Secure Elliptic Curve Generation And Key Establishment On

This is likewise one of the factors by obtaining the soft documents of this **Secure Elliptic Curve Generation And Key Establishment On** by online. You might not require more mature to spend to go to the books inauguration as without difficulty as search for them. In some cases, you likewise pull off not discover the pronouncement Secure Elliptic Curve Generation And Key Establishment On that you are looking for. It will completely squander the time.

However below, afterward you visit this web page, it will be appropriately definitely simple to acquire as well as download guide Secure Elliptic Curve Generation And Key Establishment On

It will not agree to many get older as we run by before. You can reach it even though action something else at home and even in your workplace. so easy! So, are you question? Just exercise just what we have enough money under as competently as review **Secure Elliptic Curve Generation And Key Establishment On** what you past to read!

Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems - Lorenzo Cavallaro 2013-05-21
This volume constitutes the refereed proceedings of the 7th IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Security and Privacy of Mobile Devices in Wireless Communication, WISTP 2013, held in Heraklion, Crete, Greece, in May 2013. The 9 revised full papers presented together with two keynote speeches were carefully reviewed and selected from 19 submissions. The scope of the workshop spans the theoretical aspects of cryptography and cryptanalysis, mobile security, smart cards and embedded devices.
Information Security Applications - Jae-Kwang Lee 2007-05-30
This book constitutes the refereed proceedings of the 7th International Workshop on Information Security Applications, WISA 2006, held in Jeju Island, Korea in August 2006. Coverage in the 30 revised full papers includes public key crypto applications and virus protection, cyber indication and intrusion detection, biometrics and security trust management, secure software and systems, smart cards and secure hardware, and mobile security.
Security in Cyber-Physical Systems - Ali Ismail Awad 2021-03-05
This book is a relevant reference for any readers interested in the security aspects of Cyber-Physical Systems and particularly useful for those looking to keep informed on the latest advances in this dynamic area. Cyber-Physical Systems (CPSs) are characterized by the intrinsic combination of software and physical components. Inherent elements often include wired or wireless data communication, sensor devices, real-time operation and automated control of physical elements. Typical examples of associated application areas include industrial control systems, smart grids, autonomous vehicles and avionics, medial monitoring and robotics. The incarnation of the CPSs can therefore range from considering individual Internet-of-Things devices through to large-scale infrastructures. Presented across ten chapters authored by international researchers in the field from both academia and industry, this book offers a series of high-quality contributions that collectively address and analyze the state of the art in the security of Cyber-Physical Systems and related technologies. The chapters themselves include an effective mix of theory and applied content, supporting an understanding of the underlying security issues in the CPSs domain, alongside related coverage of the technological advances and solutions proposed to address them. The chapters comprising the later portion of the book are specifically focused upon a series of case examples, evidencing how the protection concepts can translate into practical application.
Guide to Elliptic Curve Cryptography - Darrel Hankerson 2004-01-08
After two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features & Benefits: * Breadth of coverage and unified, integrated approach to elliptic curve cryptosystems * Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology * Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic * Distills complex mathematics and algorithms for easy understanding * Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software tools This comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security.
Case Studies in Secure Computing - Biju Issac 2014-08-29
In today's age of wireless and mobile computing, network and computer security is paramount. Case Studies in Secure Computing: Achievements and Trends gathers the latest research from researchers who share their insights and best practices through illustrative case studies.This book examines the growing security attacks and countermeasures in the s
Computer and Information Security Handbook - John R. Vacca 2017-05-10
Computer and Information Security Handbook, Third Edition, provides the most current and complete reference on computer security available in one volume. The book offers deep coverage of an extremely wide range of issues in computer and cybersecurity theory, applications, and best practices, offering the latest insights into established and emerging technologies and advancements. With new parts devoted to such current topics as Cloud Security, Cyber-Physical Security, and Critical Infrastructure Security, the book now has 100 chapters written by leading experts in their fields, as well as 12 updated appendices and an expanded glossary. It continues its successful format of offering problem-solving techniques that use real-life case studies, checklists, hands-on exercises, question and answers, and summaries. Chapters new to this edition include such timely topics as Cyber Warfare, Endpoint Security, Ethical Hacking, Internet of Things Security, Nanoscale Networking and Communications Security, Social Engineering, System Forensics, Wireless Sensor Network Security, Verifying User and Host Identity, Detecting System Intrusions, Insider Threats, Security Certification and Standards Implementation, Metadata Forensics, Hard Drive Imaging, Context-Aware Multi-Factor Authentication, Cloud Security, Protecting Virtual Infrastructure, Penetration Testing, and much more. Written by leaders in the field Comprehensive and up-to-date coverage of the latest security technologies, issues, and best practices Presents methods for analysis, along with problem-solving techniques for implementing practical solutions
Cryptography and Security Services: Mechanisms and Applications - Mogollon, Manuel 2008-01-31
Addresses cryptography from the perspective of security services and mechanisms available to implement them. Discusses issues such as e-mail security, public-key architecture, virtual private networks, Web services security, wireless security, and confidentiality and integrity. Provides a working knowledge of fundamental encryption algorithms and systems supported in information technology and secure communication networks.
Distributed Computing and Networking - Mainak Chatterjee 2014-01-02
This book constitutes the proceedings of the 15th International Conference on Distributed Computing and Networking, ICDCN 2014, held in Coimbatore, India, in January 2014. The 32 full papers and 8 short papers presented in this volume were carefully reviewed and selected from 110 submissions. They are organized in topical sections named: mutual exclusion, agreement and consensus; parallel and multi-core computing; distributed algorithms; transactional memory; P2P and

distributed networks; resource sharing and scheduling; cellular and cognitive radio networks and backbone networks.

Wireless Network Security - Lei Chen 2013-08-23

Wireless Network Security Theories and Applications discusses the relevant security technologies, vulnerabilities, and potential threats, and introduces the corresponding security standards and protocols, as well as provides solutions to security concerns. Authors of each chapter in this book, mostly top researchers in relevant research fields in the U.S. and China, presented their research findings and results about the security of the following types of wireless networks: Wireless Cellular Networks, Wireless Local Area Networks (WLANs), Wireless Metropolitan Area Networks (WMANs), Bluetooth Networks and Communications, Vehicular Ad Hoc Networks (VANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), and Radio Frequency Identification (RFID). The audience of this book may include professors, researchers, graduate students, and professionals in the areas of Wireless Networks, Network Security and Information Security, Information Privacy and Assurance, as well as Digital Forensics. Lei Chen is an Assistant Professor at Sam Houston State University, USA; Jiahuang Ji is an Associate Professor at Sam Houston State University, USA; Zihong Zhang is a Sr. software engineer at Jacobs Technology, USA under NASA contract.

2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) - IEEE Staff 2019-04-09

This international conference provides a unique forum to discuss practical approaches and state of the art findings in using the applied electrical engineering and computing technologies to solve national problems that face Jordan and other developing countries

Encyclopedia of Cryptography and Security - Henk C.A. van Tilborg 2014-07-08

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.

Advances in Wireless Sensors and Sensor Networks - Subhas Chandra Mukhopadhyay 2010-04-16

In recent times wireless sensors and sensor networks have become a great interest to research, scientific and technological community. Though the sensor networks have been in place for more than a few decades now, the wireless domain has opened up a whole new application spaces of sensors. Wireless sensors and sensor networks are different from traditional wireless networks as well computer networks and therefore pose more challenges to solve such as limited energy, restricted life time, etc. This book intends to illustrate and to collect recent advances in wireless sensors and sensor networks, not as an encyclopedia but as clever support for scientists, students and researchers in order to stimulate exchange and discussions for further developments.

Information Security Management Handbook, Volume 6 - Harold F. Tipton 2016-04-19

Updated annually, the Information Security Management Handbook, Sixth Edition, Volume 6 is the most comprehensive and up-to-date reference available on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay

Introduction to Computer Networks and Cybersecurity - Chwan-Hwa (John) Wu 2016-04-19

If a network is not secure, how valuable is it? Introduction to Computer Networks and Cybersecurity takes an integrated approach to networking and cybersecurity, highlighting the interconnections so that you quickly understand the complex design issues in modern networks. This full-color book uses a wealth of examples and illustrations to effective

IoT Security - Madhusanka Liyanage 2020-02-10

An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

Security in RFID and Sensor Networks - Paris Kitsos 2016-04-19

In the past several years, there has been an increasing trend in the use of Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) as well as in the integration of both systems due to their complementary nature, flexible combination, and the demand for ubiquitous computing. As always, adequate security remains one of the open areas of concern before wide deployment of RFID and WSNs can be achieved. Security in RFID and Sensor Networks is the first book to offer a comprehensive discussion on the security challenges and solutions in RFID, WSNs, and integrated RFID and WSNs, providing an essential reference for those who regularly interface with these versatile technologies. Exposes Security Risks The book begins with a discussion of current security issues that threaten the effective use of RFID technology. The contributors examine multi-tag systems, relay attacks, authentication protocols, lightweight cryptography, and host of other topics related to RFID safety. The book then shifts the focus to WSNs, beginning with a background in sensor network security before moving on to survey intrusion detection, malicious node detection, jamming, and other issues of concern to WSNs and their myriad of applications. Offers Viable Solutions In each chapter, the contributors propose effective solutions to the plethora of security challenges that confront users, offering practical examples to aid in intuitive understanding. The last part of the book reviews the security problems inherent in integrated RFID & WSNs. The book ends with a glimpse of the future possibilities in

these burgeoning technologies and provides recommendations for the proactive design of secure wireless embedded systems.

Security in Wireless Mesh Networks - Yan Zhang 2008-08-21

Wireless mesh networks (WMN) encompass a new area of technology set to play an important role in the next generation wireless mobile networks. WMN is characterized by dynamic self-organization, self-configuration, and self-healing to enable flexible integration, quick deployment, easy maintenance, low costs, high scalability, and reliable services.

Wireless Security and Cryptography - Nicolas Sklavos 2017-12-19

As the use of wireless devices becomes widespread, so does the need for strong and secure transport protocols. Even with this intensified need for securing systems, using cryptography does not seem to be a viable solution due to difficulties in implementation. The security layers of many wireless protocols use outdated encryption algorithms, which have proven unsuitable for hardware usage, particularly with handheld devices. Summarizing key issues involved in achieving desirable performance in security implementations, Wireless Security and Cryptography: Specifications and Implementations focuses on alternative integration approaches for wireless communication security. It gives an overview of the current security layer of wireless protocols and presents the performance characteristics of implementations in both software and hardware. This resource also presents efficient and novel methods to execute security schemes in wireless protocols with high performance. It provides the state of the art research trends in implementations of wireless protocol security for current and future wireless communications. Unique in its coverage of specification and implementation concerns that include hardware design techniques, Wireless Security and Cryptography: Specifications and Implementations provides thorough coverage of wireless network security and recent research directions in the field.

Security in Wireless Communication Networks - Yi Qian 2021-12-01

Receive comprehensive instruction on the fundamentals of wireless security from three leading international voices in the field Security in Wireless Communication Networks delivers a thorough grounding in wireless communication security. The distinguished authors pay particular attention to wireless specific issues, like authentication protocols for various wireless communication networks, encryption algorithms and integrity schemes on radio channels, lessons learned from designing secure wireless systems and standardization for security in wireless systems. The book addresses how engineers, administrators, and others involved in the design and maintenance of wireless networks can achieve security while retaining the broadcast nature of the system, with all of its inherent harshness and interference. Readers will learn: A comprehensive introduction to the background of wireless communication network security, including a broad overview of wireless communication networks, security services, the mathematics crucial to the subject, and cryptographic techniques An exploration of wireless local area network security, including Bluetooth security, Wi-Fi security, and body area network security An examination of wide area wireless network security, including treatments of 2G, 3G, and 4G Discussions of future development in wireless security, including 5G, and vehicular ad-hoc network security Perfect for undergraduate and graduate students in programs related to wireless communication, Security in Wireless Communication Networks will also earn a place in the libraries of professors, researchers, scientists, engineers, industry managers, consultants, and members of government security agencies who seek to improve their understanding of wireless security protocols and practices.

Information Systems Security - Indrajit Ray 2016-11-24

This book constitutes the refereed proceedings of the 12th International Conference on Information Systems Security, ICISS 2016, held in Jaipur, India, in December 2016. The 24 revised full papers and 8 short papers presented together with 4 invited papers were carefully reviewed and selected from 196 submissions. The papers address the following topics: attacks and mitigation; authentication; authorization and information flow control; crypto systems and protocols; network security and intrusion detection; privacy; software security; and wireless, mobile and IoT security.

Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks - Sagayam, K. Martin 2020-06-12

Wireless sensor networks have gained significant attention industrially and academically due to their wide range of uses in various fields. Because of their vast amount of applications, wireless sensor networks are vulnerable to a variety of security attacks. The protection of wireless sensor networks remains a challenge due to their resource-constrained nature, which is why researchers have begun applying several branches of artificial intelligence to advance the security of these networks. Research is needed on the development of security practices in wireless sensor networks by using smart technologies. Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks provides emerging research exploring the theoretical and practical advancements of security protocols in wireless sensor networks using artificial intelligence-based techniques. Featuring coverage on a broad range of topics such as clustering protocols, intrusion detection, and energy harvesting, this book is ideally designed for researchers, developers, IT professionals, educators, policymakers, practitioners, scientists, theorists, engineers, academicians, and students seeking current research on integrating intelligent techniques into sensor networks for more reliable security practices.

Number-Theoretic Methods in Cryptology - Jerzy Kaczorowski 2018-03-09

This book constitutes the refereed post-conference proceedings of the First International Conference on Number-Theoretic Methods in Cryptology, NuTMiC 2017, held in Warsaw, Poland, in September 2017.The 15 revised full papers presented in this book together with 3 invited talks were carefully reviewed and selected from 32 initial submissions. The papers are organized in topical sections on elliptic curves in cryptography; public-key cryptography; lattices in cryptography; number theory; pseudorandomness; and algebraic structures and analysis.

NETWORKING 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet - Amitabha Das 2008-04-25

GeneralChairs' Message Welcome to the proceedings of the 7th IFIP Networking Conference, which was held in Singapore during 5–9 May 2008. This was the ?rst time that IFIP N- working Conference was held in Asia. An interesting program consisting of high-quality papers from researchers around the world was organized by the Program Chairs, Amitabha Das and Pung Hung Keng. There were a lot of opportunities for the participants to share their researchand views. This was also a great opportunity for researchers and practitioners to network and we hope the friendship will continue beyond Singapore. The success of the conference is due to the hardwork of a lot of people. Our appreciation goes to the authors, who contributed to the conference through their presence and their high-quality research papers. Oursincerethanksto theOrganizingCommittee,whoworkedveryhardh- dling the paper reviews, logistics, publication, ?nancial matters, etc. to ensure that the conference ran smoothly. Special thanks to our committee members from overseas who helped us in publicizing the conference as well as providing valuableinputandsharingtheirexperienceswithus.Wewouldalsoliketothank the numerous paper reviewers for their e?ort and time. Finally,wethankthesponsorsandthelocalinstitutions,NanyangTechnol- ical University and National University of Singapore, for lending their support to the conference.

Cryptography for Developers - Tom St Denis 2006-12-01

The only guide for software developers who must learn and implement cryptography safely and cost effectively. Cryptography for Developers begins with a chapter that introduces the subject of cryptography to the reader. The second chapter discusses how to implement large integer arithmetic as required by RSA and ECC public key algorithms The subsequent chapters discuss the implementation of symmetric ciphers, one-way hashes, message authentication codes, combined authentication and encryption modes, public key cryptography and finally portable coding practices. Each chapter includes in-depth discussion on memory/size/speed performance trade-offs as well as what cryptographic problems are solved with the specific topics at hand. The author is the developer of the industry standard cryptographic suite of tools called LibTom A regular expert speaker at industry conferences and events on this development

Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks - Olivier Markowitch 2009-08-28

This volume contains the 12 papers presented at the WISTP 2009 conference, held in Brussels, Belgium in September 2009. WISTP 2009 was the third int- national workshop devoted to information security theory and practice. WISTP 2009 built on the successful WISTP 2007 and 2008 conferences, held in Heraklion, Crete, Greece and Seville, Spain in May 2007 and May 2008, - spectively. The proceedings of WISTP 2007 and WISTP 2008 were published as volumes 4462 and 5019 of the Lecture Notes in Computer Science series. This workshop received the following support: – Co-sponsored by IFIP WG 11. 2 Small System

Security – Co-sponsored by VDE ITG – Technical sponsorship of the IEEE Systems, Man & Cybernetics Society – Supported by the Technical Committee on Systems Safety and Security – Organized in cooperation with the ACM SIGSAC – Supported by ENISA – Supported by the Institute for Systems and Technologies of Information, Control and Communication (INSTICC) These proceedings contain 12 original papers covering a range of theoretical and practical topics in information security. For the purposes of the organi- tion of the WISTP program, the papers were divided into four main categories, namely: – Mobility – Attacks and Secure Implementations – Performance and Security – Cryptography
The12papersincludedherewereselectedfromatotalof27submissions. The refereeing process was rigorous,involving at least three (and mostly four or ?ve) independent reports being prepared for each submission.

IoT Security - Madhusanka Liyanage 2019-12-02
An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

Wireless Technologies: Concepts, Methodologies, Tools and Applications - Management Association, Information Resources 2011-08-31
Contains the latest research, case studies, theories, and methodologies within the field of wireless technologies.

Cyber Security Applications for Industry 4.0 - R Sujatha 2022-10-20
Cyber Security Applications for Industry 4.0 (CSAI 4.0) provides integrated features of various disciplines in Computer Science, Mechanical, Electrical, and Electronics Engineering which are defined to be Smart systems. It is paramount that Cyber-Physical Systems (CPS) provide accurate, real-time monitoring and control for smart applications and services. With better access to information from real-time manufacturing systems in industrial sectors, the CPS aim to increase the overall equipment effectiveness, reduce costs, and improve efficiency. Industry 4.0 technologies are already enabling numerous applications in a variety of industries. Nonetheless, legacy systems and inherent vulnerabilities in an organization's technology, including limited security mechanisms and logs, make the move to smart systems particularly challenging. Features: Proposes a conceptual framework for Industry 4.0-based Cyber Security Applications concerning the implementation aspect Creates new business models for Industrialists on Control Systems and provides productive workforce transformation Outlines the potential development and organization of Data Protection based on strategies of cybersecurity features and planning to work in the new area of Industry 4.0 Addresses the protection of plants from the frost and insects, automatic hydroponic irrigation techniques, smart industrial farming and crop management in agriculture relating to data security initiatives The book is primarily aimed at industry professionals, academicians, and researchers for a better understanding of the secure data transition between the Industry 4.0 enabled connected systems and their limitations

Financial Cryptography and Data Security - Nicolas Christin 2014-11-08
This book constitutes the thoroughly refereed post-conference proceedings of the 18th International Conference on Financial Cryptography and Data Security (FC 2014), held in Christ Church, Barbados, in March 2014. The 19 revised full papers and 12 short papers were carefully selected and reviewed from 165 abstract registrations and 138 full papers submissions. The papers are grouped in the following topical sections: payment systems, case studies, cloud and virtualization, elliptic curve cryptography, privacy-preserving systems, authentication and visual encryption, network security, mobile system security, incentives, game theory and risk, and bitcoin anonymity.

Secure Key Establishment - Kim-Kwang Raymond Choo 2008-10-25
Research on Secure Key Establishment has become very active within the last few years. Secure Key Establishment discusses the problems encountered in this field. This book also introduces several improved protocols with new proofs of security. Secure Key Establishment identifies several variants of the key sharing requirement. Several variants of the widely accepted Bellare and Rogaway (1993) model are covered. A comparative study of the relative strengths of security notions between these variants of the Bellare–Rogaway model and the Canetti–Krawczyk model is included. An integrative framework is proposed that allows protocols to be analyzed in a modified version of the Bellare–Rogaway model using the automated model checker tool. Secure Key Establishment is designed for advanced level students in computer science and mathematics, as a secondary text or reference book. This book is also suitable for practitioners and researchers working for defense agencies or security companies.

Mastering Ethereum - Andreas M. Antonopoulos 2018-11-13
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

Risks and Security of Internet and Systems - Akka Zemmari 2019-01-24
This book constitutes the revised selected papers from the 13th International Conference on Risks and Security of Internet and Systems, CRiSIS 2018, held in Arcachon, France, in October 2018. The 12 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 34 submissions. They cover diverse research themes that range from classic topics, such as vulnerability analysis and classification; apps security; access control and filtering; cloud security; cyber-insurance and cyber threat intelligence; human-centric security and trust; and risk analysis.

Guide to Elliptic Curve Cryptography - Darrel Hankerson 2006-06-01
After two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features & Benefits: * Breadth of coverage and unified, integrated approach to elliptic curve cryptosystems * Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology * Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic * Distills complex mathematics and algorithms for easy understanding * Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software tools This comprehensive, highly focused reference is a useful and indispensable

resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security.

Security and Privacy Assurance in Advancing Technologies: New Developments - Nemati, Hamid 2010-11-30

"This book provides a comprehensive collection of knowledge from experts within the field of information security and privacy and explores the changing roles of information technology and how this change will impact information security and privacy"--Provided by publisher.

CCNA Security 210-260 Official Cert Guide - Omar Santos 2015-09-01

Trust the best selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for exam success. They are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. --Master Cisco CCNA Security 210-260 Official Cert Guide exam topics --Assess your knowledge with chapter-opening quizzes --Review key concepts with exam preparation tasks This is the eBook edition of the CCNA Security 210-260 Official Cert Guide. This eBook does not include the companion CD-ROM with practice exam that comes with the print edition. CCNA Security 210-260 Official Cert Guide presents you with an organized test-preparation routine through the use of proven series elements and techniques. “Do I Know This Already?” quizzes open each chapter and enable you to decide how much time you need to spend on each section. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. CCNA Security 210-260 Official Cert Guide focuses specifically on the objectives for the Cisco CCNA Security exam. Networking Security experts Omar Santos and John Stuppi share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. Well regarded for its level of detail, assessment features, comprehensive design scenarios, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The official study guide helps you master all the topics on the CCNA Security exam, including --Networking security concepts --Common security threats --Implementing AAA using IOS and ISE --Bring Your Own Device (BYOD) --Fundamentals of VPN technology and cryptography --Fundamentals of IP security --Implementing IPsec site-to-site VPNs --Implementing SSL remote-access VPNs using Cisco ASA --Securing Layer 2 technologies --Network Foundation Protection (NFP) --Securing the management plane on Cisco IOS devices --Securing the data plane --Securing routing protocols and the control plane --Understanding firewall fundamentals --Implementing Cisco IOS zone-based firewalls --Configuring basic firewall policies on Cisco ASA --Cisco IPS fundamentals --Mitigation technologies for e-mail- and web-based threats --Mitigation technologies for endpoint threats CCNA Security 210-260 Official Cert Guide is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit http://www.cisco.com/web/learning/index.html.

CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide - Omar Santos 2020-04-14

Trust the best-selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for exam success. They are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. Master Cisco CCNP and CCIE Security Core SCOR 350-701 exam topics Assess your knowledge with chapter-opening quizzes Review key concepts with exam preparation tasks This is the eBook edition of the CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. This eBook does not include access to the companion website with practice exam that comes with the print edition. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide presents you with an organized test preparation routine through the use of proven series elements and techniques. “Do I Know This Already?” quizzes open each chapter and allow you to decide how much time you need to spend on each section. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, focuses specifically on the objectives for the Cisco CCNP and CCIE Security SCOR exam. Best-selling author and leading security engineer Omar Santos shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. Well regarded for its level of detail, assessment features, comprehensive design scenarios, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. The official study guide helps you master all the topics on the CCNP and CCIE Security SCOR 350-701 exam, including: Cybersecurity fundamentals Cryptography Software-Defined Networking security and network programmability Authentication, Authorization, Accounting (AAA) and Identity Management Network visibility and segmentation Infrastructure security Cisco next-generation firewalls and intrusion prevention systems Virtual Private Networks (VPNs) Securing the cloud Content security Endpoint protection and detection CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/web/learning/index.html

Embedded Computing Systems: Applications, Optimization, and Advanced Design - Khalgui, Mohamed 2013-04-30

Embedded computing systems play an important and complex role in the functionality of electronic devices. With our daily routines becoming more reliant on electronics for personal and professional use, the understanding of these computing systems is crucial. Embedded Computing Systems: Applications, Optimization, and Advanced Design brings together theoretical and technical concepts of intelligent embedded control systems and their use in hardware and software architectures. By highlighting formal modeling, execution models, and optimal implementations, this reference source is essential for experts, researchers, and technical supporters in the industry and academia.

Mobile Internet Security - Ilsun You 2020-11-01

This book constitutes the refereed proceedings of the 4th International Symposium on Mobile Internet Security, MobiSec 2019, held in Taichung, Taiwan, in October 2019. The 13 revised full papers presented were carefully reviewed and selected from 44 submissions. The papers are organized in the topical sections: mobile internet security; mobile application and security; vehicular network security; deep learning applications.

Understanding and Applying Cryptography and Data Security - Adam J. Elbirt 2009-04-09

A How-to Guide for Implementing Algorithms and Protocols Addressing real-world implementation issues, Understanding and Applying Cryptography and Data Security emphasizes cryptographic algorithm and protocol implementation in hardware, software, and embedded systems. Derived from the author’s teaching notes and research publications, the text is designed for electrical engineering and computer science courses. Provides the Foundation for Constructing Cryptographic Protocols The first several chapters present various types of symmetric-key cryptographic algorithms. These chapters examine basic substitution ciphers, cryptanalysis, the Data Encryption Standard (DES), and the Advanced Encryption Standard (AES). Subsequent chapters on public-key cryptographic algorithms cover the underlying mathematics behind the computation of inverses, the use of fast exponentiation techniques, tradeoffs between public- and symmetric-key algorithms, and the minimum key lengths necessary to maintain acceptable levels of security. The final chapters present the components needed for the creation of cryptographic protocols and investigate different security services and their impact on the construction of cryptographic protocols. Offers Implementation Comparisons By examining tradeoffs between code size, hardware logic resource requirements, memory usage, speed and throughput, power consumption, and more, this textbook provides students with a feel for what they may encounter in actual job situations. A solutions manual is available to qualified instructors with course adoptions.

International Conference on Security and Privacy in Communication Networks - Jing Tian 2015-11-21

This 2-volume set constitutes the thoroughly refereed post-conference proceedings of the 10th International Conference on Security and Privacy in Communication Networks, SecureComm 2014, held in Beijing, China, in September 2014. The 27 regular and 17 short papers presented were carefully reviewed. It also presents 22 papers accepted for four

workshops (ATCS, SSS, SLSS, DAPRO) in conjunction with the conference, 6 doctoral symposium papers and 8 poster papers. The papers are grouped in the following topics: security and privacy in wired, wireless, mobile, hybrid, sensor, ad hoc networks; network intrusion detection and prevention, firewalls, packet filters; malware, and distributed denial of service; communication privacy and anonymity; network and internet forensics techniques; public key infrastructures, key management, credential management; secure routing, naming/addressing, network management; security and privacy in pervasive and ubiquitous computing; security & privacy for emerging technologies: VoIP, peer-to-peer and overlay network systems; security & isolation in data center networks; security & isolation in software defined networking.