Angewandte Kryptographie

As recognized, adventure as capably as experience more or less lesson, amusement, as skillfully as arrangement can be gotten by just checking out a ebook **angewandte kryptographie** as well as it is not directly done, you could say you will even more re this life, on the subject of the world.

We offer you this proper as competently as easy quirk to acquire those all. We present angewandte kryptographie and numerous ebook collections from fictions to scientific research in any way. in the midst of them is this angewandte kryptographie that can be your partner.

Einführung in die Informations- und Codierungstheorie Dirk W. Hoffmann 2014-03-21 Gegenstand dieses Buches sind die Grundlagen der Informations- und Codierungstheorie, wie sie in den Fächern Informatik, Nachrichtentechnik, Elektrotechnik und Informationstechnik an vielen Hochschulen und Universitäten unterrichtet werden. Im Mittelpunkt stehen die unterschiedlichen Facetten der digitale Datenübertragung. Das Gebiet wird aus informationstheoretischer Sicht aufgearbeitet und zusammen mit den wichtigsten Konzepten und Algorithmen der Quellen-, Kanal- und Leitungscodierung vorgestellt. Um eine enge Verzahnung zwischen Theorie und Praxis zu erreichen, wurden zahlreiche historische Notizen in das Buch eingearbeitet und die theoretischen Kapitel an vielen Stellen um Anwendungsbeispiele und Querbezüge ergänzt.

Agents and Multi-Agent Systems in Construction Chimay Anumba 2007-04-11 This book describes current advances and future directions in the theory and application of intelligent agents and multi-agent systems in the Architecture, Engineering and Construction (AEC) sector. It is the product of an international effort involving a network of construction IT and computing researchers, investigating different aspects of agent theory and applications. The contributed chapters cover different perspectives and application areas, and represent significant efforts to harness emerging technologies such as intelligent agents and multi-agent systems for improved business processes in the AEC sector. The first four chapters cover the theoretical foundations of agent technology whilst the remaining chapters deal with the application of agent-based systems in solving problems in the construction domain.

Data Security Thomas H. Lenhard 2022-01-04 Using many practical examples and notes, the book offers an easy-to-understand introduction to technical and organizational data security. It provides an insight into the technical knowledge that is mandatory for data protection officers. Data security is an inseparable part of data protection, which is becoming more and more important in our society. It can only be implemented effectively if there is an understanding of technical interrelationships and threats. Data security covers much more information than just personal data. It secures all data and thus the continued existence of companies and organizations. This book is a translation of the original German 2nd edition Datensicherheit by Thomas H. Lenhard, published by Springer Fachmedien Wiesbaden GmbH, part of Springer Nature in 2020. The translation was done with the help of artificial intelligence (machine translation by the service DeepL.com). A subsequent human revision was done primarily in terms of content, so that the book will read stylistically differently from a conventional translation. Springer Nature works continuously to further the development of tools for the production of books and on the related technologies to support the authors.

Basiswissen angewandte Mathematik Burkhard Lenze 2007

Sicherheit und Kryptographie im Internet Jörg Schwenk 2010-04-15 Besonderen Wert legt der Autor auf die Darstellung, wie bekannte kryptographische Verfahren an die jeweiligen Erfordernisse der Internet-Dienste angepasst wurden.

Angewandte Kryptographie Wolfgang Ertel 2012

Digital Rights Management Eberhard Becker 2003-11-04 The content industries consider Digital Rights Management (DRM) to contend with unauthorized downloading of copyrighted material, a practice that costs artists and distributors massively in lost revenue. Based on two conferences that brought together high-profile specialists in this area - scientists, lawyers, academics, and business practitioners - this book presents a broad, well-balanced, and objective approach that covers the entire DRM spectrum. Reflecting the interdisciplinary nature of the field, the book is structured using three different perspectives that cover the technical, legal, and business issues. This monograph-like anthology is the first consolidated book on this young topic.

Digital Watermarking for Digital Media Juergen Seitz 2005-01-01 "The book discusses new aspects of digital watermarking in a worldwide context"--Provided by publisher.

Ideen der Informatik Uwe Schöning 2008-01-01

Codierung und Kryptologie Thomas Borys 2011-06-28 Thomas Borys untersucht aus didaktischer Sicht, welchen Beitrag die Inhalte Codierung und Kryptologie zur mathematischen bzw. informatischen Bildung leisten. Seine epistemologische Analyse erfolgt auf Basis des genetischen Prinzips und der fundamentalen Ideen der Mathematik und der Informatik, die als Leitlinien der mathematischen bzw. informatischen Bildung dienen. An ausgewählten Beispielen der Codierung und Kryptologie wird gezeigt, was bei der Umsetzung im Unterricht zu beachten ist.

Auswirkungen von Seitenkanalangriffen auf das Design kryptographischer Algorithmen Jens Rüdinger 2009

Smart Card Applications Wolfgang Rankl 2007-04-30 A practical guide to the specification, design, and programming of smart card systems for working applications. More than 3 billion smartcards are produced every year. Generally defined as any pocket-sized card with embedded integrated circuits or chips, they have a huge number of applications including travel cards, chip and pin cards, pet tags, mobile phone SIMs and pallet trackers. Now with modern Smart Card technology such as Java Card and Basic Card it is possible for everyone to create his or her own applications on a smart card. This book provides generic solutions for programming smart cards, enabling the creation of working applications and systems. Key features: Presents a comprehensive introduction to the topic of smart cards, explaining component elements and the smart card microcontrollers. Sets out information on operating systems with case studies of a range of applications including credit card security, mobile phones and transport payment cards. Gives detailed advice on the monitoring of smart card applications, recognizing potential attacks on security and improving system integrity. Provides modules and examples so that all types of systems can be built up from a small number of individual components. Offers guidelines on avoiding and overcoming design errors. Ideal for practising engineers and designers looking to implement smart cards in their business, it is also a valuable reference for postgraduate students taking courses on embedded system and smart card design.

Datenschutz Ronald Petrlic 2017-04-29 Dieses Lehrbuch behandelt schwerpunktmäßig technische

Maßnahmen, die den Schutz personenbezogener Daten sicherstellen. Dazu werden grundlegende Verfahren der Anonymisierung und der Gewährleistung von Anonymität im Internet (z. B. Tor) vorgestellt. Das Buch gibt einen Überblick über gängige Verfahren des Identitätsmanagements (z. B. OpenID Connect) und die in elektronischen Ausweisdokumenten (z. B. im Personalausweis) verwendeten Sicherheitsmaßnahmen. Die Datenschutz-Garantien der vermittelten Ansätze werden im Detail behandelt. Im Bereich des World Wide Web erfährt der Leser, wo die Probleme aus Sicht des Datenschutzes liegen und wie diese Lücken geschlossen werden können. Anonyme Bezahlverfahren und eine Untersuchung von Bitcoin runden den technischen Teil des Buches ab. Der Leser lernt Ansätze aus der Praxis kennen, um so je nach Anforderungen in der Systementwicklung das passende Verfahren auswählen zu können. Daneben werden die Grundlagen des Datenschutzrechts behandelt, weil das Recht auch Anforderungen an technische Lösungen stellt. Betrachtet werden das informationelle Selbstbestimmungsrecht, die Grundzüge des Bundesdatenschutzgesetzes sowie die Datenschutzbestimmungen des Telemediengesetzes. Beispielhaft werden datenschutzrechtliche Fälle bearbeitet.

Recent Developments in Individual and Organizational Adoption of ICTs Yildiz, Orkun 2020-08-28 In recent years, information and communication technologies (ICTs) have gained significant importance and become vital to the operations of both organizations and individuals. However, there are numerous factors that have affected the adoption of ICTs including access and accessibility barriers, political participation, and social empowerment. This has attracted the attention of researchers who are interested in understanding the socioeconomic influences of ICT adoption and how these technologies impact the infrastructure of modern organizational activities. Recent Developments in Individual and Organizational Adoption of ICTs is a collection of innovative research on the methods of organizational and infrastructural advancement through the application of information and communication technologies. While highlighting topics including internet banking, supply chain management, and e-government services, this book is ideally designed for managers, researchers, policymakers, politicians, business practitioners, educators, decision scientists, strategists, and students seeking current research on the socioeconomic impact of ICT adoption.

Information und Kommunikation Markus Hufschmid 2007-01-16 Modulationsverfahren, Codierungstechniken und Kryptologie sind eng verwandte Gebiete. Das vorliegende Lehrbuch stellt sie mit ihren Verzahnungen thematisch umfassend, methodisch genau und mathematisch verständlich dar. Ausgehend von einer Einführung in die Informationstheorie werden Themen behandelt, deren Kenntnis für die systematische Analyse von Systemen zur Informationsübertragung notwendig ist. Dazu gehören die Quellen- und Kanalcodierung, die analogen und digitalen Modulationsverfahren sowie die Beschreibung von stochastischen Prozessen. Das Buch wird durch eine ausgedehnte Einführung in die Kryptologie abgerundet, in der neben den gebräuchlichsten Algorithmen auch die wichtigsten Protokolle vorgestellt und analysiert werden. Besonderer Wert wurde darauf gelegt, modernen Verfahren wie z.B. Turbo Codes, OFDM, Elliptische Kurven oder auch die Quantenkryptographie einzubeziehen.

Innovative Internet Computing Systems Thomas Böhme 2003-05-15 Nowadays, the Internet is the most commonly used medium for the exchange of data in di?erent forms. Presently, over 60 million machines have access to the Internet and to its resources. However, the Internet is also the largest distributed system o?ering di?erent computational services and possibilities not only for cluster computing. If the needs of modern mobile computing and multimedia systems are taken into account, it becomes clear that modern methods must ensure an e?ective development and management of the Internet allowing each user fast access to this huge resource space. The Innovative Internet Computing Systems workshop is organized by the Gesellschaft fur¨ Informatik(GI) in Germany. It intends to be an open me- ing point for

scientists dealing with di?erent aspects of this complex topic. In contrast to the Distributed Communities on the Web workshops, which can be 2 considered as the roots of I CS, special attention is given to fundamental - search works and the application of theoretical and formal results in practical implementations.

Instructional Technologies Paul Darbyshire 2005-01-01 E-Commerce and M-Commerce Technologies explores the emerging area of mobile commerce. The chapters in this book look specifically at the development of emerging technologies and their application in Internet commerce. From E-business to mobile database developments, this book offers a compilation of readings that will prove useful to individuals and organizations in the academic study and research surrounding mobile commerce as well as in the practical application of these technologies.

From Integrated Publication and Information Systems to Information and Knowledge Environments Matthias Hemmje 2005-01-31 This book constitutes a commemorative volume devoted to Erich J. Neuhold on the occasion of his 65th birthday. The 32 invited reviewed papers presented are written by students and colleagues of Erich Neuhold throughout all periods of his scientific career. The papers are organized in the following topical sections: Database management enabling information systems Semantic Web drivers for advanced information management Securing dynamic media content integration From digital libraries to intelligent knowledge environments Visualization – key to external cognition in virtual information environments From human-computer interaction to human-artefact interaction Domains for virtual information and knowledge environments.

Angewandte Kryptographie Wolfgang Ertel 2012

Der Schutz "privater" Informationen bei Cloud Computing Michael Busching 2019-11-28 Cloud Computing ist zwischenzeitlich sowohl im privaten als auch beruflichen Bereich kaum noch wegzudenken. Berufsgeheimnistrager - wie Arzte und Rechtsanwalte - stellen derartige Entwicklungen jedoch haufig vor grosse Herausforderungen. Fur sie gelten besondere Vorschriften, die mit dem "Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausubung schweigepflichtiger Personen" und der Datenschutzgrundverordnung der EU vor noch nicht allzu langer Zeit einige Anderungen erfahren haben. Inwieweit bestehen fur Arzte und Rechtsanwalte nach der nunmehr geltenden "neuen" Rechtslage straf, datenschutz- und berufsrechtliche Sanktionsrisiken? Dieser Frage geht Michael Busching in seiner Untersuchung nach. Hierbei werden sowohl die einschlagigen Sanktionsvoraussetzungen sowie damit zusammenhangende Probleme benannt und systematisch abgearbeitet als auch mogliche Massnahmen erortert, durch die eine Sanktionierung unter Umstanden vermieden werden kann.

Das Internet als Vertriebskanal für Zeitschriftenverlage Andreas Klatt 2003-10-13 Inhaltsangabe:Einleitung: Das Internet stellt für Verlage aus der Zeitschriftenbranche eine große Herausforderung dar. Als klassische Produzenten von Inhalten scheinen sie die optimalen Voraussetzungen mitzubringen, um im Internet erfolgreich zu sein. Das stimmt zwar, aber die allerwenigsten Verlage verstehen diese zu nutzen. Wie kommt das? Obwohl es Unmengen von Büchern und Internetseiten zu E-Business, Web-Marketing, Web-Shops und zahlreichen anderen Web -relevanten Themen gibt, fehlt es an Literatur, die auf Zeitschriftenverlage zugeschnitten ist. Was den meisten Verantwortlichen nicht bewusst zu sein scheint und an dieser Stelle als ein Ergebnis vorweggenommen werden soll: Zeitschriftenverlage dürfen sich konzeptionell weder an ihrem Offline-Angebot noch an dem Online-Angebot anderer Internet-Akteure orientieren. Für sie gelten eigene Regeln, die es im Zuge dieser Diplomarbeit auszuarbeiten gilt. Eine zentrale Position nimmt dabei die Frage nach dem Umgang mit

dem eigentlichen Gut, den redaktionell verfassten Inhalten, ein. Das einfache kostenlose Bereitstellen von Zeitschrifteninhalten auf der Internetseite kann fatale Folgen haben. Das kostenpflichtige Anbieten über umständliche Zahlungsabwicklungen oder das Verschlüsseln der Inhalte mit dem Ziel einer kontrollierbaren Nutzung ebenso. Im Vordergrund steht also das Wie . Wie lassen sich die Vorteile des Internets ausreizen, ohne sich selbst dabei zu schaden? Wie lässt sich das Produkt einer Zeitschrift sinnvoll vertreiben? Es ist ein Gesamtkonzept notwendig, das jedoch aktuelle und profunde Kenntnisse über die Situation der Verlage im Internet und den bestmöglichen Umgang beim Erstellen, Platzieren und Vertreiben der Inhalte und Angebote voraussetzt. Im Folgenden soll ein kurzer Überblick über den inhaltlichen Rahmen der Arbeit gegeben werden. Gang der Untersuchung: Den Anfang bildet eine in Kapitel 2 vorgenommene Untersuchung auf die Unterschiedlichkeiten zwischen den beiden Medien Internet und Zeitschrift. Neben der Rolle des jeweiligen Mediums innerhalb unserer Gesellschaft wird ebenso der Frage nach den Unterschieden im Leseverhalten am Bildschirm und in der Zeitschrift auf den Grund gegangen. Kapitel 3 beleuchtet den bisherigen Umgang der Verlage mit dem Internet. Eine Marktübersicht lässt drei verschiedene Typen von Verlegern erkennen, die anhand von Beispielen vorgestellt werden. Des Weiteren wird der Versuch unternommen, die durch einen Online-Auftritt entstehenden Kosten zu [...]

Angewandte Kryptographie Wolfgang Ertel 2019-11-11

Privacy-Respecting Intrusion Detection Ulrich Flegel 2007-08-28 Effective response to misuse or abusive activity in IT systems requires the capability to detect and understand improper activity. Intrusion Detection Systems observe IT activity, record these observations in audit data, and analyze the collected audit data to detect misuse. Privacy-Respecting Intrusion Detection introduces the concept of technical purpose binding, which restricts the linkability of pseudonyms in audit data to the amount necessary for misuse detection. Also, it limits the recovery of personal data to pseudonyms involved in a detected misuse scenario. The book includes case studies demonstrating this theory, and solutions that are constructively validated by providing algorithms.

Mathematik für Informatiker Gerald Teschl 2013-06-22 In diesem Lehrbuch werden die mathematischen Grundlagen exakt und dennoch anschaulich und gut nachvollziehbar vermittelt. Sie werden durchgehend anhand zahlreicher Musterbeispiele illustriert, durch Anwendungen in der Informatik motiviert und durch historische Hintergründe oder Ausblicke in angrenzende Themengebiete aufgelockert. Am Ende jedes Kapitels befinden sich Kontrollfragen, die das Verständnis testen und typische Fehler bzw. Missverständnisse ausräumen. Zusätzlich helfen zahlreiche Aufwärmübungen (mit vollständigem Lösungsweg) und weiterführende Übungsaufgaben das Erlernte zu festigen und praxisrelevant umzusetzen. Dieses Lehrbuch ist daher auch sehr gut zum Selbststudium geeignet. Ergänzend wird in eigenen Abschnitten das Computeralgebrasystem Mathematica vorgestellt und eingesetzt, wodurch der Lehrstoff visualisiert und somit das Verständnis erleichtert werden kann.

Kryptografie Klaus Schmeh 2016-04-21 Dieses umfassende Einführungs- und Übersichtswerk zur Kryptografie beschreibt eine große Zahl von Verschlüsselungs-, Signatur und Hash-Verfahren in anschaulicher Form, ohne unnötig tief in die Mathematik einzusteigen. Hierbei kommen auch viele Methoden zur Sprache, die bisher kaum in anderen Kryptografiebüchern zu finden sind. Auf dieser breiten Basis geht das Buch auf viele spezielle Themen ein: Kryptografische Protokolle, Implementierungsfragen, Sicherheits-Evaluierungen, Seitenkanalangriffe, Malware-Angriffe, Anwenderakzeptanz, Schlüsselmanagement, Smartcards, Biometrie, Trusted Computing und vieles mehr werden ausführlich behandelt. Auch spezielle Kryptografieanwendungen wie Digital Rights Management kommen nicht zu kurz. Besondere Schwerpunkte bilden zudem die Themen Public-Key-Infrastrukturen

(PKI) und kryptografische Netzwerkprotokolle (WEP, SSL, IPsec, S/MIME, DNSSEC und zahlreiche andere). Die Fülle an anschaulich beschriebenen Themen macht das Buch zu einem Muss für jeden, der einen Einstieg in die Kryptografie oder eine hochwertige Übersicht sucht. Der Autor ist ein anerkannter Krypto-Experte mit langjähriger Berufserfahrung und ein erfolgreicher Journalist. Er versteht es, Fachwissen spannend und anschaulich zu vermitteln. Die Neuauflage ist aktualisiert und geht auf neueste Standards, Verfahren sowie Protokolle ein. "Eines der umfangreichsten, verständlichsten und am besten geschriebenen Kryptografie-Bücher der Gegenwart." David Kahn, US-Schriftsteller und Kryptografie-Historiker

Angewandte Kryptographie Wolfgang Ertel 2001

Zahlungsverkehr im Internet aus deutscher Perspektive Peter Mattke 1997-10-27
Inhaltsangabe:Einleitung: 7.00 Uhr. Der Tag beginnt. Der Computer schaltet sich automatisch ein, ein freundliches Gesicht lächelt mich an und mahnt zum Aufstehen. Ich bestelle beim Bäcker um die Ecke, der sich einem virtuellen Warenhaus angeschlossen hat, meine Brötchen per Internet. Der Preis wird über die Kreditkarte von meinem Bankkonto online abgebucht. Die Lieferung erfolgt zügig. Ich informiere mich im Netz über die neuesten Nachrichten und überweise schnell die letzte Autorechnung über das Internet-Homebanking. Anschließend widme ich mich meiner Tätigkeit als virtueller Berater einer Großbank und betreue über Videokonferenz meine Kunden... Ist dieses Szenario reine Fiktion oder schon bald Wirklichkeit?! Fakt ist, dass stürmische Zeiten nahen. „Der Strukturwandel von der Industrie- zur Dienstleistungsgesellschaft geht in großen Schritten hin zur Informations- und Kommunikationsgesellschaft.“ Neue Kommunikationsmedien sorgen für eine Informationsübermittlung, bei der Zeit und Raum eine sehr untergeordnete Rolle spielen. Das Internet als eine der neuesten Errungenschaften ist ein Spiegelbild dieser Entwicklung. Weltweite Kommunikation, verbunden mit einer extrem hohen Transportgeschwindigkeit der Daten und einem schier unerschöpflichen Angebot an Informationen, Waren und Dienstleistungen sind wichtige Kennzeichen. In diesem riesigen Netz sollen aber nicht nur Informationen ausgetauscht, Waren oder Dienstleistungen verglichen und bestellt werden. Der letzte Schritt ist, auch Geldtransfers über das Internet abzuwickeln. Gang der Untersuchung: Die vorliegende Diplomarbeit beschäftigt sich mit diesem Thema, wobei speziell die Entwicklung in Deutschland betrachtet wird. Da es sich hier nicht um Gefälligkeiten, sondern um den Transfer von hart erarbeitetem Geld handelt, müssen Vorkehrungen zur Absicherung getroffen werden. Gleichzeitig gibt es viele Details und Einflüsse, die beachtet werden müssen, um eine Gesamtbewertung vorzunehmen. Zunächst werden in Kapitel 2 die Möglichkeiten dargelegt, in Deutschland Zahlungsverkehr abzuwickeln. Aufbauend auf den immer noch bedeutsamen traditionellen Formen kam es durch die technische Entwicklung in den letzten Jahren zu zahlreichen Innovationen und Vereinfachungen in diesem Bereich. Vorläufiger Endpunkt der Entwicklung ist der Zahlungsverkehr im Internet. Weltweites Tätigen von Bankgeschäften und länderübergreifendes Bezahlen von Waren und Dienstleistungen sind das aktuelle Nonplusultra. In Kapitel 3 [...]

VPN mit Linux Ralf Spenneberg 2004

Information Security and Ethics: Concepts, Methodologies, Tools, and Applications Nemati, Hamid 2007-09-30 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.

Sicherheit in vernetzten Systemen Albrecht Ude 2021-03-15 Im Namen der DFN-CERT Services GmbH

und des Programm-Komitees präsentieren wir Ihnen den Konferenzband zur 28. DFN-Konferenz "Sicherheit in vernetzten Systemen" in Hamburg. Seit 1994 jährlich stattfindend, hat diese sich mit einer betont technischen und wissenschaftlichen Ausrichtung als eine der größten deutschen Sicherheitstagungen etabliert. In diesem Band finden Sie die Langfassungen der ausgewählten Beiträge bzw. der Redner auf der Tagung. Die Beiträge befassen sich u.a. mit den Themen Post-Quanten-Kryptographie, Phishing-Awareness, Business-Continuity-Konzepten, neuen Rahmenbedingungen für die Cybersicherheit, Informationssicherheit.

Sicherheit Gunter Scholtz 2003 Vorwort T. Borsche: Orientierung im unsicheren Feld der Begriffe D. Schneider: Von abgebrochenen Glücksspielen zur Nicht-Existenz einer Zukunft. Der mühsame Weg zu vernünftigen Entscheidungen unter Unsicherheit E. Pankoke: Solidarität und Sekurität in der Risikogesellschaft. Modernisierungsschwellen und Modernisierungskrisen sozialer Sicherung S. Suckut: Die DDR-Staatssicherheit. Von der Labilität des anscheinend Stabilen B. Meyer: Wenn die Ausnahme zur Regel wird. Staatliche Reaktionen auf den Terrorismus im Spannungsfeld von Sicherheit und Freiheit G. Kleinhenz: Zukunft der Erwerbsarbeit und soziale Sicherung E. Eichenhofer: Wie sicher ist die soziale Sicherheit im Europa von Morgen? E. Welteke: Harte Währung Vertrauensanker für neue Märkte G. Bechmann: Zukunft als Risiko oder Gefahr. Zur Bedeutung des Nichtwissens und der Sicherheit in der modernen Gesellschaft A. Heuser: Der Mensch im Netz. Chancen und Risiken der Informationsgesellschaft N. Leygraf: Gefährliche Straftäter O.H. Pesch: Heilsgewißheit Sicherheit durch Glauben? Gesellschaftliche Implikationen eines theologischen Schlüsselbegriffs Autorenverzeichnis Personenregister Sachregister.

IT Systems in Public Transport Gero Scholz 2016-08-24 At first glance, public transport in the majority of cities and regions around the world would not be considered high-tech by most passengers. However, when taking a closer look at the systems that are necessary to attract/retain passengers and ensure efficient operations, the importance of IT and the high-tech nature of the public transport sector becomes clear. Transport operators use advanced information technology products in order to plan, optimise and manage their fleets and staff. Sophisticated software systems support and drive these tasks. Furthermore, these systems are used to manage daily operations, which includes monitoring and dispatching of rolling stock and crew, providing passengers with realtime information, electronic ticketing and much more. As in many industries, public transport and associated IT standards vary around the world. Several operators have invested significantly in public transport, while others have a great deal of catching up to do. Strategic investments in public transport can significantly improve the quality of life in cities and regions. IT systems play a vital role in supporting this aim. Why write this book? For what purpose and for which audience? Above all, this book is intended for those who develop, implement and operate public transport IT systems. These readers need to be familiar with the software and understand public transport IT systems both at a high level and in detail. This is achieved through descriptions of public transport business processes and a detailed illustration of a comprehensive systems data model. Furthermore, the book was written for professors and students of transport and IT, at universities and other institutes of higher education. Finally, the book is intended for those in the public transport industry who use these systems and want, or need, to understand the systems in further detail.

Organic and Pervasive Computing -- ARCS 2004 Christian Müller-Schloer 2004-02-12 Where is system architecture heading? The special interest group on Computer and Systems Architecture (Fachausschuss Rechner- und Systemarchitektur) of the German computer and information technology associations GI and ITG a- ed this question and discussed it during two Future Workshops in 2002. The result in a nutshell: Everything will change but everything else will remain. Future systems technologies will build on a mature basis of silicon and IC technology,onwell-

understoodprogramminglanguagesandsoftwareengineering techniques, and on well-established operating systems and middleware concepts. Newer and still exotic but exciting technologies like quantum computing and DNA processing are to be watched closely but they will not be mainstream in the next decade. Although there will be considerable progress in these basic technologies, is there any major trend which uni?es these diverse developments? There is a common denominator – according to the result of the two - ture Workshops – which marks a new quality. The challenge for future systems technologies lies in the mastering of complexity. Rigid and in?exible systems, built under a strict top-down regime, have reached the limits of manageable complexity, as has become obvious by the recent failure of several large-scale projects. Nature is the most complex system we know, and she has solved the problem somehow. We just haven't understood exactly how nature does it. But it is clear that systems designed by nature, like an anthill or a beehive or a swarm of birds or a city, are di?erent from today's technical systems that have beendesignedbyengineersandcomputerscientists.

Angewandte Kryptographie Franz Scheerer 2018-10-29 Einen strikten mathematischen Beweis für die Sicherheit der digitalen Signatur gibt es für das 1979 von Michael Oser Rabin vorgeschlagene Verfahren unter der Voraussetzung, dass es praktisch unmöglich ist die Primzahlen aus dem Produkt n gleich p mal q zu bestimmen und bestimmte als plausibel angenommene Annahmen für die Hash-Werte gelten.

Sicherheitsaspekte kryptographischer Verfahren beim Homebanking Lars Nöbel 2002-07-04 Inhaltsangabe:Zusammenfassung: In der vorliegenden Arbeit werden kryptographische Verfahren und Protokolle vorgestellt, die im HBCI-Standard zum Einsatz kommen. Das Hauptaugenmerk liegt hierbei auf den derzeit verwendeten Algorithmen DES und RSA sowie deren möglichen Nachfolgern Rijndael und ElGamal mit elliptischen Kurven. Die dafür notwendigen mathematischen Grundlagen werden ebenso wie die grundlegenden Begriffe der Kryptographie eingeführt. Es wird auf Sicherheitsaspekte der untersuchten Algorithmen und auf die zukünftige Entwicklung eingegangen. Dabei stellt sich heraus, daß mit den benutzten Verfahren die Sicherheit der Kommunikationspartner nur unwesentlich bis gar nicht beeinträchtigt werden kann. Beim praktischen Einsatz existieren aber noch Lücken, die für einen Angriff ausgenutzt werden können. Inhaltsverzeichnis:Inhaltsverzeichnis: 1.Einleitung1 2.Mathematische Grundlagen3 2.1Hilfsmittel aus der Zahlentheorie3 2.1.1Komplexität von Algorithmen3 2.1.2Der Euklidische Algorithmus5 2.1.3Der Chinesische Restsatz7 2.1.4Der Satz von Euler-Fermat8 2.1.5Galoisfelder9 2.2Einwegfunktionen9 2.2.1Faktorisierung natürlicher Zahlen9 2.2.2Der diskrete Logarithmus10 2.2.3Nichtlineare Transformationen11 2.3Erzeugung von Zufallszahlen11 2.3.1Zufallszahlengeneratoren11 2.3.2Kongruenzgeneratoren12 2.3.3Schieberegister14 2.3.4Weitere Generatoren14 2.4Primzahltests und Faktorisierung15 2.4.1Probedivision und Fermat-Test15 2.4.2Der Miller-Rabin-Test16 2.4.3Pollards Methode17 2.4.4Das Quadratische Sieb18 3.Kryptographische Grundlagen19 3.1Grundbegriffe19 3.1.1Kryptosysteme19 3.1.2Block- und Stromchiffren20 3.2Symmetrische Kryptosysteme23 3.2.1Cäsar-Chiffre und One-Time-Pad23 3.2.2Der DES-Algorithmus24 3.2.3Weitere Algorithmen27 3.3Asymmetrische Kryptosysteme29 3.3.1Einführende Bemerkungen29 3.3.2Der RSA-Algorithmus30 3.3.3Weitere Verfahren31 3.4Hashfunktionen32 3.4.1SHA32 3.4.2MD4 und seine Varianten32 3.4.3RIPEMD-16033 3.4.4MDC-233 3.4.5Message Authentication Codes34 3.5Digitale Signaturen34 3.5.1RSA-Signaturen34 3.5.2ElGamal-Signaturen und DSA34 3.6Kryptographische Protokolle35 3.6.1Festcodes und Wechselcodes35 3.6.2Bidirektionale Protokolle36 3.6.3Weitere Protokolle37 4.Angriffe auf Kryptosysteme39 4.1Angriffe auf Kryptosysteme39 4.1.1Angriffsklassen39 4.1.2Brute-Force-Angriff40 4.1.3Kryptanalyse41 4.2Angriffe auf Protokolle42 4.2.1Einfache Angriffe42 4.2.2Arglistige Täuschung42 4.3Schwachstelle [...]

Geheimsprachen Albrecht Beutelspacher 2013-06-07 Wer glaubt, Geheimsprachen und Geheimcodes seien bestenfalls für Agenten, der irrt. Fernbedienungen, Geldautomaten, Handys und Smartphones,

Transaktionen im Internet, all dies und noch einiges mehr würde ohne Kryptographie nicht funktionieren. Das Buch bietet einen gut lesbaren, umfassenden Einblick in die Wissenschaft sowie in die vielfältigen Techniken des Ver- und Entschlüsselns und ihre zeitgenössischen Anwendungen.

Security Issues in Mobile NFC Devices Michael Roland 2015-02-11 This work provides an assessment of the current state of near field communication (NFC) security, it reports on new attack scenarios, and offers concepts and solutions to overcome any unresolved issues. The work describes application-specific security aspects of NFC based on exemplary use-case scenarios and uses these to focus on the interaction with NFC tags and on card emulation. The current security architectures of NFC-enabled cellular phones are evaluated with regard to the identified security aspects.

Angewandte Kryptographie Bruce Schneier 2006

IT-Sicherheit für TCP/IP- und IoT-Netzwerke Steffen Wendzel 2018-08-22 Die Bedeutung der digitalen Infrastruktur, insbesondere von Netzwerken, ist in den letzten zehn Jahren kontinuierlich gestiegen. Das gilt gleichermaßen für die IT-Sicherheit. Denn ohne sichere Netzwerke können Technologien wie Künstliche Intelligenz oder das Internet der Dinge weder betrieben noch weiterentwickelt werden. Dieses Buch liefert das Fundament, um die Konzeption von TCP/IP- und IoT-Netzwerken und ihre Sicherheit in einer zunehmend vernetzten Welt zu verstehen. Es vereint praxisrelevantes Know-how mit den wissenschaftlichen Grundlagen und aktuellen Forschungsideen zu einem umfassenden Werk. Der Autor legt großen Wert darauf, die Grundlagen der Netzwerktechnik und der IT-Sicherheit verständlich und ausführlich darzustellen. Daneben greift er auch die folgenden Themen auf: · Die Kryptographie, ihre historischen und modernen Verfahren sowie ihre Anwendung beispielsweise in VPNs (Virtual Private Networks) · Die wichtigsten Angriffs- und Verteidigungsmethoden für Netzwerke · Die Sicherheit des Internets der Dinge und sein Einsatz etwa in Smart Buildings und Industriesteueranlagen Das Buch ist so konzipiert, dass Leserinnen und Leser mit einem eher praktischen Zugang zum Thema IT- und Netzwerksicherheit genauso profitieren wie jene mit einem mehr theoretischen Zugang. Durch zahlreiche Übungen – inklusive klassischer Klausuraufgaben – ist es sowohl für die Lehre als auch für das Selbststudium bestens geeignet. Zusatzmaterial wie Vorlesungsunterlagen und selektierte Lösungen zu den Übungen stehen online zum Download zur Verfügung.

Crypto-Politics Linda Monsees 2019-07-19 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.