Data Security And Encryption Technique For Cloud Storage

This book constitutes the proceedings of the Second International Conference on Codes, Cryptology and Information Security, C2SI 2017, held in Rabat, Morocco, in April 2017. The 19 regular papers presented together with 5 invited talks were carefully reviewed and selected from 72 submissions. The first aim of this conference is to pay homage to Claude Carlet for his valuable contribution in teaching and disseminating knowledge in coding theory and cryptography worldwide, especially in Africa. The second aim of the conference is to provide an international forum for researchers from academia and practitioners from industry from all over the world for discussion of all forms of cryptology, coding theory and information security.

Encryption protects information stored on smartphones, laptops, and other devices - in some cases by default. Encrypted communications are provided by widely used computing devices and services - such as smartphones, laptops, and messaging applications - that are used by hundreds of millions of users. Individuals, organizations, and governments rely on encryption to counter threats from a wide range of actors, including unsophisticated and sophisticated criminals, foreign intelligence agencies, and repressive governments. Encryption on its own does not solve the challenge of providing effective security for data and systems, but it is an important tool. At the same time, encryption is relied on by criminals to avoid investigation and prosecution, including criminals who may unknowingly benefit from default settings as well as those who deliberately use encryption. Thus, encryption complicates law enforcement and intelligence investigations. When communications are encrypted "end-to-end," intercepted messages cannot be understood. When a smartphone is locked and encrypted, the contents cannot be read if the phone is seized by investigators. Decrypting the Encryption Debate reviews how encryption is used, including its applications to cybersecurity; its role in protecting privacy and civil liberties; the needs of law enforcement and the intelligence community for information; technical and policy options for accessing plaintext; and the international landscape. This book describes the context in which decisions about providing authorized government agencies access to the plaintext version of encrypted information would be made and identifies and characterizes possible mechanisms and alternative means of obtaining information.

Regulatory and industry-specific requirements, such as SOX, Visa PCI, HIPAA, and so on, require that sensitive data must be stored securely and protected against unauthorized access or modifications. Several of the requirements state that data must be encrypted. IBM® i5/OS® offers several options that allow customers to encrypt data in the database tables. However, encryption is not a trivial task. Careful planning is essential for successful implementation of data encryption project. In the worst case, you would not be able to retrieve clear text information from encrypted data. This IBM Redbooks® publication is designed to help planners, implementers, and programmers by providing three key pieces of information: Part 1, "Introduction to data encryption" on page 1, introduces key concepts, terminology, algorithms, and key management. Understanding these is important to follow the rest of the book. If *you are already familiar with the general concepts of cryptography and the data encryption aspect of it, you may skip this part. Part 2, "Planning for data encryption" on page 37, provides critical information for planning a data encryption project on i5/OS. Part 3, "Implementation of data encryption" on page 113, provides various implementation scenarios with a step-by-step guide.*

Cyber security is the protection of information systems, hardware, software, and information as well from theft, damages, interruption or misdirection to any of these resources. In other words, cyber security focuses on protecting computers, networks, programs and data (in use, in rest, in motion) from unauthorized or unintended access, change or destruction. Therefore, strengthening the security and resilience of cyberspace has become a vital homeland security mission. Cyber security attacks are growing exponentially. Security specialists must occupy in the lab, concocting new schemes to preserve the resources and to control any new attacks. Therefore, there are various emerging algorithms and techniques viz. DES, AES, IDEA, WAKE, CAST5, Serpent Algorithm, Chaos-Based Cryptography McEliece, Niederreiter, NTRU, Goldreich–Goldwasser–Halevi, Identity Based Encryption, and Attribute Based Encryption. There are numerous applications of security algorithms like cyber security, web security, e-commerce, database security, smart card technology, mobile security, cloud security, digital signature, etc. The book offers comprehensive coverage of the most essential topics, including: Modular Arithmetic, Finite Fields Prime Number, DLP, Integer Factorization Problem Symmetric Cryptography Asymmetric Cryptography Post-Quantum Cryptography Identity Based Encryption Attribute Based Encryption Key Management Entity Authentication, Message Authentication Digital Signatures Hands-On "SageMath" This book serves as a textbook/reference book for UG, PG, PhD students, Teachers, Researchers and Engineers in the disciplines of Information Technology, Computer Science and Engineering, and Electronics and Communication Engineering.

Modern Cryptography

Computer Security and Cryptography

Applied Mathematics for Encryption and Information Security

Decrypting the Encryption Debate

Use of a Two Key Cipher Technique in a Data Base Security System

IBM System i Security: Protecting i5/OS Data with Encryption

Everyone wants privacy and security online, something that most computer users have more or less given up on as far as their personal data is concerned. There is no shortage of good encryption software, and no shortage of books, articles and essays that purport to be about how to use it. Yet there is precious little for ordinary users who want just enough information about encryption to use it safely and securely and appropriately--WITHOUT having to become experts in cryptography. Data encryption is a powerful tool, if used properly. Encryption turns ordinary, readable data into what looks like gibberish, but gibberish that only the end user can turn back into readable data again. The difficulty of encryption has much to do with deciding what kinds of threats one needs to protect against and then using the proper tool in the correct way. It's kind of like a manual transmission in a car: learning to drive with one is easy; learning to build one is hard. The goal of this title is to present just enough for an average reader to begin protecting his or her data, immediately. Books and *articles currently available about encryption start out with statistics and reports on the costs of data loss, and quickly get bogged down in cryptographic theory and jargon followed by attempts to comprehensively list all the latest and greatest tools and techniques. After step-by-step walkthroughs of the download and install process, there's precious little room left for what most readers really want: how to encrypt a thumb drive or email message, or digitally sign a data file. There are terabytes of content that explain how cryptography works, why it's important, and all the different pieces of software that can be used to do it; there is precious little content available that couples concrete threats to data with explicit responses to those threats. This title fills that niche. By reading this title readers will be provided with a step by step hands-on guide that includes: Simple descriptions of actual threat scenarios Simple, step-by-step instructions for securing data How to use open source, time-proven and peer-reviewed cryptographic software Easy to follow tips for safer computing Unbiased and platform-independent coverage of encryption tools and techniques Simple descriptions of actual threat scenarios Simple, step-by-step instructions for securing data How to use open source, time-proven and peer-reviewed cryptographic software Easy-to-follow tips for safer computing Unbiased and platform-independent coverage of encryption tools and techniques*

Privacy protection within large databases can be a challenge. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. HCI Challenges and Privacy Preservation in Big Data Security is an informative scholarly publication that discusses how human-computer interaction impacts privacy and security in almost all sectors of modern life. Featuring relevant topics such as large scale security data, threat detection, big data encryption, and identity management, this reference source is ideal for academicians, researchers, advanced-level students, and engineers that are interested in staying current on the advancements and drawbacks of human-computer interaction within the world of big data.

Encryption algorithms. Cryptographic technique. Access controls. Information controls. Inference controls.

Coded representation, Coding (programming), Cryptography, Data representation, Data transmission, Data codes, Data security, Interfaces (data processing), Algorithms, Data storage protection, Programming techniques, Data processing

Information Technology. Security Techniques. Encryption Algorithms. Asymmetric Ciphers

COMBINING MULTIPLE ENCRYPTION ALGORITHMS AND A DISTRIBUTED SYSTEM TO IMPROVE DATABASE SECURITY IN CLOUD COMPUTING.

A Framework for Decision Makers

Codes, Cryptology and Information Security

Information Technology. Security Techniques. Encryption Algorithms. Stream Ciphers

Scope of the conference will be to provide inroads to enhance the security and privacy to ever increasing cyber threats and digital crimes It will also encompass all areas of digital privacy, thus providing plausible solutions to these problems

This textbook is a practical yet in depth guide to cryptography and its principles and practices. The book places cryptography in real-world security situations using the hands-on information contained throughout the chapters. Prolific author Dr. Chuck Easttom lays out essential math skills and fully explains how to implement cryptographic algorithms in today's data protection landscape. Readers learn and test out how to use ciphers and hashes, generate random keys, handle VPN and Wi-Fi security, and encrypt VoIP, Email, and Web communications. The book also covers cryptanalysis, steganography, and cryptographic backdoors and includes a description of quantum computing and its impact on cryptography. This book is meant for those without a strong mathematics background _only just enough math to understand the algorithms given. The book contains a slide presentation, questions and answers, and exercises throughout. Presents a comprehensive coverage of cryptography in an approachable format; Covers the basic math needed for cryptography _number theory, discrete math, and algebra (abstract and linear); Includes a full suite of classroom materials including exercises, Q&A, and examples.

Covering classical cryptography, modern cryptography, and steganography, this volume details how data can be kept secure and private. Each topic is presented and explained by describing various methods, techniques, and algorithms. Moreover, there are numerous helpful examples to reinforce the reader's understanding and expertise with these techniques and methodologies. Features & Benefits: * Incorporates both data encryption and data hiding * Supplies a wealth of exercises and solutions to help readers readily understand the material * Presents information in an accessible, nonmathematical style * Concentrates on specific methodologies that readers can choose from and pursue, for their data-security needs and goals * Describes new topics, such as the advanced encryption standard (Rijndael), quantum cryptography, and elliptic-curve cryptography. The book, with its accessible style, is an essential companion for all security practitioners and professionals who need to understand and effectively use both information hiding and encryption to protect digital data and communications. It is also suitable for self-study in the areas of programming, software engineering, and security.

Data processing, Data security, Data storage protection, Algorithms, Cryptography, Coded representation, Codes, Data conversion, Identification methods

Cloud Security and Privacy

Cyber Security

Challenges and Future Trends

Cryptographic Security Solutions for the Internet of Things

An Enterprise Perspective on Risks and Compliance

Cryptography and Data Security

CYBER SECURITY AND DIGITAL FORENSICS Cyber security is an incredibly important issue that is constantly changing, with new methods, processes, and technologies coming online all the time. Books like this are invaluable to professionals working in this area, to stay abreast of all of these changes. Current cyber threats are getting more complicated and advanced with the rapid evolution of adversarial techniques. Networked computing and portable electronic devices have broadened the role of digital forensics beyond traditional investigations into computer crime. The overall increase in the use of computers as a way of storing and retrieving high-security information requires appropriate security measures to protect the entire computing and communication scenario worldwide. Further, with the introduction of the internet and its underlying technology, facets of information security are becoming a primary concern to protect networks and cyber infrastructures from various threats. This groundbreaking new volume, written and edited by a wide range of professionals in this area, covers broad technical and socio-economic perspectives for the utilization of information and communication technologies and the development of practical solutions in cyber security and digital forensics. Not just for the professional working in the field, but also for the student or academic on the university level, this is a must-have for any library. Audience: Practitioners, consultants, engineers, academics, and other professionals working in the areas of cyber analysis, cyber security, homeland security, national defense, the protection of national critical infrastructures, cyber-crime, cyber vulnerabilities, cyber-attacks related to network systems, cyber threat reduction planning, and those who provide leadership in cyber security management both in public and private sectors

The widespread use of image, audio, and video data makes media content protection increasingly necessary and urgent. For maximum safety, it is no longer sufficient to merely control access rights. In order to fully protect multimedia data from piracy or unauthorized use, it must be secured through encryption prior to its transmission or distribution. Multimedia Content Encryption: Techniques and Applications presents the latest research results in this dynamic field. The book begins with the history of multimedia encryption and then examines general performance requirements of encryption and fundamental encrypting techniques. It discusses common techniques of complete, partial, and compression-combined encryption; as well as the more specialized forms, including perception, scalable, and commutative encryption. In addition, the author reviews watermarking and joint fingerprint embedding and decryption. Later chapters discuss typical attacks on multimedia encryption, as well as the principles for designing secure algorithms and various applications. An exploration of open issues, up-and-coming topics, and areas for further research rounds out the coverage. Shiguo Lian is the author or co-author of more than fifty peer-reviewed journal and conference articles covering topics of network security and multimedia content protection, including cryptography, secure P2P content sharing, digital rights management (DRM), encryption, watermarking, digital fingerprinting, and authentication. By following the techniques outlined in this book, users will be better able to protect the integrity of their multimedia data and develop greater confidence that their data will not be misappropriated.

Bulletproof SSL and TLS is a complete guide to using SSL and TLS encryption to deploy secure servers and web applications. Written by Ivan Ristic, the author of the popular SSL Labs web site, this book will teach you everything you need to know to protect your systems from eavesdropping and impersonation attacks. In this book, you'll find just the right mix of theory, protocol detail, vulnerability and weakness information, and deployment advice to get your job done: - Comprehensive coverage of the ever-changing field of SSL/TLS and Internet PKI, with updates to the digital version - For IT security professionals, help to understand the risks - For system administrators, help to deploy systems securely For developers, help to design and implement secure web applications - Practical and concise, with added depth when details are relevant - Introduction to cryptography and the latest TLS protocol version - Discussion of weaknesses at every level, covering implementation issues, HTTP and browser problems, and protocol vulnerabilities - Coverage of the latest attacks, such as BEAST, CRIME, BREACH, Lucky 13, RC4 biases, Triple Handshake Attack, and Heartbleed - Thorough deployment advice, including advanced technologies, such as Strict Transport Security, Content Security Policy, and pinning - Guide to using OpenSSL to generate keys and certificates and to create and run a private certification authority - Guide to using OpenSSL to test servers for vulnerabilities - Practical advice for secure server configuration using Apache httpd, IIS, Java, Nginx, Microsoft Windows, and Tomcat This book is available in paperback and a variety of digital formats without DRM.

The Internet of Things is a technological revolution that represents the future of computing and communications. Even though efforts have been made to standardize Internet of Things devices and how they communicate with the web, a uniform architecture is not followed. This inconsistency directly impacts and limits security standards that need to be put in place to secure the data being exchanged across networks. Cryptographic Security Solutions for the Internet of Things is an essential reference source that discusses novel designs and recent developments in cryptographic security control procedures to improve the efficiency of existing security mechanisms that can help in securing sensors, devices, networks, communication, and data in the Internet of Things. With discussions on cryptographic algorithms, encryption techniques, and authentication procedures, this book is ideally designed for managers, IT consultants, startup companies, ICT procurement managers, systems and network integrators, infrastructure service providers, students, researchers, and academic professionals.

2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS INBUSH)

A Practical Guide to Secure Computing

Best Practices for Securing Infrastructure

Data Breach and Encryption Handbook

Web Security, Privacy & Commerce

Identity and Data Security for Web Development

Cryptographic access control (CAC) is an approach to securing data by encrypting it with a key, so that only the users in possession of the correct key are able to decrypt the data and/or perform further encryptions. Applications of cryptographic access control will benefit companies, governments and the military where structured access to information is essential. The purpose of this book is to highlight the need for adaptability in cryptographic access control schemes that are geared for dynamic environments, such as the Internet. Adaptive Cryptographic Access Control presents the challenges of designing hierarchical cryptographic key management algorithms to implement Adaptive Access Control in dynamic environments and suggest solutions that will overcome these challenges. Adaptive Cryptographic Access Control is a cutting-edge book focusing specifically on this topic in relation to security and cryptographic access control. Both the theoretical and practical aspects and approaches of cryptographic access control are introduced in this book. Case studies and examples are provided throughout this book.

The era of quantum computing is about to begin, with profound implications for the global economy and the financial system. Rapid development of quantum computing brings both benefits and risks. Quantum computers can revolutionize industries and fields that require significant computing power, including modeling financial markets, designing new effective medicines and vaccines, and empowering artificial intelligence, as well as creating a new and secure way of communication (quantum Internet). But they would also crack many of the current encryption algorithms and threaten financial stability by compromising the security of mobile banking, e-commerce, fintech, digital currencies, and Internet information exchange. While the work on quantum-safe encryption is still in progress, financial institutions should take steps now to prepare for the cryptographic transition, by assessing future and retroactive risks from quantum computers, taking an inventory of their cryptographic algorithms (especially public keys), and building cryptographic agility to improve the overall cybersecurity resilience.

With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercrimes have begun to take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is secured and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists, practitioners, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing data.

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.

Defensive Security Handbook

Information Technology. Security Techniques. Encryption Algorithms. General

A Beginner’s Guide

Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications

Enhancing Video Encryption and Watermarking Robustness and Performance

Research Anthology on Privatizing and Securing Data

Developers, designers, engineers, and creators can no longer afford to pass responsibility for identity and data security onto others. Web developers who don’t understand how to obscure data in transmission, for instance, can open security flaws on a site without realizing it. With this practical guide, you’ll learn how and why everyone working on a system needs to ensure that users and data are protected. Authors Jonathan LeBlanc and Tim Messerschmidt provide a deep dive into the concepts, technology, and programming methodologies necessary to build a secure interface for data and identity—without compromising usability. You’ll learn how to plug holes in existing systems, protect against viable attack vectors, and work in *environments that sometimes are naturally insecure. Understand the state of web and application security today Design security password encryption, and combat password attack vectors Create digital fingerprints to identify users through browser, device, and paired device detection Build secure data transmission systems through OAuth and OpenID Connect Use alternate methods of identification for a second factor of authentication Harden your web applications against attack Create a secure data transmission system using SSL/TLS, and synchronous and asynchronous cryptography This book introduces the state-of-the-art algorithms for data and computation privacy. It mainly focuses on searchable symmetric encryption algorithms and privacy preserving multi-party computation algorithms. This book also introduces algorithms for breaking privacy, and gives intuition on how to design algorithm to counter privacy attacks. Some well-designed differential privacy algorithms are also included in this book. Driven by lower cost, higher reliability, better performance, and faster deployment, data and computing services are increasingly outsourced to clouds. In this computing paradigm, one often has to store privacy sensitive data at parties, that cannot fully trust and perform privacy sensitive computation with parties that again cannot fully trust. For both scenarios, preserving data privacy and computation privacy is extremely important. After the Facebook–Cambridge Analytical data scandal and the implementation of the General Data Protection Regulation by European Union, users are becoming more privacy aware and more concerned with their privacy in this digital world. This book targets database engineers, cloud computing engineers and researchers working in this field. Advanced-level students studying computer science and electrical engineering will also find this book useful as a reference or secondary text.*

You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from *three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security*

Data processing, Data security, Data storage protection, Algorithms, Cryptography, Data transmission, Data codes, Software engineering techniques, Coded representation, Data representation, Coding (programming), Programming techniques

Best Practices

An Introduction to Cyber Security

Information Technology. Security Techniques. Encryption Algorithms. Block Ciphers

Techniques and Applications

Design of New Block and Stream Cipher Encryption Algorithms for Data Security

HCI Challenges and Privacy Preservation in Big Data Security

Most applications these days are at least somewhat network aware, but how do you protect those applications against common network security threats? Many developers are turning to OpenSSL, an open source version of SSL/TLS, which is the most widely used protocol for secure network communications.The OpenSSL library is seeing widespread adoption for web sites that require cryptographic functions to protect a broad range of sensitive information, such as credit card numbers and other financial transactions. The library is the only free, full-featured SSL implementation for C and C++, and it can be used programmatically or from the command line to secure most TCP-based network protocols.Network Security with OpenSSL enables developers to use this protocol much more effectively. Traditionally, getting something simple done in OpenSSL could easily take weeks. This concise book gives you the guidance you need to avoid pitfalls, while allowing you to take advantage of the library?s advanced features. And, instead of bogging you down in the technical details of how SSL works under the hood, this book provides only the information that is necessary to use OpenSSL safely and effectively. In step-by-

step fashion, the book details the challenges in securing network communications, and shows you how to use OpenSSL tools to best meet those challenges.As a system or network administrator, you will benefit from the thorough treatment of the OpenSSL command-line interface, as well as from step-by-step directions for obtaining certificates and setting up your own certification authority. As a developer, you will further benefit from the in-depth discussions and examples of how to use OpenSSL in your own programs. Although OpenSSL is written in C, information on how to use OpenSSL with Perl, Python and PHP is also included.OpenSSL may well answer your need to protect sensitive data. If that?s the case, Network Security with OpenSSL is the only guide available on the subject.

Gain the skills and knowledge needed to create effective data security systems This book updates readers with all the tools, techniques, and concepts needed to understand and implement data security systems. It presents a wide range of topics for a thorough understanding of the factors that affect the efficiency of secrecy, authentication, and digital signature schema. Most importantly, readers gain hands-on experience in cryptanalysis and learn how to create effective cryptographic systems. The author contributed to the design and analysis of the Data Encryption Standard (DES), a widely used symmetric-key encryption algorithm. His recommendations are based on firsthand experience of what does and does not work. Thorough in its coverage, the book starts with a discussion of the history of cryptography, including a description of the basic encryption systems and many of the cipher systems used in the twentieth century. The author then discusses the theory of symmetric- and public-key cryptography. Readers not only discover what cryptography can do to protect sensitive data, but also learn the practical limitations of the technology. The book ends with two chapters that explore a wide range of cryptography applications. Three basic types of chapters are featured to facilitate learning: Chapters that develop technical skills Chapters that describe a cryptosystem and present a method of analysis Chapters that describe a cryptosystem, present a method of analysis, and provide problems to test your grasp of the material and your ability to implement practical solutions With consumers becoming increasingly wary of identity theft and companies struggling to develop safe, secure systems, this book is essential reading for professionals in e-commerce and information technology. Written by a professor who teaches cryptography, it is also ideal for students.

Cloud Security and PrivacyAn Enterprise Perspective on Risks and Compliance"O'Reilly Media, Inc."

Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering applies the principles of cryptographic systems to real-world scenarios, explaining how cryptography can protect businesses' information and ensure privacy for their networks and databases. It delves into the specific security requirements within various emerging application areas and discusses

procedures for engineering cryptography into system design and implementation.

Improvements on Data Security Algorithms for Streaming Multimedia
Data Security Issues and Encryption Algorithms
Information Encryption and Cyphering
Simple Steps to Data Encryption
Intelligent Data Security Solutions for e-Health Applications
Multimedia Content Encryption

E-health applications such as tele-medicine, tele-radiology, tele-ophthalmology, and tele-diagnosis are very promising and have immense potential to improve global healthcare. They can improve access, equity, and quality through the connection of healthcare facilities and healthcare professionals, diminishing geographical and physical barriers. One critical issue, however, is related to the security of data transmission and access to the technologies of medical information. Currently, medical-related identity theft costs billions of dollars each year and altered medical information can put a person’s health at risk through misdiagnosis, delayed treatment or incorrect prescriptions. Yet, the use of hand-held devices for storing, accessing, and transmitting medical information is outpacing the privacy and security protections on those devices. Researchers are starting to develop some imperceptible marks to ensure the tamper-proofing, cost effective, and guaranteed originality of the medical records. However, the robustness, security and efficient image archiving and retrieval of medical data information against these cyberattacks is a challenging area for researchers in the field of e-health applications. Intelligent Data Security Solutions for e-Health Applications focuses on cutting-edge academic and industry-related research in this field, with particular emphasis on interdisciplinary approaches and novel techniques to provide security solutions for smart applications. The book provides an overview of cutting-edge security techniques and ideas to help graduate students, researchers, as well as IT professionals who want to understand the opportunities and challenges of using emerging techniques and algorithms for designing and developing more secure systems and methods for e-health applications. Investigates new security and privacy requirements related to eHealth technologies and large sets of applications Reviews how the abundance of digital information on system behavior is now being captured, processed, and used to improve and strengthen security and privacy Provides an overview of innovative security techniques which are being developed to ensure the guaranteed authenticity of transmitted, shared or stored data/information

"Web Security, Privacy & Commerce" cuts through the hype and the front page stories. It tells readers what the real risks are and explains how to minimize them. Whether a casual (but concerned) Web surfer or a system administrator responsible for the security of a critical Web server, this book will tells users what they need to know.

Cybersecurity is undoubtedly one of the fastest-growing fields. However, there is an acute shortage of skilled workforce. The cybersecurity beginners guide aims at teaching security enthusiasts all about organizational digital assets' security, give them an overview of how the field operates, applications of cybersecurity across sectors and industries, and skills and certifications one needs to build and scale up a career in this field.

This book takes an in-depth look at the issue of escalating data breaches and their legal ramifications. It focuses on the law and its implications, encryption technology, recognized methods of resolving a breach, and many related aspects of information security. The book also examines a number of the major data breach incidents from a variety of legal and technology perspectives, and provides instructive graphics to illustrate the methodologies hackers use to cause these breaches.

Second International Conference, C2SI 2017, Rabat, Morocco, April 10–12, 2017, Proceedings - In Honor of Claude Carlet

Information Technology. Security Techniques. Encryption Algorithms. Identity-Based Ciphers

Understanding and Applying Cryptography and Data Security

Bulletproof SSL and TLS

Network Security with OpenSSL

Cryptography for Secure Communications

Despite the increase of high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations don't have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost. Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Learn fundamentals of starting or redesigning an InfoSec program Create a base set of policies, standards, and procedures Plan and design incident response, disaster recovery, compliance, and physical security Bolster Microsoft and Unix systems, network infrastructure, and password management Use segmentation practices and designs to compartmentalize your network Explore automated process and tools for *vulnerability management Securely develop code to reduce exploitable errors Understand basic penetration testing concepts through purple teaming Delve into IDS, IPS, SOC, logging, and monitoring*

This book comprises select proceedings of the annual convention of the Computer Society of India. Divided into 10 topical volumes, the proceedings present papers on state-of-the-art research, surveys, and succinct reviews. The volume covers diverse topics ranging from information security to cryptography and from encryption to intrusion detection. This book focuses on Cyber Security. It aims at informing the readers about the technology in general and the internet in particular. The book uncovers the various nuances of information security, cyber security and its various dimensions. This book also covers latest security trends, ways to combat cyber threats including the detection and mitigation of security threats and risks. The contents of this book will prove useful to professionals and researchers alike.

This book focuses on three topics. The first topic is the effectiveness of the selective encryption approach. Selective encryption algorithms are very effective, thus have some weak points in their security. In this book, two successful security attacks against I-frame and DCT selective encryption algorithms are performed. Two algorithms are then proposed and evaluated accordingly. Our second topic is the coordination of multimedia security services. The conflict of data security algorithms and compression has introduced performance degradation and defective results. We invented an algorithm to completely eliminate compression from the fingerprinting loop to optimize performance. A second algorithm was invented for entertainment-level fast/effective encryption, particularly suitable for mobile devices, without noticeable compression overhead. The third topic is about how to detect and distinguish malicious attacks from allowable modifications in authentication. Using the hypothesis of decision border surface, an ideal solution of content authentication is proposed using a combination of generic authentications with classification techniques.

Proceedings of CSI 2015

Emerging Security Algorithms and Techniques

Algorithms for Data and Computation Privacy

Adaptive Cryptographic Access Control
Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering
Cyber Security and Digital Forensics