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

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.

In the eyes of many, one of the most challenging problems of the information society is that we are faced with an ever expanding mass of information. Based on the work done within the European Network of Excellence (NoE) on the Future of Identity in Information Society (FIDIS), a set of authors from different disciplinary backgrounds and jurisdictions share their understanding of profiling as a technology that may be preconditional for the future of our information society.

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.

The announcement of the Clipper chip by the U.S. Government in April 1993 set off a frenzy of discussions about cryptography policy in the technological community. The shock waves from it ultimately included front page treatment in The New York Times, repeated questions to the Vice President, creation of several new newsgroups on the Internet, and some very productive public discussions about striking the balance between national security, law enforcement, and civil liberties. We still don't have good answers for some of the questions that have been raised. As the Global Information Infrastructure is being built, we are writing portions of the Constitution for Cyberspace. I've been fortunate to have a front row seat and to share much of this with my students. The original reading and selection of materials was made by the

first cohort of students* in The George Washington University Accel erated Master of Science Program in Telecommunications and Com puters at the Ashburn, Virginia campus. They worked many long hours-reading, debating, and selecting materials for this book. In addition, Bob Patton spent a great deal of time scanning and editing the material. Nestor Torres prepared the index. And Harish Nalinak shan provided an enormous amount of technical and administrative assistance and kept the project on track as new developments took place in the debate and new papers and legislation reflected these. As with most readings books, some of the selections cover similar material. We have tried to hold this duplication to an acceptable level.

This book examines current debates about the politics of technology and the future of democratic practices in the digital era. The volume centres on the debates on digital encryption in Germany and the USA, during the aftermath of Edward Snowden’s leaks, which revolved around the value of privacy and the legitimacy of surveillance practices. Using a discourse analysis of mass media and specialist debates, it shows how these are closely interlinked with technological controversies and how, as a result, contestation emerges not within one public sphere but within multiple expert circles. The book develops the notion of ‘publicness’ in order to grasp the political significance of these controversies, thereby making an innovative contribution to Critical Security Studies by introducing digital encryption as an important site for understanding the broader debates on cyber security and surveillance. This book will be of much interest to students of critical security studies, science and technology studies, and International Relations.

This exciting new resource provides a comprehensive overview of the field of cryptography and the current state of the art. It delivers an overview about cryptography as a field of study and the various unkeyed, secret key, and public key cryptosystems that are available, and it then delves more deeply into the technical details of the systems. It introduces, discusses, and puts into perspective the cryptographic technologies and techniques, mechanisms, and systems that are available today. Random generators and random functions are discussed, as well as one-way functions and cryptography hash functions. Pseudorandom generators and their functions are presented and described. Symmetric encryption is explored, and message authentical and authenticated encryption are introduced. Readers are given overview of discrete mathematics, probability theory and complexity theory. Key establishment is explained. Asymmetric encryption and digital signatures are also identified. Written by an expert in the field, this book provides ideas and concepts that are beneficial to novice as well as experienced practitioners.

We live in a wired society, with computers containing and passing around vital information on both personal and public matters. Keeping this data safe is of paramount concern to all. Yet, not a day seems able to pass without some new threat to our computers. Unfortunately, the march of technology has given us the benefits of computers and electronic

tools, while also opening us to unforeseen dangers. Identity theft, electronic spying, and the like are now standard worries. In the effort to defend both personal privacy and crucial databases, computer security has become a key industry. A vast array of companies devoted to defending computers from hackers and viruses have cropped up. Research and academic institutions devote a considerable amount of time and effort to the study of information systems and computer security. Anyone with access to a computer needs to be aware of the developing trends and growth of computer security. To that end, this book presents a comprehensive and carefully selected bibliography of the literature most relevant to understanding computer security. Following the bibliography section, continued access is provided via author, title, and subject indexes. With such a format, this book serves as an important guide and reference tool in the defence of our computerised culture.

This book focuses on the building of a crypto economy as an alternative economic space and discusses how the crypto economy should be governed. The crypto economy is examined in its productive and financialised aspects, in order to distil the need for governance in this economic space. The author argues that it is imperative for regulatory policy to develop the economic governance of the blockchain-based business model, in order to facilitate economic mobilisation and wealth creation. The regulatory framework should cater for a new and unique enterprise organisational law and the fund-raising and financing of blockchain-based development projects. Such a regulatory framework is crucially enabling in nature and consistent with the tenets of regulatory capitalism. Further, the book acknowledges the rising importance of private monetary orders in the crypto economy and native payment systems that do not rely on conventional institutions for value transfer. A regulatory blueprint is proposed for governing such monetary orders as 'commons' governance. The rise of Decentralised Finance and other financial innovations in the crypto economy are also discussed, and the book suggests a framework for regulatory consideration in this dynamic landscape in order to meet a balance of public interest objectives and private interests. By setting out a reform agenda in relation to economic and financial governance in the crypto economy, this forward-looking work argues for the extension of 'regulatory capitalism' to this perceived 'wild west' of an alternative economic space. It advances the message that an innovative regulatory agenda is needed to account for the economically disruptive and technologically transformative developments brought about by the crypto economy.

"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.

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to

this subject.

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

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 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.

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.

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.

Whether you're new to the field or looking to broaden your knowledge of contemporary cryptography, this newly revised edition of an Artech House classic puts all aspects of this important topic into perspective. Delivering an accurate introduction to the current state-of-the-art in modern cryptography, the book offers you an in-depth understanding of essential tools and applications to help you with your daily work. The second edition has been reorganized and expanded, providing mathematical fundamentals and important cryptography principles in the appropriate appendixes, rather than summarized at the beginning of the book. Now you find all the details you need to fully master the material in the relevant sections. This allows you to quickly delve into the practical information you need for your projects. Covering unkeyed, secret key, and public key cryptosystems, this authoritative reference gives you solid working knowledge of the latest and most critical concepts, techniques, and systems in contemporary cryptography. Additionally, the book is supported with over 720 equations, more than 60 illustrations, and numerous time-saving URLs that connect you to websites with related information.

Comprised of eighteen chapters contributed by experts in the fields of biology, computer science, information technology, law, and philosophy, Ethics, Computing, and Genomics provides instructors with a flexible resource for undergraduate

and graduate courses in an exciting new field of applied ethics: computational genomics. The chapters are organized in a way that takes the reader from a discussion of conceptual frameworks and methodological perspectives, including ethical theory, to an in-depth analysis of controversial issues involving privacy and confidentiality, information consent, and intellectual property. The volume concludes with some predictions about the future of computational genomics, including the role that nanotechnology will likely play as biotechnologies and information technologies continue to converge.

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

175 countries, four billion dollars, one scam: the thrilling rise and fall of the biggest cryptocurrency con in history and the woman behind it all In 2016, on stage at Wembley Arena in front of thousands of adoring fans, Dr. Ruja Ignatova promised her followers a financial revolution. The future, she said, belonged to cryptocurrencies such as Bitcoin. And the Oxford-educated, self-styled cryptoqueen vowed that she had invented the Bitcoin Killer. OneCoin would not only earn its investors untold fortunes; it would change the world. By March 2017, more than $4 billion had been invested in OneCoin in countries all around the world. But by October 2017, Ruja Ignatova had disappeared, and it slowly became clear that her revolutionary cryptocurrency was not all it seemed. Fortune was left asking, "Is OneCoin the biggest financial fraud in history?" In The Missing Cryptoqueen, acclaimed tech journalist Jamie Bartlett tells the story he began in his smash hit BBC podcast, entering the murky worlds of little-regulated cryptocurrencies and multilevel marketing schemes. Through a globe-crossing investigation into the criminal underworlds, corrupt governments, and the super-rich, he reveals a very modern tale of intrigue, techno-hype and herd madness that allowed OneCoin to become a million-person pyramid scheme - where, at the top, investors were making millions and, at the bottom, people were putting their livelihoods at risk. It's the inside story of the smartest and biggest scam of the 21st Century - and the genius behind it, who is still on the run.

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 world has changed radically since the first edition of this book was published in 2001. Spammers, virus writers, phishermen, money launderers, and spies now trade busily with each other in a lively online criminal economy and as they specialize, they get better. In this indispensable, fully updated guide, Ross Anderson reveals how to build systems that stay dependable whether faced with error or malice. Here's straight talk on critical topics such as technical engineering basics, types of attack, specialized protection mechanisms, security psychology, policy, and more.

The Crypto Controversy:A Key Conflict in the Information SocietyKluwer Law International B.V.

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.

So rapid have been the developments of e-commerce, that it is now frequently said that this is the future of any commerce and that it carries the potential for enormous growth - at least for the business to business ("B2B") sector. This text covers some important legal issues arising in e-commerce.

Cyber attacks are on the rise. The media constantly report about data breaches and increasingly sophisticated cybercrime. Even governments are affected. At the same time, it is obvious that technology alone cannot solve the problem. What can countries do? Which issues can be addressed by policies and legislation? How to draft a good law? The report assists countries in understanding what cybercrime is about, what the challenges are in fighting such crime

and supports them in drafting policies and laws.

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.

Secure message transmission is of extreme importance in today's information-based society: military, diplomatic, and corporate data transmissions must be safeguarded; so also must the account of every individual who has an automatic-teller bank account or whose purchases are subject to point-of-sale, direct account debiting. The only known way to keep all such transactions secret and authentic is by way of cryptographic techniques. But most cryptosystems in use today are not fool-proof-- their "symmetric" nature allows them to be compromised if either the sender's or the receiver's "key" (decoding algorithm) falls into the wrong hands. This book reports on the enormous amount of work that has been done in the past on the concept, "asymmetric" cryptography.

Legal problems abound in the information society. Electronic commerce, copyright, privacy, illegal and harmful content, taxes, wiretapping governments face an enormous challenge to meet the advent of the Internet and ICT with a flexible, up-to-date, and adequate legal framework. Yet one aspect makes this challenge even more daunting: internationalisation. Law is still to a great extent based on nation states, but the information society is above all a borderless and global society. Territoriality and national sovereignty clash with the need for a global approach to address ICT-law issues. Should states leave everything to the global market, or should they intervene to protect vital national interests? How can one enforce national rules in a world where acts take place somewhere' in Cyberspace? This book presents the positions on these issues of the governments of the Netherlands, Germany, France, the UK, and the US, as well as of international organisations. How do they think about co-regulation, law enforcement, harmonisation, international cooperation, and alternative dispute resolution? How do they deal with applicable law and online contracts, privacy, international liability of Internet providers, and electronic signatures? What are the implications of the European Electronic Commerce Directive and the draft Crime in Cyberspace convention? Any legal framework that is to fit the

global information society must take into account internationalisation. This volume shows to what extent governments are meeting this challenge.

Although much literature exists on the subject of RSA and public-key cryptography, until now there has been no single source that reveals recent developments in the area at an accessible level. Acclaimed author Richard A. Mollin brings together all of the relevant information available on public-key cryptography (PKC), from RSA to the latest applications of PKC, including electronic cash, secret broadcasting, secret balloting systems, various banking and payment protocols, high security logins, smart cards, and biometrics. Moreover, he covers public-key infrastructure (PKI) and its various security applications. Throughout the book, Mollin gives a human face to cryptography by including nearly 40 biographies of the individuals who helped develop cryptographic concepts. He includes a number of illustrative and motivating examples, as well as optional topics that go beyond the basics, such as Lenstra's elliptic curve method and the number field sieve. From history and basic concepts to future trends and emerging applications, this book provides a rigorous and detailed treatment of public-key cryptography. Accessible to anyone from the senior undergraduate to the research scientist, RSA and Public-Key Cryptography offers challenging and inspirational material for all readers.

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.

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.

Financial crime affects virtually all areas of public policy and is increasingly transnational. The essays in this volume address both the theoretical and policy issues arising from financial crime and feature a wide variety of case studies, and cover topics such as state revenue collection, criminal enterprises, money laundering, the use of new technologies and methods in financial crime, corruption, terrorism, proliferation of WMD, sanctions, third-world debt, procurement, telecommunications, cyberspace, the defense industry and intellectual property. Taken together, these essays form a must-read collection for scholars and students in law, finance and criminology.

Steganography is the art and science of hiding information in inconspicuous cover data so that even the existence of a secret message is kept confidential, and steganalysis is the task of detecting secret messages in covers. This research monograph focuses on the role of cover signals, the distinguishing feature that requires us to treat steganography and steganalysis differently from other secrecy techniques. The main theoretical contribution of the book is a proposal to structure approaches to provably secure steganography according to their implied assumptions on the limits of the adversary and on the nature of covers. A further contribution is the emphasis on dealing with heterogeneity in cover distributions, crucial for security analyses. The author's work complements earlier approaches based on information, complexity, probability and signal processing theory, and he presents numerous practical implications. The scientific advances are supported by a survey of the classical steganography literature; a new proposal for a unified terminology and notation that is maintained throughout the book; a critical discussion of the results achieved and their limitations; and an assessment of the possibility of transferring elements of this research's empirical perspective to other domains in information security. The book is suitable for researchers working in cryptography and information security, practitioners in the corporate and national security domains, and graduate students specializing in multimedia security and data hiding.