 47 revised full papers and 4 short papers together with 3 as Systematization of Knowledge (SoK) papers were carefully selected and reviewed from 223 submissions. The accepted papers were organized according to their topics in 12 sessions: Smart Contracts, Anonymity and Privacy in Cryptocurrencies, Secure Multi-Party Computation, System and Application Security, Zero-Knowledge Proofs, Blockchain Protocols, Payment Channels, Mining, Scaling Blockchains, Authentication and Usability, Measurement, and Cryptography.
Hearing Before the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Sixth Congress, First Session, June 10, 1999 Springer Nature
Ethereum represents the gateway to a worldwide, decentralized computing paradigm. This platform enables you to run decentralized applications (DApps) and smart contracts that have no central points of failure or control, integrate with a payment network, and operate on an open blockchain. With this practical guide, Andreas M. Antonopoulos and Gavin Wood provide everything you need to know about building smart contracts and DApps on Ethereum and other virtual-machine blockchains. Discover why IBM, Microsoft, NASDAQ, and hundreds of other organizations are experimenting with Ethereum. This essential guide shows you how to develop the skills necessary to be an innovator in this growing and exciting new industry. Run an Ethereum client, create and transmit basic transactions, and program smart contracts Learn the essentials of public key cryptography, hashes, and digital signatures Understand how "wallets" hold digital keys that control funds and smart contracts Interact with Ethereum clients programmatically using JavaScript libraries and Remote Procedure Call interfaces Learn security best practices, design patterns, and anti-patterns with real-world examples Create tokens that represent assets, shares, votes, or access control rights Build decentralized applications using multiple peer-to-peer (P2P) components
The Labyrinth Key CRC Press
This reference guide to creating high quality security software covers the complete suite of security applications referred to as end2end security. It illustrates basic concepts of security engineering through real-world examples.

Strategies of the EU and the US in Combating Transnational Organized Crime John Wiley & Sons
Cryptography is essential for information security and electronic commerce, yet it can also be abused by criminals to thwart police wiretaps and computer searches. How should governments address this conflict of interests? Will they require people to deposit crypto keys with a `trusted' agent? Will governments outlaw cryptography that does not provide for law-enforcement access? This is not yet another study of the crypto controversy to conclude that this or that interest is paramount. This is not a study commissioned by a government, nor is it a report that campaigns on the electronic frontier. The Crypto Controversy is neither a cryptography handbook nor a book drenched in legal jargon. The Crypto Controversy pays attention to the reasoning of both privacy activists and law-enforcement agencies, to the particulars of technology as well as of law, to `solutions' offered both by cryptographers and by governments. Koops proposes a method to balance the conflicting interests and applies this to the Dutch situation, explaining both technical and legal issues for anyone interested in the subject.
Authentication in Insecure Environments CRC Press
Sebastian Pape discusses two different scenarios for authentication. On the one hand, users cannot trust their devices and nevertheless want to be able to do secure authentication. On the other hand, users may not want to be tracked while their service provider does not want them to share their credentials. Many users may not be able to determine whether their device is trustworthy, i.e. it might contain malware. One solution is to use visual cryptography for authentication. The author generalizes this concept to human decipherable encryption schemes and establishes a relationship to CAPTCHAS. He proposes a new security model and presents the first visual encryption scheme which makes use of noise to complicate the adversary's task. To prevent service providers from keeping their users under surveillance, anonymous credentials may be used. However, sometimes it is desirable to prevent the users from sharing their credentials. The author compares existing approaches based on non-transferable anonymous credentials and proposes an approach which combines biometrics and smartcards.
Trust in Electronic Commerce:The Role of Trust from a Legal, an Organizational, and a Technical Point of View Kluwer Law International B.V.
Hackers have uncovered the dark side of cryptography—thatdevice developed to defeat Trojan horses, viruses, password theft,and other cyber-crime. It’s called cryptovirology, the art ofturning the very methods designed to protect your data into a meansof subverting it. In this fascinating, disturbing volume, theexperts who first identified cryptovirology show you exactly whatyou’re up against and how to fight back. They will take you inside the brilliant and devious mind of ahacker—as much an addict as the vacant-eyed denizen of thecrackhouse—so you can feel the rush and recognize youropponent’s power. Then, they will arm you for thecounterattack. This book reads like a futuristic fantasy, but be assured, thethreat is ominously real. Vigilance is essential, now. Understand the mechanics of computationally secure informationstealing Learn how non-zero sum Game Theory is used to developsurvivable malware Discover how hackers use public key cryptography to mountextortion attacks Recognize and combat the danger of kleptographic attacks onsmart-card devices Build a strong arsenal against a cryptovirology attack
Understanding Cryptography O'Reilly Media
In a secret war waged in worlds both virtual and real, the fates of nations depend on the definitive weapon. And that weapon is knowledge—knowledge to die for. . . . The race is heating up between the U.S. and China to develop a quantum computer with infinite capabilities to crack any enemy’s codes, yet keep secure its own secrets. The government that achieves this goal will win a crucial prize. No other computer system will be safe from the reach of this master machine. Dr. Jaron Kwok was working for the U.S. government to build such a computer. But in a posh hotel in Hong Kong, a Chinese policewoman sifts through the bizarre, ashlike remains of what’s left of the doctor. With the clock ticking, alliances will be forged—and there are those who will stop at nothing to discover what the doctor knew. As the search for answers intensifies, it becomes chillingly clear that the quantum computer both sides so desperately want will be more powerful, more dangerous than anyone could have ever imagined. For in the twenty-first century, machines become gods, gods become machines, and the once-impossible now lies within reach. The key to unlimited knowledge will create the ultimate weapon of mass destruction—or humanity’s last chance to save itself. . . .
The Fight for Privacy in the Digital Age: A Political History of Digital Encryption IGI Global
This book constitutes the refereed post-conference proceedings of the Second International Conference on Cryptology and Malicious Security, held in Kuala Lumpur, Malaysia, December 1-2, 2016. The 26 revised full papers, two short papers and two keynotes presented were carefully reviewed and selected from 51 submissions. The papers are organized in topical sections on revisiting tradition; different paradigms; cryptofication; malicious cryptography; advances in cryptanalysis; primitives and features; cryptanalysis correspondence.
IJC. Del Rey
"Digital forensics is the science of collecting the evidence that can be used in a court of law to prosecute the individuals who engage in electronic crime"--Provided by publisher.
The Key to Digital Security, How It Works, and Why It Matters Springer Science & Business Media
Policy makers no longer focus on repressive aspects of organised crime alone, but want to be informed about coming challenges and threats to allow them to take appropriate preventive action and target their reactive response better. For that reason, there is a growing demand to change the traditional assessments into analyses that include more prospective elements about current and potential future organised crime situations to identify specific risks or threats to society. The book outlines a methodology to perform analyses of long-term threats of organised crime and scenario studies and applies this on four case studies at two different levels: three studies at Member State level (Belgium, Slovenia, and Sweden) and one at the European Union level. In a last chapter, conclusions and recommendations about the method and its applications are presented. The developed methodological tool and the scenarios are intended as a guide for action and consideration for all actors involved in the fight against organised crime.
Cryptography CRC Press
From 23 to 26 January 2001 the incoming Belgian Presidency of the European Union organized an international conference on the strategies of the European Union and the United States in combating transnational organized crime. The conference gathered policy-makers, police and judicial authorities and other actors with a view to discussing important problems regarding the fight against organized crime. Apart from focusing on the European dimension of the subject (including Eastern Europe), the conference primarily addressed co-operation with the United States. This book collects, along with a number of plenary reports, texts that have been presented and discussed at the conference during the workshops, dealing with integrity and control on information exchange, cross-border operational activities, international/regional framework to fight organized crime, intelligence gathering in the context of peace-keeping activities, training of law enforcement authorities, integrity/corruption, drug trafficking, trafficking in human beings, money laundering and cyber crime.
Cryptography 101: From Theory to Practice "O'Reilly Media, Inc."
Electronic commerce is here to stay. No matter how big the dot-com crisis was or how far the e-entrepreneurs' shares fell in the market, the fact remains that there is still confidence in electronic trading. At least it would appear that investors are confident in e-companies again. However, not only trust of venture capitalists is of importance -- consumers also have to have faith in on-line business. After all, without consumers there is no e-business. Interacting lawyers, technicians and economists are needed to create a trustworthy electronic commerce environment. To achieve this environment, thorough and inter-disciplinary research is required and that is exactly what this book is about. Researchers of the project Enabling Electronic Commerce from the Dutch universities of Tilburg and Eindhoven have chosen a number of e-topics to elaborate on trust from their point of view. This volume makes clear that the various disciplines can and will play a role in developing conditions for trust and thus contribute to a successful electronic market.
74th Annual Discussion and Debate Source Book Kluwer Law International B.V.
This book constitutes the refereed proceedings of the Third International Workshop on Applied Parallel Computing, PARA'96, held in Lyngby, Denmark, in August 1996. The volume presents revised full versions of 45 carefully selected contributed papers together with 31 invited presentations. The papers address all current aspects of applied parallel computing relevant for industrial computations. The invited papers review the most important numerical algorithms and scientific applications on several types of parallel machines.
Legal Aspects of Paperless Communication Maklu
This book constitutes the thoroughly refereed post-proceedings of the 15th International Workshop on Security Protocols, held in Brno, Czech Republic, in April 2007. The 15 revised full papers presented together with edited transcriptions of some of the discussions following the presentations have passed through multiple rounds of reviewing, revision, and selection. The topics addressed reflect the question "When is a Protocol Broken?" and how can it degrade gracefully in the face of partially broken assumptions, or how can it work under un(der)specified assumptions.
Secure Communications And Asymmetric Cryptosystems John Wiley & Sons
This volume is a presentation of all methods of legal knowledge representation from the point of view of jurisprudence as well as computer science. A new method of automatic analysis of legal texts is presented in four case studies. Law is seen as an information system with legally formalised information processes. The achieved coverage of legal knowledge in information retrieval systems has to be followed by the next step: conceptual indexing and automatic analysis of texts. Existing approaches of automatic knowledge representations do not have a proper link to the legal language in information systems. The concept-based model for semi-automatic analysis of legal texts provides this necessary connection. The knowledge base of descriptors, context-sensitive rules and meta-rules formalises properly all important passages in the text corpora for automatic analysis. Statistics and self-organising maps give assistance in knowledge acquisition. The result of the analysis is organised with automatically generated hypertext links. Four case studies show the huge potential but also some drawbacks of this approach.
Contemporary Cryptography, Second Edition Springer Science & Business Media
A nuts-and-bolts explanation of cryptography from a leading expert in information security.
The Crypto Controversy:A Key Conflict in the Information Society
The first edition of this award-winning book attracted a wide audience. This second edition is both a joy to read and a useful classroom tool. Unlike traditional textbooks, it requires no mathematical prerequisites and can be read around the mathematics presented. If used as a textbook, the mathematics can be prioritized, with a book both students and instructors will enjoy reading. Secret History: The Story of Cryptology, Second Edition incorporates new material concerning various eras in the long history of cryptology. Much has happened concerning the political aspects of cryptology since the first edition appeared. The still unfolding story is updated here. The first edition of this book contained chapters devoted to the cracking of German and Japanese systems during World War II. Now the other side of this cipher war is also told, that is, how the United States was able to come up with systems that were never broken. The text is in two parts. Part I presents classic cryptology from ancient times through World War II. Part II examines modern computer cryptology. With numerous real-world examples and extensive references, the author skillfully balances the history with mathematical details, providing readers with a sound foundation in this dynamic field. FEATURES Presents a chronological development of key concepts Includes the Vigenère cipher, the one-time pad, transposition ciphers, Jefferson’s wheel cipher, Playfair cipher, ADFGX, matrix encryption, Enigma, Purple, and other classic methods Looks at the work of Claude Shannon, the origin of the National Security Agency, elliptic curve cryptography, the Data Encryption Standard, the Advanced Encryption Standard, public-key cryptography, and many other topics New chapters detail SIGABA and SIGSALY, successful systems used during World War II for text and speech, respectively Includes quantum cryptography and the impact of quantum computers
Second International Conference, Mycrypt 2016, Kuala Lumpur, Malaysia, December 1-2, 2016, Revised Selected Papers Artech House
The crypto wars have raged for half a century. In the 1970s, digital privacy activists prophesied the emergence of an Orwellian State, made possible by computer-mediated mass surveillance. The antidote: digital encryption. The U.S. government warned encryption would not only prevent surveillance of law-abiding citizens, but of criminals, terrorists, and foreign spies, ushering in a rival dystopian future. Both parties fought to defend the citizenry from what they believed the most perilous threats. The government tried to control encryption to preserve its surveillance capabilities; privacy activists armed citizens with cryptographic tools and challenged encryption regulations in the courts. No clear victor has emerged from the crypto wars. Governments have failed to forge a framework to govern the, at times conflicting, civil liberties of privacy and security in the digital age—an age when such liberties have an outsized influence on the citizen–State power balance. Solving this problem is more urgent than ever. Digital privacy will be one of the most important factors in how we architect twenty-first century societies—its management is paramount to our stewardship

of democracy for future generations. We must elevate the quality of debate on cryptography, on how we govern security and privacy in our technology-infused world. Failure to end the crypto wars will result in societies sleepwalking into a future where the citizen–State power balance is determined by a twentieth-century status quo unfit for this century, endangering both our privacy and security. This book provides a history of the crypto wars, with the hope its chronicling sets a foundation for peace.

RSA and Public-Key Cryptography Haifa Center of Law & Technology

Expanded into two volumes, the Second Edition of Springer’s Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the topic: Definitive information on cryptography and information security from highly regarded researchers Effective tool for professionals in many fields and researchers of all levels Extensive resource with more than 700 contributions in Second Edition 5643 references, more than twice the number of references that appear in the First Edition With over 300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the First Edition’s base of 464 entries, the information in the Encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The Second Edition’s editorial board now includes 34 scholars, which was expanded from 18 members in the First Edition. Representing the work of researchers from over 30 countries, the Encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text’s practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, bibliographies, and links to related literature. Extensive cross-references to other entries within the Encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the Encyclopedia of Cryptography and Security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences; Web Security. Topics covered: Data Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Appl.Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

Profiling the European Citizen Springer

Cryptography, the science of secret writing, is the biggest, baddest security tool in the application programmer's arsenal. Cryptography provides three services that are crucial in secure programming. These include a cryptographic cipher that protects the secrecy of your data; cryptographic certificates, which prove identity (authentication); and digital signatures, which ensure your data has not been damaged or tampered with.This book covers cryptographic programming in Java. Java 1.1 and Java 1.2 provide extensive support for cryptography with an elegant architecture, the Java Cryptography Architecture (JCA). Another set of classes, the Java Cryptography Extension (JCE), provides additional cryptographic functionality. This book covers the JCA and the JCE from top to bottom, describing the use of the cryptographic classes as well as their innards.The book is designed for moderately experienced Java programmers who want to learn how to build cryptography into their applications. No prior knowledge of cryptography is assumed. The book is peppered with useful examples, ranging from simple demonstrations in the first chapter to full-blown applications in later chapters.Topics include: The Java Cryptography Architecture (JCA) The Java Cryptography Extension (JCE) Cryptographic providers The Sun key management tools Message digests, digital signatures, and certificates (X509v3) Block and stream ciphers Implementations of the ElGamal signature and cipher algorithms A network talk application that encrypts all data sent over the network An email application that encrypts its messages Covers JDK 1.2 and JCE 1.2.