Implementasi Algoritma Kriptografi Rijndael Untuk

The Definitive Guide to HTML5 WebSocketCollaborative Learning TechniquesReport on the Development of the Advanced Encryption Standard (AES)Developing Software with UMLSoftware EngineeringKOLEKSI PROJEK C#.NETCircle of PreyUML 2 For DummiesA Brief History of Cryptology and Cryptographic AlgorithmsThe Twofish Encryption AlgorithmIntroduction to CryptographyAn Introduction to CryptographyMultimodal Signal ProcessingExpress.js GuideAn Introduction to Human-Computer Interaction (Psychology Revivals)Real 802.11 SecuritySoftware Modeling and DesignWireless Security HandbookDiscrete Mathematics and Its ApplicationsAdvanced CISSP Prep GuidePengantar Ilmu Kriptografi: Teori Analisis & ImplementasiKumpulan Program Penyandian Data dengan VB .NETThe American Black ChamberImage EncryptionFundamentals of Artificial Neural NetworksUML 2 and the Unified ProcessCryptography For DummiesHandbook of Applied CryptographyIntroduction to Modern CryptographyCryptography and Secure CommunicationsHigh-Tech CeramicsTWO BOOKS IN ONE: Koleksi Projek C# dan VBCryptanalysis of Number Theoretic CiphersMySQL/PHP Database ApplicationsPublic Key CryptographyComputer Networking EssentialsJava 1.1Lean Implementation in Hospital DepartmentsPGP: Pretty Good PrivacySoftware Engineering (Sie) 7E

The Definitive Guide to HTML5 WebSocket

Visual Basic merupakan bahasa pemrograman yang telah luas digunakan sejak lahirnya pada tahun 1991. Visual Basic (2012, 2013, dan versi seterusnya) menawarkan beberapa pembaharuan unik. Para programer Visual Basic sangat antusias mengadopsi fitur-fitur tangguh dari bahasa ini. Pembelajar dapat membuktikan bahwa Visual Basic merupakan perangkat ideal untuk memahami perkembangan pemrograman komputer. Buku teori tentang kriptografi sudah banyak beredar. Tetapi, sangat sedikit yang menunjukkan bagaimana setiap kriptosistem digunakan dan diimplementasikan dengan bahasa pemrograman tertentu. Buku ini, di sisi lain, tidak memberikan teori, karena teori kriptografi dapat Anda dapatkan dari banyak buku lain. Buku ini menyajikan kepada Anda bagaimana mengimplamentasikan sejumlah kriptosistem, fungsi hash, dan sidik digital berbasis Visual Basic dengan memanfaatkan pustaka .NET. Tujuan utama dari buku ini adalah memberikan kesempatan bagi para pembelajar untuk memperbaiki keterampilan pemrograman Visual Basic dalam mengimplementasikan sejumlah kasus kriptografi. Dengan penyelesaian berbagai kasus tersebut, buku ini mendorong para pembelajar untuk mengeksplorasi terapan Visual Basic sebagai perangkat pembantu dalam menyelesaikan topik-topik kriptografi yang lebih rumit. Berikut merupakan kasus-kasus yang disajikan pada buku ini. Kriptosistem Simetris: Algoritma RC4, Algoritma AES, Algoritma TripleDES, Algoritma IDEA, Algoritma Rijndael, Algoritma Rijndael Versi 2, Algoritma RC2, Algoritma DES, Algoritma DES Versi 2. Fungsi Hash dan Otentikasi Pesan: Fungsi Hash MD5, Fungsi Hash SHA1, RIPEMD160, Fungsi Hash SHA256, Fungsi Hash SHA512, Fungsi Hash SHA384, Sejumlah Otentikasi HMAC, Tanda-Tangan dan Verifikasi dengan MD5, Tanda-Tangan dan Verifikasi dengan SHA1, Tanda-Tangan dan Verifikasi dengan SHA256, Tanda-Tangan dan Verifikasi dengan SHA384, Tanda-Tangan dan Verifikasi dengan SHA512. Kriptosistem Asimetris dan Sidik Digital: Kriptosistem RSA, Sidik Digital dengan RSA, Membangkitkan Kunci Berbasis Password dengan PKCS5, Sidik Digital dengan DSA. Bonus: Pemrosesan Citra Digital: Manipulasi Citra, Konversi Citra, Penapisan Citra, Penapisan Citra Lanjut.

Collaborative Learning Techniques

The Wireless Security Handbook provides a well-rounded overview of wireless network security. It examines wireless from multiple perspectives, including those of an auditor, security architect, and hacker. This wide scope benefits anyone who has to administer, secure, hack, or conduct business on a wireless network. This text tackles wirele

Report on the Development of the Advanced Encryption Standard (AES)

Multimodal signal processing is an important research and development field that processes signals and combines information from a variety of modalities – speech, vision, language, text – which significantly enhance the understanding, modelling, and performance of human-computer interaction devices or systems enhancing human-human communication. The overarching theme of this book is the application of signal processing and statistical machine learning techniques to problems arising in this multi-disciplinary field. It describes the capabilities and limitations of current technologies, and discusses the technical challenges that must be overcome to develop efficient and user-friendly multimodal interactive systems. With contributions from the leading experts in the field, the present book should serve as a reference in multimodal signal processing for signal processing researchers, graduate students, R&D engineers, and computer engineers who are interested in this emerging field. Presents state-of-art methods for multimodal signal processing, analysis, and modeling Contains numerous examples of systems with different modalities combined Describes advanced applications in multimodal Human-Computer Interaction (HCI) as well as in computer-based analysis and modelling of multimodal human-human communication scenes.

Developing Software with UML

"Computer Networking Essentials" starts with an introduction to networking concepts. Readers learn computer networking terminology and history, and then dive into the technical concepts involved in sharing data across a computer network.

Software Engineering

PGP is a freely available encryption program that protects the privacy of files and electronic mail. It uses powerful public key cryptography and works on virtually every platform. This book is both a readable technical user's guide and a fascinating behind-the-scenes look at cryptography and privacy. It describes how to use PGP and provides background on cryptography, PGP's history, battles over public key cryptography patents and U.S. government export restrictions, and public debates about privacy and free speech.

KOLEKSI PROJEK C#.NET

Cryptography, in particular public-key cryptography, has emerged in the last 20 years as an important discipline that is not only the subject of an enormous amount of research, but provides the foundation for information security in many applications. Standards are emerging to meet the demands for cryptographic protection in most areas of data communications. Public-key cryptographic techniques are now in widespread use, especially in the financial services industry, in the public sector, and by individuals for their personal privacy, such as in electronic mail. This Handbook will serve as a valuable reference for the novice as well as for the expert who needs a wider scope of coverage within the area of cryptography. It is a necessary and timely guide for professionals who practice the art of cryptography. The Handbook of Applied Cryptography provides a treatment that is multifunctional: It serves as an introduction to the more practical aspects of both conventional and public-key cryptography It is a valuable source of the latest techniques and algorithms for the serious practitioner It provides an integrated treatment of the field, while still presenting each major topic as a self-contained unit It provides a mathematical treatment to accompany practical discussions It contains enough abstraction to be a valuable reference for theoreticians while containing enough detail to actually allow implementation of the algorithms discussed Now in its third printing, this is the definitive cryptography reference that the novice as well as experienced developers, designers, researchers, engineers, computer scientists, and mathematicians alike will use.

Circle of Prey

Cryptography plays a key role in ensuring the privacy and integrity of data and the security of computer networks. Introduction to Modern Cryptography provides a rigorous yet accessible treatment of modern cryptography, with a focus on formal definitions, precise assumptions, and rigorous proofs. The authors introduce the core principles of modern cryptography, including the modern, computational approach to security that overcomes the limitations of perfect secrecy. An extensive treatment of private-key encryption and message authentication follows. The authors also illustrate design principles for block ciphers, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), and present provably secure constructions of block ciphers from lower-level primitives. The second half of the book focuses on public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, El Gamal, and other cryptosystems. After exploring public-key encryption and digital signatures, the book concludes with a discussion of the random oracle model and its applications. Serving as a textbook, a reference, or for self-study, Introduction to Modern Cryptography presents the necessary tools to fully understand this fascinating subject.

UML 2 For Dummies

Ambition - Wealth - Greed - Power Truths turning to lies, father against son, friends becoming enemies, predator turning into prey and the circle continues. In her fifth novel, Marlene Mitchell calls upon her cynical side to create a suspenseful novel involving the world of big business and insurmountable wealth. Like quicksand, the corruption of money sucks even the innocent into its depths. Pitting man against the largest and one of the smartest animals on the planet makes for an interesting turn of events as you follow the journey of Jakuta, a bull elephant who is the ultimate prey.

A Brief History of Cryptology and Cryptographic Algorithms

The science of cryptology is made up of two halves. Cryptography is the study of how to create secure systems for communications. Cryptanalysis is the study of how to break those systems. The conflict between these two halves of cryptology is the story of secret writing. For over 2,000 years, the desire to communicate securely and secretly has resulted in the creation of numerous and increasingly complicated systems to protect one's messages. Yet for every system there is a cryptanalyst creating a new technique to break that system. With the advent of computers the cryptographer seems to finally have the upper hand. New mathematically based cryptographic algorithms that use computers for encryption and decryption are so secure that brute-force techniques seem to be the only way to break them – so far. This work traces the history of the conflict between cryptographer and cryptanalyst, explores in some depth the algorithms created to protect messages, and suggests where the field is going in the future.

The Twofish Encryption Algorithm

During the 1920s Herbert O. Yardley was chief of the first peacetime cryptanalytic organization in the United States, the ancestor of today's National Security Agency. Funded by the U.S. Army and the Department of State and working out of New York, his small and highly secret unit succeeded in breaking the diplomatic codes of several nations, including Japan. The decrypts played a critical role in U.S. diplomacy. Despite its extraordinary successes, the Black Chamber, as it came to known, was disbanded in 1929. President Hoover's new Secretary of State Henry L. Stimson refused to continue its funding with the now-famous comment, "Gentlemen do not read other people's mail." In 1931 a disappointed Yardley caused a sensation when he published this book and revealed to the world exactly what his agency had done with the secret and illegal cooperation of nearly the entire American cable industry. These revelations and Yardley's right to publish them set into motion a conflict that continues to this day: the right to freedom of expression versus national security. In addition to offering an expose on post-World War I cryptology, the book is filled with exciting stories and personalities.

Introduction to Cryptography

An Introduction to Cryptography

High-tech ceramics pose many challenges to the scientist and engineer because of their demanding production and processing requirements. Leading experts in the field address these problems not only from a fundamental scientific point of view but with particular reference to a broad range of engineering applications. This edited volume is based on invited talks given at a symposium held at the ETH Zurich in November, 1988, sponsored by the International Latsis Foundation of Geneva.

Multimodal Signal Processing

Originally published in 1989 this title provided a comprehensive and authoritative introduction to the burgeoning discipline of human-computer interaction for students, academics, and those from industry who wished to know more about the subject. Assuming very little knowledge, the book provides an overview of the diverse research areas that were at the time only gradually building into a coherent and well-structured field. It aims to explain the underlying causes of the cognitive, social and organizational problems typically encountered when computer systems are introduced. It is clear and concise, whilst avoiding the oversimplification of important issues and ideas.

Express.js Guide

An Introduction to Human-Computer Interaction (Psychology Revivals)

Buku teori tentang kriptografi, watermarking, steganografi, dan pengkodean data sudah banyak beredar. Tetapi, sangat sedikit yang menunjukkan bagaimana setiap teori tersebut digunakan dan diimplementasikan dengan bahasa pemrograman tertentu. Buku ini, di sisi lain, tidak memberikan teori, karena teori-teori tersebut dapat Anda peroleh dari banyak buku lain. Buku ini menyajikan kepada Anda bagaimana mengimplamentasikan sejumlah algoritma kriptografi, watermarking, steganografi, dan pengkodean data berbasis Visual C# dengan memanfaatkan pustaka .NET. Visual C# merupakan bahasa pemrograman yang telah luas digunakan sejak lahirnya pada tahun 1991. Visual C# (2012 dan 2013) menawarkan beberapa pembaharuan unik. Para programer Visual C# sangat antusias mengadopsi fitur-fitur tangguh dari bahasa ini. Pembelajar dapat membuktikan bahwa Visual C# merupakan perangkat ideal untuk memahami perkembangan pemrograman komputer. Tujuan utama dari buku ini adalah memberikan kesempatan bagi para pembelajar untuk memperbaiki keterampilan pemrograman Visual C# dalam mengimplementasikan sejumlah kasus kriptografi, watermarking, steganografi, dan pengkodean data. Dengan penyelesaian berbagai kasus tersebut, buku ini mendorong para pembelajar untuk mengeksplorasi terapan Visual C# sebagai perangkat pembantu dalam menyelesaikan topik-topik yang lebih rumit. Berikut merupakan kasus-kasus yang disajikan pada buku ini. Kriptosistem Simetris dan Integritas Data: Kriptosistem RC4, Kriptosistem DES, Kriptosistem TripeDES, Kriptosistem Rijndael, Kriptosistem Rijndael Untuk Enkripsi File, Kriptosistem RC2/DES/Rijndael, Kriptosistem RC2/DES/Rijndael dengan Password, Kriptosistem TEA, Kriptosistem XOR, Kriptosistem BlowFish/TwoFish, Hash MD5 dan SHA1, Mesin Enigma. Kriptosistem Asimetris: Kriptosistem RSA, Kriptosistem RSA dengan Editor, Kriptosistem RSA untuk Citra Digital, Kriptosistem Fraktal, Kriptosistem Otomata Seluler, Kriptosistem Visual. Watermarking dan Steganografi: Watermarking Teks pada Citra, Watermarking Teks pada Citra: Kasus 2, Watermarking dan MDI, Steganografi pada Citra, Staganografi Teks pada Suara. Pengkodean data: Pohon Biner, Pohon Fraktal, Enkoder Basis 64, Kode Batang UPCA, Kode Batang EAN13, Kode Batang POSTNET. Algoritma: Algoritma Graham Scan, Algoritma A* untuk Mencari Jalur Terpendek, Algoritma Pengklasteran K-Means, Algoritma Levenshtein, Algoritma JST Hopfield, Algoritma JST Back-Propagation, Algoritma Kalman, Algoritma Fuzzy untuk Pengendali Crane, Kontrol PID. Grafika 2D & 3D: Grafik Fungsi, Interpolasi Newton, Interpolasi Polinomial, Interpolasi Spline, Filter Sederhana untuk Citra Digital, Filter Lanjut untuk Citra Digital.

Real 802.11 Security

This book describes new approaches to wireless security enabled by the recent development of new core technologies for Wi-Fi/802.11. It shows how the new approaches work and how they should be applied for maximum effect. For system administrators, product designers, or advanced home users.

Software Modeling and Design

Cryptography is the most effective way to achieve data securityand is essential to e-commerce activities such as online shopping,stock trading, and banking This invaluable introduction to the basics of encryption coverseverything from the terminology used in the field to specifictechnologies to the pros and cons of different implementations Discusses specific technologies that incorporate cryptographyin their design, such as authentication methods, wirelessencryption, e-commerce, and smart cards Based entirely on real-world issues and situations, thematerial provides instructions for already available technologiesthat readers can put to work immediately Expert author Chey Cobb is retired from the NRO, where she helda Top Secret security clearance, instructed employees of the CIAand NSA on computer security and helped develop the computersecurity policies used by all U.S. intelligence agencies

Wireless Security Handbook

The first and only guide to one of today's most important new cryptography algorithms The Twofish Encryption Algorithm A symmetric block cipher that accepts keys of any length, up to 256 bits, Twofish is among the new encryption algorithms being considered by the National Institute of Science and Technology (NIST) as a replacement for the DES algorithm. Highly secure and flexible, Twofish works extremely well with large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. Now from the team who developed Twofish, this book provides you with your first detailed look at: * All aspects of Twofish's design and anatomy * Twofish performance and testing results * Step-by-step instructions on how to use it in your systems * Complete source code, in C, for implementing Twofish On the companion Web site you'll find: * A direct link to Counterpane Systems for updates on Twofish * A link to the National Institute of Science and Technology (NIST) for ongoing information about the competing technologies being considered for the Advanced Encryption Standard (AES) for the next millennium For updates on Twofish and the AES process, visit these sites: * www.wiley.com/compbooks/schneier * www.counterpane.com * www.nist.gov/aes Wiley Computer Publishing Timely.Practical.Reliable Visit our Web site at www.wiley.com/compbooks/ Visit the companion Web site at www.wiley.com/compbooks/schneier

Discrete Mathematics and Its Applications

The Comprehensive Book on Express.js The in-depth, detailed, hand-on manual on Express.js, the most popular Node.js framework. Will get you up and running fast and save you time. Understand the concepts, learn the best practices. Become an Express.js expert today. Express.js API reference, quick start guides, 20+ meticulously explained examples and tutorials -- over 270 pages with more than 60 illustrations. Quick Start The Interface TIps and Tricks Tutorials and Examples Why Express.js is the most popular Node.js web framework yet. As of this writing (September of 2013), there are no books that are solely dedicated to it. Its official website has bits of insights for advanced Node.js programmers. However, I found that many people -- including those who go through HackReactor7 program and come to my Node.js classes at General Assembly and pariSOMA -- are interested in a comprehensive resource. The one that would cover all the different components of Express.js work together in a real production-like application. The goal of Express.js Guide is to become such resource. What This Book is Express.js Guide is a concise book on one particular library. This book contains Express.js API 3.3.58 description, the best practices on code organization and patterns, real-world examples of web apps. The topics include but not limited to middleware, command-line interface and scaffolding, ren- dering templates, extracting params from dynamic URLs, parsing payloads and cookies, managing authentication with sessions, error handling and prepping apps for production. For more details and for what exactly the book covers, please refer to the Table of Contents. What This Book is Not This book is not an introduction to Node.js, nor is it a book that covers all aspects of building a modern day web application, e.g., websockets, databases and (of course) front-end development. Keep in mind that readers also won't find in Express.js Guide a resource for learning programming and/or JavaScript fundamentals. You might want to take a look at Rapid Prototyping with JS9 for the introduction to Node.js, MongoDB and front-end development with Backbone.js. In the real-world and especially in Node.js development, due to its modularized philosophy, we seldom use just a single framework. In the book, we have tried to stick only to Express.js and leave everything else out as much as possible, without compromising the usefulness of examples. Therefore, we intentionally left out some important chunks of web developments, for example databases, authentication and testing. Although these elements are present in tutorials and examples, they're not explained in detail. For those materials, you could check books in the Related Reading and Resources section at the end of the book. Who This Book is For This book is for people fluent in programming and front-end JavaScript. In addition, to get the most benefits, readers must be familiar with basic Node.js concepts like process and global, and know core modules, including streams, clusters and buffer type. If you're thinking of starting a Node.js app, or of rewriting an existing one, and your weapon of choice is Express.js -- this guide is for you! It will answer most of your "how" and "why" questions.

Advanced CISSP Prep Guide

Practical guide to exploiting the power of Object Technology & UML in your software development process.

Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi

More businesses and ambitious individuals are trying to bring applications to the Web but they are bewildered with the array of components and concepts needed to create a data-driven site. The cost, stability and ease of development using the Open Source PHP 4 scripting language and a MySQL database makes this combination the best choice for small and mid-size Web-based applications. PHP4/MySQL Database Applications demonstrates web-application development by presenting seven real, ready-to-use examples starting with a simple guess book and ending with a fully-functional e-commerce site with a shopping cart. Inexperienced users will learn the essentials of working with PHP4 and MySQL so they can start building and customizing database applications for the web right away!

Kumpulan Program Penyandian Data dengan VB .NET

This book covers all you need to know to model and design software applications from use cases to software architectures in UML and shows how to apply the COMET UML-based modeling and design method to real-world problems. The author describes architectural patterns for various architectures, such as broker, discovery, and transaction patterns for service-oriented architectures, and addresses software quality attributes including maintainability, modifiability, testability, traceability, scalability, reusability, performance, availability, and security. Complete case studies illustrate design issues for different software architectures: a banking system for client/server architecture, an online shopping system for service-oriented architecture, an emergency monitoring system for component-based software architecture, and an automated guided vehicle for real-time software architecture. Organized as an introduction followed by several short, self-contained chapters, the book is perfect for senior undergraduate or graduate courses in software engineering and design, and for experienced software engineers wanting a quick reference at each stage of the analysis, design, and development of large-scale software systems.

The American Black Chamber

Presenting encryption algorithms with diverse characteristics, Image Encryption: A Communication Perspective examines image encryption algorithms for the purpose of secure wireless communication. It considers two directions for image encryption:

permutation-based approaches and substitution-based approaches. Covering the spectrum of image encryption principles and techniques, the book compares image encryption with permutation- and diffusion-based approaches. It explores number theory-based encryption algorithms such as the Data Encryption Standard, the Advanced Encryption Standard, and the RC6 algorithms. It not only details the strength of various encryption algorithms, but also describes their ability to work within the limitations of wireless communication systems. Since some ciphers were not designed for image encryption, the book explains how to modify these ciphers to work for image encryption. It also provides instruction on how to search for other approaches suitable for this task. To make this work comprehensive, the authors explore communication concepts concentrating on the orthogonal frequency division multiplexing (OFDM) system and present a simplified model for the OFDM communication system with its different implementations. Complete with simulation experiments and MATLAB® codes for most of the simulation experiments, this book will help you gain the understanding required to select the encryption method that best fulfills your application requirements.

Image Encryption

"This book manages to convey the practical use of UML 2 in clear and understandable terms with many examples and guidelines. Even for people not working with the Unified Process, the book is still of great use. UML 2 and the

Unified Process, Second Edition is a must-read for every UML 2 beginner and a helpful guide and reference for the experienced practitioner." --Roland Leibundgut, Technical Director, Zuehlke Engineering Ltd. "This book is a good starting point for organizations and individuals who are adopting UP and need to understand how to provide visualization of the different aspects needed to satisfy it. " --Eric Naiburg, Market Manager, Desktop Products, IBM Rational Software This thoroughly revised edition provides an indispensable and practical guide to the complex process of object-oriented analysis and design using UML 2. It describes how the process of OO analysis and design fits into the software development lifecycle as defined by the Unified Process (UP). UML 2 and the Unified Process contains a wealth of practical, powerful, and useful techniques that you can apply immediately. As you progress through the text, you will learn OO analysis and design techniques, UML syntax and semantics, and the relevant aspects of the UP. The book provides you with an accurate and succinct summary of both UML and UP from the point of view of the OO analyst and designer. This book provides Chapter roadmaps, detailed diagrams, and margin notes allowing you to focus on your needs Outline summaries for each chapter, making it ideal for revision, and a comprehensive index that can be used as a reference New to this edition: Completely revised and updated for UML 2 syntax Easy to understand explanations of the new UML 2 semantics More real-world examples A new section on the Object Constraint Language (OCL) Introductory material on the OMG's Model Driven Architecture (MDA) The accompanying website provides A complete example of a simple e-commerce system Open source tools for requirements engineering and use case modeling Industrial-strength UML course materials based on the book

Fundamentals of Artificial Neural Networks

UML 2 and the Unified Process

BUKU 1: KOLEKSI PROJEK C#.NET Buku teori tentang kriptografi, watermarking, steganografi, dan pengkodean data sudah banyak beredar. Tetapi, sangat sedikit yang menunjukkan bagaimana setiap teori tersebut digunakan dan diimplementasikan dengan bahasa pemrograman tertentu. Buku ini, di sisi lain, tidak memberikan teori, karena teori-teori tersebut dapat Anda peroleh dari banyak buku lain. Buku ini menyajikan kepada Anda bagaimana mengimplamentasikan sejumlah algoritma kriptografi, watermarking, steganografi, dan pengkodean data berbasis Visual C# dengan memanfaatkan pustaka .NET. Visual C# merupakan bahasa pemrograman yang telah luas digunakan sejak lahirnya pada tahun 1991. Visual C# (2012 dan 2013) menawarkan beberapa pembaharuan unik. Para programer Visual C# sangat antusias mengadopsi fitur-fitur tangguh dari bahasa ini. Pembelajar dapat membuktikan bahwa Visual C# merupakan perangkat ideal untuk memahami perkembangan pemrograman komputer. Tujuan utama dari buku ini adalah memberikan kesempatan bagi para pembelajar untuk memperbaiki keterampilan pemrograman Visual C# dalam mengimplementasikan sejumlah kasus kriptografi, watermarking, steganografi, dan pengkodean data. Dengan penyelesaian berbagai kasus tersebut, buku ini mendorong para pembelajar untuk mengeksplorasi terapan Visual C# sebagai perangkat pembantu dalam menyelesaikan topik-topik yang lebih rumit. Berikut merupakan kasus-kasus yang disajikan pada buku ini. Kriptosistem Simetris dan Integritas Data: Kriptosistem RC4, Kriptosistem DES, Kriptosistem TripeDES, Kriptosistem Rijndael, Kriptosistem Rijndael Untuk Enkripsi File, Kriptosistem RC2/DES/Rijndael, Kriptosistem RC2/DES/Rijndael dengan Password, Kriptosistem TEA, Kriptosistem XOR, Kriptosistem BlowFish/TwoFish, Hash MD5 dan SHA1, Mesin Enigma. Kriptosistem Asimetris: Kriptosistem RSA, Kriptosistem RSA dengan Editor, Kriptosistem RSA untuk Citra Digital, Kriptosistem Fraktal, Kriptosistem Otomata Seluler, Kriptosistem Visual. Watermarking dan Steganografi: Watermarking Teks pada Citra, Watermarking Teks pada Citra: Kasus 2, Watermarking dan MDI, Steganografi pada Citra, Staganografi Teks pada Suara. Pengkodean data: Pohon Biner, Pohon Fraktal, Enkoder Basis 64, Kode Batang UPCA, Kode Batang EAN13, Kode Batang POSTNET. Algoritma: Algoritma Graham Scan, Algoritma A* untuk Mencari Jalur Terpendek, Algoritma Pengklasteran K-Means, Algoritma Levenshtein, Algoritma JST Hopfield, Algoritma JST Back-Propagation, Algoritma Kalman, Algoritma Fuzzy untuk Pengendali Crane, Kontrol PID. Grafika 2D & 3D: Grafik Fungsi, Interpolasi Newton, Interpolasi Polinomial, Interpolasi Spline, Filter

Sederhana untuk Citra Digital, Filter Lanjut untuk Citra Digital. BUKU 2: KOLEKSI PROJEK VISUAL BASIC.NET DAN VISUAL C#.NET Visual Basic dan Visual C# merupakan bahasa pemrograman yang telah luas digunakan sejak lahirnya pada tahun 1991. Visual Basic dan Visual C# (2012 dan 2013) menawarkan beberapa pembaharuan unik. Para programer Visual Basic dan Visual C# sangat antusias mengadopsi fitur-fitur tangguh dari bahasa ini. Pembelajar pemula akan membuktikan bahwa keduanya merupakan perangkat ideal untuk memahami perkembangan pemrograman komputer. Buku ini membantu pembelajar agar secara utuh memahami logika, semantika, dan sintaksis dari pemrograman. Melalui kasus-kasus windows form, animasi, dan game, buku ini membantu mengatrol kompetensi pemrograman dari pembelajar awal yang sering mengalami kesulitan dalam memahami konsep dan paradigma dasar dari bahasa pemrograman level-tinggi. Buku ini dimaksudkan sebagai buku mandiri, yang memuat sejumlah projek-projek program Visual Basic dan Visual C#. Tujuan utama dari buku ini adalah memberikan kesempatan bagi para pembelajar untuk memperbaiki keterampilan pemrograman Visual Basic dan Visual C# dalam mengimplementasikan sejumlah kasus (khususnya animasi dan game) Dengan penyelesaian berbagai kasus tersebut, buku ini mendorong para pembelajar untuk mengeksplorasi terapan Visual Basic dan Visual C# sebagai perangkat pembantu dalam menyelesaikan topik-topik yang lebih rumit. Beberapa sasaran ketika buku teks ini ditulis adalah: 1. Mengembangkan bab-bab secara terfokus. Daripada merangkum banyak bab dengan kedalaman permukaan saja, buku ini hanya difokuskan pada subjek-subjek bahasan konsentrasi (windows form, animasi, dan game). 2. Menggunakan windows form, animasi, dan game. Meskipun data uji pada program tidak merepresentasikan data riil, tetapi kekayaan kasus pada buku ini mengilustrasikan banyak teknik pemrograman yang sangat dibutuhkan para pembejalar. 3. Menjadikan buku bagi pembelajar mandiri. Pada tiap fokus bahasan, buku ini tidak bertele-tele, langsung ke sasaran dengan penyajian kasus-kasus. Buku ini bisa dipakai sebagai panduan cepat bagi para insinyur atau programer. Berikut merupakan kasus-kasus yang disajikan pada buku ini. Kompilasi Projek Visual Basic Tingkat Dasar: Kalkulator Sederhana, Kalkulator Saintifik Sederhana, Kalkulator Saintifik, Aplikasi Catatan Sederhana, TextPad, Captcha, Validasi Form, Sistem Aplikasi Parkir Sederhana, Aplikasi Pembayaran Restoran dan Kafe, Sistem Informasi Mahasiswa, Brain Game, Game Menangkap Bola, Stopwatch, Game Tic Tac Toe, Penghitung Huruf Vokal dan Huruf Konsonan, Drag and Drop, Penggambar Grafik, Penghitung Mundur, Penggulung Teks, Event Hover, Pemindahan Konten ListBox, Metode-Metode List, Penghitung Kecepatan Pengetikan, Media Player, MP3 Player, Cash Register Restoran, WordPad, Game Hangman, Game Ular, Game Pacman. Kompilasi Projek Visual Basic Tingkat Menengah: Kalkulator Lanjut, Daftar Warna, Digitizer, Game Mencocokkan Binatang, Konverter Biner, Game Mencocokkan Ikon, Menampilkan Kode Karakter, Konsol DJ, Game Total 15, Keyboard, Midi Keyboard, Perekam Suara, Game Tetris, Jam Progressbar, MP3 dan MP4 Player. Kompilasi Projek Visual Basic Tingkat Lanjut: Game Cheese, Carousel Citra, Kalender, Bangun 3D Sederhana, Merotasi Kubik 3D, Game Mengacak Angka, Sistem Administrasi Nilai, Administrasi PhoneBook Tanpa Database, Game Penyerang, Game Pendekar, File Downloader, ListView Watermark, Game Tetris Pro. Bonus: Kompilasi Game Dengan Visual C#: Game Hangman, Game Bata, Game Batu-Gunting-Kertas, Game Melatih Otak, Game Tic Tic Toe, Game Pemakan, Game Jigsaw, Game Tetris, Game Dot, Game Pesawat Tempur, Game Pemakan Versi 2.0.

Cryptography For Dummies

A systematic account of artificial neural network paradigms that identifies fundamental concepts and major methodologies. Important results are integrated into the text in order to explain a wide range of existing empirical observations and commonly used heuristics.

Handbook of Applied Cryptography

Two leading authors bring their reputations to this hands-on, authoritative reference work on Java. Completely updated and expanded, this second edition covers new technologies such as Java Beans, updated AWT Class information, Java Database Connectivity API, and RMI/CORBA integration.

Introduction to Modern Cryptography

Complete coverage of the current major public key cryptosystemstheir underlying mathematics and the most common techniques used inattacking them Public Key Cryptography: Applications andAttacks introduces and explains the fundamentals of public keycryptography and explores its application in all major public keycryptosystems in current use, including ElGamal, RSA, EllipticCurve, and digital signature schemes. It provides the underlyingmathematics needed to build and study these schemes as needed, andexamines attacks on said schemes via the mathematical problems onwhich they are based – such as the discrete logarithm problemand the difficulty of factoring integers. The book contains approximately ten examples with detailedsolutions, while each chapter includes forty to fifty problems withfull solutions for odd-numbered problems provided in the Appendix.Public Key Cryptography: • Explains fundamentals of public key cryptography • Offers numerous examples and exercises • Provides excellent study tools for those preparing totake the Certified Information Systems Security Professional(CISSP) exam • Provides solutions to the end-of-chapter problems Public Key Cryptography provides a solid background foranyone who is employed by or seeking employment with a governmentorganization, cloud service provider, or any large enterprise thatuses public key systems to secure data.

Cryptography and Secure Communications

Lean healthcare is waste elimination in every service area with the goal of reducing inventory, cycle time of service, and cost, so that high-quality patient care can be provided in a way that is as efficient, as effective, and as responsive as possible while retaining the financial integrity of a hospital. The Lean philosophy in healthcare demands a person's attitude, in all aspects of care, understand the process which happens, observe it, and gather information in order to identify the root of an inefficiency of the process. In short, Lean and its emphasis on efficiency can be a critical tool in the management of health services in hospitals around the world. This book provides guidance and examples on how Lean principles can be implemented into the infrastructure and every day operations of a hospital from the emergency room to hospital facilities and maintenance. The book also demonstrates how Lean is the cultural commitment of organizations to implement the scientific method in designing, conducting, and improving work sustainably through teamwork, bringing in better value and satisfaction to the patient. It shortens the time between ordering and service delivery by eliminating waste from the service flow value. The author uses numerous examples of Lean thinking in various hospital departments with the overall of goal of taking that department from good to great.

High-Tech Ceramics

Engaging students in active learning is a predominant theme in today's classrooms. To promote active learning, teachers across the disciplines and in all kinds of colleges are incorporating collaborative learning into their teaching. Collaborative Learning Techniques is a scholarly and well-written handbook that guides teachers through all aspects of group work, providing solid information on what to do, how to do it, and why it is important to student learning. Synthesizing the relevant research and good practice literature, the authors present detailed procedures for thirty collaborative learning techniques (CoLTs) and offer practical suggestions on a wide range of topics, including how to form groups, assign roles, build team spirit, solve problems, and evaluate and grade student participation.

TWO BOOKS IN ONE: Koleksi Projek C# dan VB

The Definitive Guide to HTML5 WebSocket is the ultimate insider’s WebSocket resource. This revolutionary new web technology enables you to harness the power of true real-time connectivity and build responsive, modern web applications. This book contains everything web developers and architects need to know about WebSocket. It discusses how WebSocket-based architectures provide a dramatic reduction in unnecessary network overhead and latency compared to older HTTP

(Ajax) architectures, how to layer widely used protocols such as XMPP and STOMP on top of WebSocket, and how to secure WebSocket connections and deploy WebSocket-based applications to the enterprise. Build real-time web applications with HTML5. This book: Introduces you to the WebSocket API and protocol Describes and provides real-world examples of protocol communication over WebSocket Explains WebSocket security and enterprise deployment

Cryptanalysis of Number Theoretic Ciphers

Uses friendly, easy-to-understand For Dummies style to helpreaders learn to model systems with the latest version of UML, themodeling language used by companies throughout the world to developblueprints for complex computer systems Guides programmers, architects, and business analysts throughapplying UML to design large, complex enterprise applications thatenable scalability, security, and robust execution Illustrates concepts with mini-cases from different businessdomains and provides practical advice and examples Covers critical topics for users of UML, including objectmodeling, case modeling, advanced dynamic and functional modeling,and component and deployment modeling

MySQL/PHP Database Applications

The opening section of this book covers key concepts of cryptography, from encryption and digital signatures to cryptographic protocols. Essential techniques are demonstrated in protocols for key exchange, user identification, electronic elections and digital cash. The second part addresses advanced topics, such as the bit security of one-way functions and computationally perfect pseudorandom bit generators. Examples of provably secure encryption and signature schemes and their security proofs are given. Though particular attention is given to the mathematical foundations, no special background in mathematics is presumed. The necessary algebra, number theory and probability theory are included in the appendix. Each chapter closes with a collection of exercises. The second edition presents new material, including a complete description of the AES, an extended section on cryptographic hash functions, a new section on random oracle proofs, and a new section on public-key encryption schemes that are provably secure against adaptively-chosen-ciphertext attacks.

Public Key Cryptography

In 1997, NIST initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclass.) Fed. info. In 1998, NIST announced the acceptance of 15 candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. This analysis included an initial exam. of the security and efficiency characteristics for each algorithm. NIST reviewed the results of this research and selected MARS, RC, Rijndael, Serpent and Twofish as finalists. After further public analysis of the finalists, NIST has decided to propose Rijndael as the AES. The research results and rationale for this selection are documented here.

Computer Networking Essentials

Continuing a bestselling tradition, An Introduction to Cryptography, Second Edition provides a solid foundation in cryptographic concepts that features all of the requisite background material on number theory and algorithmic complexity as well as a historical look at the field. With numerous additions and restructured material, this edition

Java 1.1

At the heart of modern cryptographic algorithms lies computational number theory. Whether you're encrypting or decrypting ciphers, a solid background in number theory is essential for success. Written by a number theorist and practicing cryptographer, Cryptanalysis of Number Theoretic Ciphers takes you from basic number theory to the inner workings of ciphers and protocols. First, the book provides the mathematical background needed in cryptography as well as definitions and simple examples from cryptography. It includes summaries of elementary number theory and group theory, as well as common methods of finding or constructing large random primes, factoring large integers, and computing discrete logarithms. Next, it describes a selection of cryptographic algorithms, most of which use number theory. Finally, the book presents methods of attack on the cryptographic algorithms and assesses their effectiveness. For each attack method the author lists the systems it applies to and tells how they may be broken with it. Computational number theorists are some of the most successful cryptanalysts against public key systems. Cryptanalysis of Number Theoretic Ciphers builds a solid foundation in number theory and shows you how to apply it not only when breaking ciphers, but also when designing ones that are difficult to break.

Lean Implementation in Hospital Departments

Get ready to pass the CISSP exam and earn your certification with this advanced test guide Used alone or as an in-depth supplement to the bestselling The CISSP Prep Guide, this book provides you with an even more intensive preparation for the CISSP exam. With the help of more than 300 advanced questions and detailed answers, you'll gain a better understanding of the key concepts associated with the ten domains of the common body of knowledge (CBK). Each question is designed to test you on the information you'll need to know in order to pass the exam. Along with explanations of the answers to these advanced questions, you'll find discussions on some common incorrect responses as well. In addition to serving as an excellent tutorial, this book presents you with the latest developments in information security. It includes new information on: Carnivore, Echelon, and the U.S. Patriot Act The Digital Millennium Copyright Act (DMCA) and recent rulings The European Union Electronic Signature Directive The Advanced Encryption Standard, biometrics, and the Software Capability Maturity Model Genetic algorithms and wireless security models New threats and countermeasures The CD-ROM includes all the questions and answers from the book with the Boson-powered test engine.

PGP: Pretty Good Privacy

This one-of-a-kind reference condenses into a single volume a wealth of practical information on the processes required to design computer software under today's primary architectures. Examples, exercises, and case studies give readers a solid grasp of all concepts and techniques described in the text.

Software Engineering (Sie) 7E

This book provides a practical introduction to cryptographic principles & algorithms for communication security & data privacy-both commercial & military-written by one of the world's leading authorities on encryption & coding. Covering the latest developments in cryptography for all data communication professionals who need an understanding of cryptographic technology, the book explains the Data Encryption Standard, stream ciphers, public-key cryptosystems, arithmetic operating circuits, important classes of BCH & Reed-Solomon codes for multiple-error correction, ciphertext protection against illegal deletion or injection of information, practical cryptographic applications, & more.

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN’S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION