Simulation Using Elliptic Cryptography Matlab

Methods Used to Solve Discrete Math ProblemsInteresting examples highlight the interdisciplinary nature of this areaPearls of Discrete Mathematics presents methods for solving counting problems and other types of problems that involve discrete structures. Through intriguing examples, problems, theorems, and proofs, the book illustrates the relation

Linear algebra forms the basis for much of modern mathematics—theoretical, applied, and computational. Finite-Dimensional Linear Algebra provides a solid foundation for the study of advanced mathematics and discusses applications of linear algebra to such diverse areas as combinatorics, differential equations, optimization, and approximation. The author begins with an overview of the essential themes of the book: linear equations, best approximation, and diagonalization. He then takes students through an axiomatic development of vector spaces, linear operators, eigenvalues, norms, and inner products. In addition to discussing the special properties of symmetric matrices, he covers the Jordan canonical form, an important theoretical tool, and the singular value decomposition, a powerful tool for computation. The final chapters present introductions to numerical linear algebra and analysis in vector spaces, including a brief introduction to functional analysis (infinite-dimensional linear algebra). Drawing on material from the author's own course, this textbook gives students a strong theoretical understanding of linear algebra. It offers many illustrations of how linear algebra is used throughout mathematics.

Simulation of ATM Using Elliptic Curve Cryptography in MatLabElliptic Curve CryptographyLAP Lambert Academic Publishing

Once the privilege of a select few, cryptography is now taught at universities around the world. Introduction to Cryptography with Open-Source Software illustrates algorithms and cryptosystems using examples and the open-source computer algebra system of Sage. The author, a noted educator in the field, provides a highly practical learning experience by progressing at a gentle pace, keeping mathematics at a manageable level, and including numerous end-of-chapter exercises. Focusing on the cryptosystems themselves rather than the means of breaking them, the book first explores when and how the methods of modern cryptography can be used and misused. It then presents number theory and the algorithms and methods that make up the basis of cryptography today. After a brief review of "classical" cryptography, the book introduces information theory and examines the public-key cryptosystems of RSA and Rabin's cryptosystem. Other public-key systems studied include the El Gamal cryptosystem, systems based on knapsack problems, and algorithms for creating digital signature schemes. The second half of the text moves on to consider bit-oriented secret-key, or symmetric, systems suitable for encrypting large amounts of data. The author describes block ciphers (including the Data Encryption Standard), cryptographic hash functions, finite fields, the Advanced Encryption Standard, cryptosystems based on elliptical curves, random number generation, and stream ciphers. The book concludes with a look at examples and applications of modern cryptographic systems, such as multi-party computation, zero-knowledge proofs, oblivious transfer, and voting protocols.

Concepts, Methodologies, Tools, and Applications

Smart Card Research and Advanced Applications

Security and Privacy in the Internet of Things

Pearls of Discrete Mathematics

Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy

Applications of Abstract Algebra with Maple and MATLAB, Second Edition

This book gathers the outcomes of the 7th International Conference on Applied Computing and Information Technology (ACIT 2019), which was held on May 29–31, 2019 in Honolulu, Hawaii. The aim of the conference was to bring together researchers and scientists, businesspeople and entrepreneurs, teachers, engineers, computer users, and students to discuss the various fields of computer science and to share their experiences and exchange new ideas and information in a meaningful way. Further, they presented research results on all aspects (theory, applications and tools) of computer and information science, and discussed the practical challenges encountered in their work and the solutions they adopted to overcome them. The book highlights the best papers from those accepted for presentation at the conference. They were chosen based on review scores submitted by members of the program committee and underwent further rigorous rounds of review. From this second round, 15 of the conference's most promising papers were selected for this Springer (SCI) book and not the conference proceedings. We eagerly await the important contributions that we know these authors will make to the field of computer and information science.

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.

Risk detection and cyber security play a vital role in the use and success of contemporary computing. By utilizing the latest technological advances, more effective prevention techniques can be developed to protect against cyber threats. Detecting and Mitigating Robotic Cyber Security Risks is an essential reference publication for the latest research on new methodologies and applications in the areas of robotic and digital security. Featuring extensive coverage on a broad range of topics, such as authentication techniques, cloud security, and mobile robotics, this book is ideally designed for students, researchers, scientists, and engineers seeking current research on methods, models, and implementations of optimized security in digital contexts.

Exploring one of the most dynamic areas of mathematics, Advanced Number Theory with Applications covers a wide range of algebraic, analytic, combinatorial, cryptographic, and geometric aspects of number theory. Written by a recognized leader in algebra and number theory, the book includes a page reference for every citing in the bibliography and mo

VISUAL BASIC .NET FOR STUDENTS

Advanced Number Theory with Applications

Select Proceedings of ICNETS2, Volume VI

Detecting and Mitigating Robotic Cyber Security Risks

Bulletin of the Institute of Mathematics and Its Applications

Applied Computing and Information Technology

Galois fields are essential blocks of building many of cryptographic schemes. The main advantage of applying Galois fields over cryptographic applications are to reduce cost and increase the sufficiency of the performance. In past, they were interested in implement Galois field of characteristic 2 in most of the crypto-system application, but in the meantime, the researcher started to work on Galois field of odd characteristics which it has applications in many areas like Elliptic Curve Cryptography, Identity-based Encryption, Short Signature Schemes and etc.In this thesis, an odd characteristic Galois field was implemented. In particular, thisthesis focuses on implementation of multiplication and reduction on GF(3m). Overviewabout the thesis idea was presented in the beginning. Finite field arithmetic was discussed where it shows some of the Galois fields important definitions and properties. In addition, irreducible polynomials over GF(p) where p is prime and the basic additional and multiplication over GF(pm) was discussed as well. Introduction to the proposed implementation started with the arithmetic of the Galois field characteristics 3. The problem formulation introduced by its mathematical representation and the Progressive Product Reduction (PPR) technique which is the technique used in this thesis. Implement three different semi-systolic arrays architecture with different projection functions. This stage followed by modeling assumption for complexity analysis for both area and delay where it used to compare proposed designs with other published designs. Proposed design gets verified by Matlab code implementation at the end of this thesis.

Handbook of Mathematical Induction: Theory and Applications shows how to find and write proofs via mathematical induction. This comprehensive book covers the theory, the structure of the written proof, all standard exercises, and hundreds of application examples from nearly every area of mathematics.In the first part of the book, the author discuss

This book mainly reflects the recent research works in evolutionary computation technologies and mobile sustainable networks with a specific focus on computational intelligence and communication technologies that widely ranges from theoretical foundations to practical applications in enhancing the sustainability of mobile networks. Today, network sustainability has become a significant research domain in both academia and industries present across the globe. Also, the network sustainability paradigm has generated a solution for existing optimization challenges in mobile communication networks. Recently, the research advances in evolutionary computing technologies including swarm intelligence algorithms and other evolutionary algorithm paradigms are considered as the widely accepted descriptors for mobile sustainable networks virtualization, optimization, and automation. To deal with the emerging impacts on mobile communication networks, this book discusses about the state-of-the research works on developing a sustainable design and their implementation in mobile networks. With the advent of evolutionary computation algorithms, this book contributes varied research chapters to develop a new perspective on mobile sustainable networks.

This book gathers selected research papers presented at the First International Conference on Digital Technologies and Applications (ICDTA 21), held at Sidi Mohamed Ben Abdellah University, Fez, Morocco, on 29–30 January 2021. highlighting the latest innovations in digital technologies as: artificial intelligence, Internet of things, embedded systems, network technology, information processing, and their applications in several areas such as hybrid vehicles, renewable energy, robotic, and COVID-19. The respective papers encourage and inspire researchers, industry professionals, and policymakers to put these methods into practice.

Computer Applications for Security, Control and System Engineering

Digital Technologies and Applications

Proceedings of ICECMSN 2021

Proceedings of the First International Conference, MMCITRE 2020

Progressive Product Reduction for Polynomial Basis Multiplication Over GF(3m)

EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing

This book constitutes the refereed proceedings of the International Conferences on Security Technology, SecTech 2012, on Control and Automation, CA 2012, and CES-CUBE 2012, the International Conference on Circuits, Control, Communication, Electricity, Electronics, Energy, System, Signal and Simulation: all held in conjunction with GST 2012 on Jeju Island, Korea, in November/December 2012. The papers presented were carefully reviewed and selected from numerous submissions and focus on the various aspects of security technology, and control and automation, and circuits, control, communication, electricity, electronics, energy, system, signal and simulation.

This book constitutes the refereed proceedings of the 4th International Workshop on Systems, Architectures, Modeling, and Simulation, SAMOS 2004, held in Samos, Greece on July 2004. Besides the SAMOS 2004 proceedings, the book also presents 19 revised papers from the predecessor workshop SAMOS 2003. The 55 revised full paper presented were carefully reviewed and selected for inclusion in the book. The papers are organized in topical sections on reconfigurable computing, architectures and implementation, and systems modeling and simulation.

This book is a tutorial on digital techniques for waveform generation, digital filters, and digital signal processing tools and techniques The typical chapter begins with some theoretical material followed by working examples and experiments using the TMS320C6713-based DSPStarter Kit (DSK) The C6713 DSK is TI's newest signal processor based on the C6x processor (replacing the C6711 DSK)

This volume constitutes the refereed proceedings of the 7th International Conference on Smart Card Research and Advanced Applications, CARDIS 2006, held in Tarragona, Spain, in April 2006. The 25 revised full papers presented were carefully reviewed and updated for inclusion in this book. The papers are organized in topical sections on smart card applications, side channel attacks, smart card networking, cryptographic protocols, RFID security, and formal methods.

Theory and Applications

Handbook of Product Graphs

Computer Systems: Architectures, Modeling, and Simulation

Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2016

Introduction to Cryptography with Mathematical Foundations and Computer Implementations

Distributed Sensing and Intelligent Systems

This book presents new knowledge and recent developments in all aspects of computational techniques, mathematical modeling, energy systems, applications of fuzzy sets and intelligent computing. The book is a collection of best selected research papers presented at the International Conference on "Mathematical Modeling, Computational Intelligence Techniques a Mathematics, Pandit Deendayal Petroleum University, in association with Forum for Interdisciplinary Mathematics, Institution of Engineers (IEI) – Gujarat and Computer Society of India (CSI) – Ahmedabad. The book provides innovative works of researchers, academicians and students in the area of interdisciplinary mathematics, statistics, computational intelligence a

This handbook examines the dichotomy between the structure of products and their subgraphs. It also features the design of efficient algorithms that recognize products and their subgraphs and explores the relationship between graph parameters of the product and factors. Extensively revised and expanded, this second edition presents full proofs of many import illustrates applications of graph products in several areas and contains well over 300 exercises. Supplementary material is available on the book's website.

This book is a collection of papers from international experts presented at International Conference on NextGen Electronic Technologies (ICNETS2-2016). ICNETS2 encompassed six symposia covering all aspects of electronics and communications domains, including relevant nano/micro materials and devices. Presenting recent research on wireless communication net to researchers, professionals and students working in the core areas of electronics and their applications, especially in signal processing, embedded systems and networking.

Accessible to undergraduate students, Introduction to Combinatorics presents approaches for solving counting and structural questions. It looks at how many ways a selection or arrangement can be chosen with a specific set of properties and determines if a selection or arrangement of objects exists that has a particular set of properties. To give students a bett examples of typical combinatorial problems. They also provide basic information on sets, proof techniques, enumeration, and graph theory—topics that appear frequently throughout the book. The next few chapters explore enumerative ideas, including the pigeonhole principle and inclusion/exclusion. The text then covers enumerative functions and the relations betw important families of functions, and the theorems of Pólya and Redfield. The authors also present introductions to computer algebra and group theory, before considering structures of particular interest in combinatorics: graphs, codes, Latin squares, and experimental designs. The last chapter further illustrates the interaction between linear algebra and combinator included at the end of each chapter. Ideal for undergraduate students in mathematics taking an introductory course in combinatorics, this text explores the different ways of arranging objects and selecting objects from a set. It clearly explains how to solve the various problems that arise in this branch of mathematics.

Simulation of ATM Using Elliptic Curve Cryptography in MatLab

Bijective Combinatorics

From Zero To Hero: .NET PROGRAMMING FOR STUDENTS

AI and Blockchain Technology in 6G Wireless Network

Mathematics Today

Cryptography and Cryptanalysis in MATLAB

Master the essentials of cryptography and cryptanalysis and learn how to put them to practical use. Each chapter of this book starts with an introduction to the concepts on which cryptographic algorithms are based and how they are used in practice, providing fully working examples for each of the algorithms presented. Implementation sections will guide you through the entire process of writing your own applications and programs using MATLAB. Cryptography and Cryptanalysis in MATLAB will serve as your complete reference, whether you are a student, professional developer, or researcher, showing how a multitude of cryptographic challenges can be overcome using the powerful tools of MATLAB. What You Will Learn Discover MATLAB's cryptography functions Work with conversion mechanisms in MATLAB Implement cryptographic algorithms using arithmetic operations Understand the classical, simple cryptosystems that form the basis of modern cryptography Develop fully working solutions (encryption/decryption operations) Study pseudo-random generators and their real-life implementations Utilize hash functions by way of practical examples Implement solutions to defend against practical cryptanalysis methods and attacks Understand asymmetric and symmetric encryption systems and how to use them Leverage visual cryptography, steganography, and chaos-based cryptography Who This Book Is For Those who are new to cryptography/analysis. Some prior exposure to MATLAB recommended.

Eliminating the need for heavy number-crunching, sophisticated mathematical software packages open the door to areas like cryptography, coding theory, and combinatorics that are dependent on abstract algebra. Applications of Abstract Algebra with Maple and MATLAB®, Second Edition explores these topics and shows how to apply the software programs to abstract algebra and its related fields. Carefully integrating MapleTM and MATLAB®, this book provides an in-depth introduction to real-world abstract algebraic problems. The first chapter offers a concise and comprehensive review of prerequisite advanced mathematics. The next several chapters examine block designs, coding theory, and cryptography while the final chapters cover counting techniques, including Pólya's and Burnside's theorems. Other topics discussed include the Rivest, Shamir, and Adleman (RSA) cryptosystem, digital signatures, primes for security, and elliptic curve cryptosystems. New to the Second Edition Three new chapters on Vigenère ciphers, the Advanced Encryption Standard (AES), and graph theory as well as new MATLAB and Maple sections Expanded exercises and additional research exercises Maple and MATLAB files and functions available for download online and from a CD-ROM With the incorporation of MATLAB, this second edition further illuminates the topics discussed by eliminating extensive computations of abstract algebraic techniques. The clear organization of the book as well as the inclusion of two of the most respected mathematical software packages available make the book a useful tool for students, mathematicians, and computer scientists.

This book gathers the proceedings of the 2nd International Conference on Advanced Intelligent Systems and Informatics (AISI2016), which took place in Cairo, Egypt during October 24–26, 2016. This international interdisciplinary conference, which highlighted essential research and developments in the field of informatics and intelligent systems, was organized by the Scientific Research Group in Egypt (SRGE) and sponsored by the IEEE Computational Intelligence Society (Egypt chapter) and the IEEE Robotics and Automation Society (Egypt Chapter). The book's content is divided into four main sections: Intelligent Language Processing, Intelligent Systems, Intelligent Robotics Systems, and Informatics.

Bijective proofs are some of the most elegant and powerful techniques in all of mathematics. Suitable for readers without prior background in algebra or combinatorics, Bijective Combinatorics presents a general introduction to enumerative and algebraic combinatorics that emphasizes bijective methods. The text systematically develops the mathematical tools, such as basic counting rules, recursions, inclusion-exclusion techniques, generating functions, bijective proofs, and linear-algebraic methods, needed to solve enumeration problems. These tools are used to analyze many combinatorial structures, including words, permutations, subsets, functions, compositions, integer partitions, graphs, trees, lattice paths, multisets, rook placements, set partitions, Eulerian tours, derangements, posets, tilings, and abaci. The book also delves into algebraic aspects of combinatorics, offering detailed treatments of formal power series, symmetric groups, group actions, symmetric polynomials,

determinants, and the combinatorial calculus of tableaux. Each chapter includes summaries and extensive problem sets that review and reinforce the material. Lucid, engaging, yet fully rigorous, this text describes a host of combinatorial techniques to help solve complicated enumeration problems. It covers the basic principles of enumeration, giving due attention to the role of bijective proofs in enumeration theory.

Proceedings of ICDSIS 2020

An Introduction to Combinatorics, Second Edition

A Project-Based Approach to Develop Desktop Applications

Introduction to Cryptography with Open-Source Software

Third and Fourth International Workshop, SAMOS 2003 and SAMOS 2004, Samos, Greece, July 21-23, 2003 and July 19-21, 2004, Proceedings

Introduction to Combinatorics

This book provides a comprehensive study of the security and privacy research advancements in Internet of Things (IoT). The book lays the context for discussion by introducing the vulnerable intrinsic features of IoT. By providing a comprehensive discussion of the vulnerable features, the book highlights the problem areas of IoT related to security and privacy. • Covers all aspects of security • Algorithms, protocols and technologies used in IoT have been explained and the security flaws in them analyzed with solutions • Discusses ways for achieving better access control and trust in the IoT ecosystem • Contributes exhaustive strategic plans to deal with security issues of IoT • Gathers contributions from leading-edge researchers from academia and industry Graduates, researchers, people from the industry and security professionals who want to explore the IoT security field will find this book useful. The book will give an in-depth insight in to what has happened, what new is happening and what opportunities exist in the field.

Book 1: VISUAL BASIC .NET FOR STUDENTS: A Project-Based Approach to Develop Desktop Applications In chapter one, you will get to know the properties and events of each control in a Windows Visual Basic application. You need to learn and know in order to be more familiar when applying them to some desktop applications in this book. In Tutorial 1.1, you will build a dual-mode stopwatch. The stopwatch can be started and stopped whenever desired. Two time traces: the running time when the stopwatch is active (running time) and the total time since the first stopwatch was activated. Two label controls are used to display the time (two more labels to display title information). Two button controls are used to start/stop and reset the application, one more button to exit the application. The timer control is used to periodically (every second) update the displayed time. In Tutorial 1.2, you will build a project so that children can practice basic skills in addition, subtraction, multiplication, and division operations. This Math Game project can be used to choose the types of questions and what factor you want to use. This project has three timing options. In Tutorial 1.3, you will build Bank Code game. The storage box is locked and can only be opened if you enter the correct digit combination. Combinations can be 2 to 4 non-repetitive digits (range of digits from 1 to 9). After a guess is given, you will be notified of how many digits are right and how many digits are in the right position. Based on this information, you will give another guess. You continue to guess until you get the right combination or until you stop the game. In Tutorial 1.4, you will build Horse Racing game. This is a simple game. Up to 10 horses will race to the finish line. You guessed two horses that you thought could win the race. By clicking on the Start button, the race will start. All horses will race speed to get to the finish line. In chapter two, you will learn the basic concepts of classes and objects. Next, it will demonstrate how to define class and type of enumeration, which shows how both are used in the application. In Tutorial 2.1, you will create a two-level application that uses a form to pass input user to the People class. The form class is the level of representation and the People class is the middle level. You will add controls to the form so people can enter ID, last name, and their height. When the user clicks the Save button, the code will assign input values to the People class properties. Finally, you will display the People object on a label. Figure below shows the form after the user clicks the Save button. In Tutorial 2.2, you will add a parameterized constructor to the People class. The application will ask the user to enter values, which will then be passed to the People constructor. Then, the application will display the values stored on the People object. In Tutorial 2.3, you will create an application that utilizes enumeration type. The user will choose one type of account that is listed in a ListBox control and what he chooses is then displayed in a Label control. In Tutorial 2.4, you will create a simple Bank application. This application has one class, BankAcc, and a startup form. In Tutorial 2.5, you will improve the simple Bank application, by implementing the following two properties in the BankAcc class: TotalDeposit- Total money saved in current account; TotalWithdraw- Total funds that have been withdrawn from current account. In Tutorial 2.6, you will create an application to calculate the time needed for a particular aircraft to reach takeoff speed. You will also calculate how long the runway will be required. For each type of aircraft, you are given (1) the name of the aircraft, (2) the required take-off speed (feet/sec), and (3) how fast the plane accelerates (feet/sec2). In Tutorial 2.7, you will provide a number of programming training for those who want to improve their programming skills. Your task here is to write an object-oriented application so that training manager can display and edit the training services offered. There are several training categories: (1) Application Development, (2) Database, (3) Networking, and (4) System Administration. The training itself consists of: (1) title, (2) training days, (3) category, and (4) cost. Create a class named Training that contains this information, along with its properties and a ToString() method. In chapter three, several tutorials will be presented to build more complex projects. You will build them gradually and step by step. In Tutorial 3.1, you will build Catching Ball game. The bird flew and dropped ball from the sky. User is challenged to position man under the fallen ball to catch it. In Tutorial 3.2, you will build Smart Tic Tac Toe game. The aim of this game is to win the game on a 3 x 3 grid with the victory of three identical symbols (X or O) on horizontal, diagonal, or vertical lines. The players will play alternately. In this game given two game options: player 1 against player 2 or human player against computer. A smart but simple strategy will be developed for computer logic to be a formidable opponent for human. In Tutorial 3.3, you will build a Matching Images game. Ten pairs of images hidden on the game board. The object of the game is to find image pairs. In Two Players mode, players will get turns in turn. In One Player mode, there are two options to choose from: Playing Alone or Against Computer. When Play Alone option is selected, the player will play alone without an opponent. If Against Computer option is selected, then the level of computer intelligence is given with several levels according to the level of difficulty of the game. In Tutorial 3.4, you will build Throwing Fire program. This program can be played by two human players or human player versus computer. In chapter four, tutorials will be presented to build two advanced projects. You will build them gradually and step by step. In Tutorial 4.1, you will build Roasted Duck Delivery simulation. In this simulation, a number of decisions are needed. The basic idea is to read the order by incoming telephone and tell the delivery scooter to go to the location of the order. You also need to make sure that you always provide a roasted duck ready to be transported by the delivery scooter. The delivery area is a 20 by 20 square grid. The more roasted duck is sold, the more profit it gets. In Tutorial 4.2, you will build a Drone Simulation. In this simulation, you control both vertical and horizontal thrusters to maneuver the ride to the landing pad. You will adjust the landing speed so that it is slow enough so that no accident occurs. Book 1: VISUAL C#.NET FOR STUDENTS: A Project-Based Approach to Develop Desktop Applications In chapter one, you will learn to know the properties and events of each control in a Windows Visual C# applications. You need to learn and know in order to be more familiar when applying them to some desktop applications in this book. In chapter two, you will build Throwing Fire program. This program can be played by two human players or human player versus computer. You will use 12 labels, a large control panel, and three control buttons on the form. In the control panel, a smaller panel with two group box controls and a button control are placed. In the first group box, you will use 2 radio buttons; in the second box group, place 4 radio buttons. Next, two timer controls are added to the project. All label controls are used for titles and provide scoring and game information. The large panel (Panel1) is the playing field. Three button controls are used to start / stop a program, set options, and exit the program. One timer control is used to control game animation and another is used to represent the computer's decision process. The second control panel (Panel2) is used to select game options. One group box contains radio buttons which are used to select number of players. A group box contains radio buttons to select the level of difficulty of the game, when playing against a computer. A small button is used to close the options panel. The default properties are set for one-player games with the easiest game difficulty. In chapter three, you will build Roasted Duck Delivery simulation. In this simulation, a number of decisions are needed. The basic idea is to read the order by incoming telephone and tell the delivery scooter to go to the location of the order. You also need to make sure that you always provide a roasted duck ready to be transported by the delivery scooter. The delivery area is a 20 by 20 square grid. The more roasted duck is sold, the more profit it gets. The panel control on the left side of the form contains the delivery grid. On the upper right are group boxes with two label controls to display the time or hour and sale results. The computer monitor (in a picture box) displays order and delivery status using a list box and label control. Another group box contains a roasting oven when the roasted ducks are displayed using eight picture box controls. Two button controls on the group box control the operation of the oven. Group boxes under the oven show how many ducks are ready to be delivered and how many are in the delivery scooter (a button control is to load the roasted duck into the scooter). The two button controls beneath are used to start/pause the game and to stop the game or exit the game. In the area under the form there are several timers for controlling a number of aspects in the program. The delivery grid consists of 400 label controls on 20 rows (marked with numbers) and 20 columns (marked with letters). Here, you will learn how to place controls on a form (or panel in this case) using code (when the program runs, not when designing the form). This mechanism can save time designing the form. In chapter four, you will build a Drone Simulation. In this simulation, you control both vertical and horizontal thrusters to maneuver the ride to the landing pad. You will adjust the landing speed so that it is slow enough so that no accident occurs. You build the form in two stages, the first stage creates two option group boxes, and then the second stage uses both those group boxes as landing controls. Two control panels are placed on the left side of the form: one panel for drawing and another panel for the edge. On the right side of the form, place the two group control boxes. In the first group box, five radio buttons and a check box are added. In the second group box, two radio buttons are placed. In the below section of the form, three buttons are added. Finally, one timer control is added. Then in the form, a group box is added overlap panel. Then, 11 label controls are added to the group box. After that, a progress bar is added. Under the bar, two control panels are added, one high panel and one short panel. In the second (short) panel control, two small label controls are added. Underneath, three button controls are placed. Under these three buttons, a label control is added. For each label control, set the AutoSize property to False to be resized and set (temporarily) the BorderStyle property to FixedSingle so that you can see the edges to facilitate the layout process. In this chapter, you will build Jumper game. In this game, you will move the jumper across the busy road, avoid the tiger, and cross the river with the changing current to get to house safely. You will place four label controls on the top part of the form (set the AutoSize property to False so that it can be resized and the BorderStyle property temporarily becomes FixedSingle so you can see the edges). Then, you use five panel controls below the labels. These panels will be a place for image graphics. Each panel has a width of 16 jumpers or 640 pixels, because one jumper will be given a width of 40 pixels. The first panel will be the jumper house, which will be given a height of 80 pixels. The next panel will become a river, with a height of 120 pixels. The next panel will be a place for tiger, 40 pixels high. Under the snake panel, there is a road panel. This panel will contain three boat lanes. Each boat has a height of 40 pixels, but you will give it a height of 140 pixels (not 120 pixels) to make room for lane markers. The fifth panel is the place where the jumper will begin its journey or leap. This panel will be given a height of 40 pixels. Add the last control panel below the form with three button controls. Then, finally, add four timer controls. Adjust the size of the form so that the panel controls can occupy according to the width of the form. BOOK 3: VISUAL C# .NET : A Step By Step, Project-Based Guide to Develop Desktop Applications In chapter one, you will learn to know the properties and events of each control in a Windows Visual C# application. You need to learn and know in order to be more familiar when applying them to some applications in this book. In chapter two, you will build a project so that children can practice basic skills in addition, subtraction, multiplication, and division operations. This Math Game project can be used to choose the types of questions and what factors you want to use. This project has three timing options. Random math problems using values from 0 to 9 will be presented. Timing options are provided to measure accuracy and speed. There are many controls used. Two label controls are used for title information, two for displaying scores. There is a wide label in the middle of the form to display math questions. And, long skinny label is used as separator. Two button controls are used to start and stop question and one button to exit the project. There are three group control boxes. The first group box holds four check box controls that are used to select the type of questions. The second group box holds eleven radio buttons that are used to select values that are used as factors in calculations. The third group box contains three radio button controls for timing options. A scroll bar control rod is used to change the time. In chapter three, you will build Bank Code game. The storage box is locked and can only be opened if you enter the correct digit combination. Combinations can be 2 to 4 non-repetitive digits (range of digits from 1 to 9). After a guess is given, you will be notified of how many digits are right and how many digits are in the right position. Based on this information, you will give another guess. You continue to guess until you get the right combination or until you stop the game. On the left side of the form is a large picture box control. On the right side, two group box controls and two button controls are placed. In the picture box, a control panel is placed. In the panel, there are four label controls (set the AutoSize property to False) and nine button controls. In the first group box control, place three radio buttons. In the second group box control, a text box control is placed. The picture box contains an image of bank and a panel. The label controls in the panel are used to display the combinations entered (the BorderStyle property set to FixedSingle to display the label size). The nine buttons on the panel are used to enter combinations. Radio buttons are used to set options. The buttons (one to start and stop the game and another to exit the project) are used to control game operations. The text box displays the results of the combinations entered. In chapter four, you will build Horse Racing game. This is a simple game. Up to 10 horses will race to the finish line. You guessed two horses that you thought could win the race. By clicking on the Start button, the race will start. All horses will race speed to get to the finish line. Labels are used to display instructions and number of horses in a race. Four button controls are used: two buttons to change number of horses, one button to start the game, and one other button to stop the game. The picture box control is used to load the horse image. A timer control is used to update the horse's movement during the race. In chapter five, you will build Catching Ball game. The bird flew and dropped ball from the sky. Users are challenged to position man under the fallen ball to catch it. Labels are used for instructions and to display game information (remaining time, number of balls captured, and game difficulty level). Two buttons are used to change the game difficulty level, one button to start the game, and another button to stop the game. Picture box controls hold images for man, bird, and ball. In chapter six, you will build Smart Tic Tac Toe game. That said, this is the first game ever programmed on a computer and one that had been programmed by Bill Gates himself when he was a teenager while attending Lakeside School in Seattle. The aim of this game is to win the game on a 3 x 3 grid with the victory of three identical symbols (X or O) on horizontal, diagonal, or vertical lines. The players will play alternately. In this game given two game options: player 1 against player 2 or human player against computer. A smart but simple strategy will be developed for computer logic to be a formidable opponent for humans. In chapter seven, you will build Fighting Plane program. This program can be played by two human players or human player versus computer. The controls of the player are done via the keyboard. Player 1 presses A key to move up, Z key to move down, and S key to throw rudal. When you choose Two players from the Options button, this game can be played by two human players. Player 1 presses the same keys, while player 2 presses key K to move up, M to move down, and key J to throw rudal. All label controls are used for titles and provide scoring and game information. The large panel (Panel1) is the playing field. Three button controls are used to start / stop a program, set options, and exit the program. One timer control is used to control game animation and another is used to represent the computer's decision process. The second control panel (Panel2) is used to select game options. One group box contains radio buttons which are used to select number of players. A group box contains radio buttons to select the level of difficulty of the game, when playing against a computer. A small button is used to close the options panel. The default properties are set for one-player games with the easiest game difficulty.

From the exciting history of its development in ancient times to the present day, Introduction to Cryptography with Mathematical Foundations and Computer Implementations provides a focused tour of the central concepts of cryptography. Rather than present an encyclopedic treatment of topics in cryptography, it delineates cryptographic concepts in chronological order, developing the mathematics as needed. Written in an engaging yet rigorous style, each chapter introduces important concepts with clear definitions and theorems. Numerous examples explain key points while figures and tables help illustrate more difficult or subtle concepts. Each chapter is punctuated with "Exercises for the Reader;" complete solutions for these are included in an appendix. Carefully crafted exercise sets are also provided at the end of each chapter, and detailed solutions to most odd-numbered exercises can be found in a designated appendix. The computer implementation section at the end of every chapter guides students through the process of writing their own programs. A supporting website provides an extensive set of sample programs as well as downloadable platform-independent applet pages for some core programs and algorithms. As the reliance on cryptography by business, government, and industry continues and new technologies for transferring data become available, cryptography plays a permanent, important role in day-to-day operations. This self-contained sophomore-level text traces the evolution of the field, from its origins through present-day cryptosystems, including public key cryptography and elliptic curve cryptography.

This proceeding features papers discussing big data innovation for sustainable cognitive computing. The papers feature detail on cognitive computing and its self-learning systems that use data mining, pattern recognition and natural language processing (NLP) to mirror the way the human brain works. This international conference focuses on cognitive computing technologies, from knowledge representation techniques and natural language processing algorithms to dynamic learning approaches. Topics covered include Data Science for Cognitive Analysis, Real-Time Ubiquitous Data Science, Platform for Privacy Preserving Data Science, and Internet-Based Cognitive Platform. The EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing (BDCC 2018), took place on 13 – 15 December 2018 in Coimbatore, India.

Wireless Communication Networks and Internet of Things

BDCC 2018

Digital Signal Processing and Applications with the C6713 and C6416 DSK

Interdisciplinary Digital Preservation Tools and Technologies

Creating and Programming Advanced Algorithms

Cloud Security: Concepts, Methodologies, Tools, and Applications

In chapter one, you will get to know the properties and events of each control in a Windows Visual Basic application. You need to learn and know in order to be more familiar when applying them to some desktop applications in this book. In Tutorial 1.1, you will build a dual-mode stopwatch. The stopwatch can be started and stopped whenever desired. Two time traces: the running time when the stopwatch is active (running time) and the total time since the first stopwatch was activated. Two label controls are used to display the time (two more labels to display title information). Two button controls are used to start/stop and reset the application, one more button to exit the application. The timer control is used to periodically (every second) update the displayed time. In Tutorial 1.2, you will build a project so that children can practice basic skills in addition, subtraction, multiplication, and division operations. This Math Game project can be used to choose the types of questions and what factor you want to use. This project has three timing options. In Tutorial 1.3, you will build Bank Code game. The storage box is locked and can only be opened if you enter the correct digit combination. Combinations can be 2 to 4 non-repetitive digits (range of digits from 1 to 9). After a guess is given, you will be notified of how many digits are right and how many digits are in the right position. Based on this information, you will give another guess. You continue to guess until you get the right combination or until you stop the game. In Tutorial 1.4, you will build Horse Racing game. This is a simple game. Up to 10 horses will race to the finish line. You guessed two horses that you thought could win the race. By clicking on the Start button, the race will start. All horses will race speed to get to the finish line. In chapter two, you will learn the basic concepts of classes and objects. Next, it will demonstrate how to define class and type of enumeration, which shows how both are used in the application. In Tutorial 2.1, you will create a two-level application that uses a form to pass input user to the People class. The form class is the level of representation and the People class is the middle level. You will add controls to the form so people can enter ID, last name, and their height. When the user clicks the Save button, the code will assign input values to the People class properties. Finally, you will display the People object on a label. Figure below shows the form after the user clicks the Save button. In Tutorial 2.2, you will add a parameterized constructor to the People class. The application will ask user to enter values, which will then be passed to the People constructor. Then, the application will display the values stored on the People object. In Tutorial 2.3, you will create an application that utilizes enumeration type. The user will choose one type of account that is listed in a ListBox control and what he chooses is then displayed in a Label control. In Tutorial 2.4, you will create a simple Bank application. This application has one class, BankAcc, and a startup form. In Tutorial 2.5, you will improve the simple Bank application, by implementing the following two properties in the BankAcc class: TotalDeposit- Total money saved in current account; TotalWithdraw- Total funds that have been withdrawn from current account. In Tutorial 2.6,

you will create an application to calculate the time needed for a particular aircraft to reach takeoff speed. You will also calculate how long the runway will be required. For each type of aircraft, you are given (1) the name of the aircraft, (2) the required take-off speed (feet/sec), and (3) how fast the plane accelerates (feet/sec2). In Tutorial 2.7, you will provide a number of programming training for those who want to improve their programming skills. Your task here is to write an object-oriented application so that training manager can display and edit the training services offered. There are several training categories: (1) Application Development, (2) Database, (3) Networking, and (4) System Administration. The training itself consists of: (1) title, (2) training days, (3) category, and (4) cost. Create a class named Training that contains this information, along with its properties and a ToString() method. In chapter three, several tutorials will be presented to build more complex projects. You will build them gradually and step by step. In Tutorial 3.1, you will build Catching Ball game. The bird flew and dropped ball from the sky. User is challenged to position man under the fallen ball to catch it. In Tutorial 3.2, you will build Smart Tic Tac Toe game. The aim of this game is to win the game on a 3 x 3 grid with the victory of three identical symbols (X or O) on horizontal, diagonal, or vertical lines. The players will play alternately. In this game given two game options: player 1 against player 2 or human player against computer. A smart but simple strategy will be developed for computer logic to be a formidable opponent for human. In Tutorial 3.3, you will build a Matching Images game. Ten pairs of images hidden on the game board. The object of the game is to find image pairs. In Two Players mode, players will get turns in turn. In One Player mode, there are two options to choose from: Playing Alone or Against Computer. When Play Alone option is selected, the player will play alone without an opponent. If Against Computer option is selected, then the level of computer intelligence is given with several levels according to the level of difficulty of the game. In Tutorial 3.4, you will build Throwing Fire program. This program can be played by two human players or human player versus computer. In chapter four, tutorials will be presented to build two advanced projects. You will build them gradually and step by step. In Tutorial 4.1, you will build Roasted Duck Delivery simulation. In this simulation, a number of decisions are needed. The basic idea is to read the order by incoming telephone and tell the delivery scooter to go to the location of the order. You also need to make sure that you always provide a roasted duck ready to be transported by the delivery scooter. The delivery area is a 20 by 20 square grid. The more roasted duck is sold, the more profit it gets. In Tutorial 4.2, you will build a Drone Simulation. In this simulation, you control both vertical and horizontal thrusters to maneuver the ride to the landing pad. You will adjust the landing speed so that it is slow enough so that no accident occurs.

Emphasizes a Problem Solving Approach A first course in combinatorics Completely revised, How to Count: An Introduction to Combinatorics, Second Edition shows how to solve numerous classic and other interesting combinatorial problems. The authors take an easily accessible approach that introduces problems before leading into the theory involved. Although the authors present most of the topics through concrete problems, they also emphasize the importance of proofs in mathematics. New to the Second Edition This second edition incorporates 50 percent more material. It includes seven new chapters that cover occupancy problems, Stirling and Catalan numbers, graph theory, trees, Dirichlet's pigeonhole principle, Ramsey theory, and rook polynomials. This edition also contains more than 450 exercises. Ideal for both classroom teaching and self-study, this text requires only a modest amount of mathematical background. In an engaging way, it covers many combinatorial tools, such as the inclusion-exclusion principle, generating functions, recurrence relations, and Pólya's counting theorem.

Cloud computing has experienced explosive growth and is expected to continue to rise in popularity as new services and applications become available. As with any new technology, security issues continue to be a concern, and developing effective methods to protect sensitive information and data on the cloud is imperative. Cloud Security: Concepts, Methodologies, Tools, and Applications explores the difficulties and challenges of securing user data and information on cloud platforms. It also examines the current approaches to cloud-based technologies and assesses the possibilities for future advancements in this field. Highlighting a range of topics such as cloud forensics, information privacy, and standardization and security in the cloud, this multi-volume book is ideally designed for IT specialists, web designers, computer engineers, software developers, academicians, researchers, and graduate-level students interested in cloud computing concepts and security.

This book highlights future research directions and latent solutions by integrating AI and Blockchain 6G networks, comprising computation efficiency, algorithms robustness, hardware development and energy management. This book brings together leading researchers in Academia and industry from diverse backgrounds to deliver to the technical community an outline of emerging technologies, advanced architectures, challenges, open issues and future directions of 6G networks. This book is written for researchers, professionals and students to learn about the integration of technologies such as AI and Blockchain into 6G network and communications. This book addresses the topics such as consensus protocol, architecture, intelligent dynamic resource management, security and privacy in 6G to integrate AI and Blockchain and new real-time application with further research opportunities.

7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, Tarragona, Spain, April 19-21, 2006, Proceedings
A Student's Guide to the Study, Practice, and Tools of Modern Mathematics
Handbook of Mathematical Induction
Finite-Dimensional Linear Algebra
International Conferences, SecTech, CA, CES3 2012, Held in Conjunction with GST 2012, Jeju Island, Korea, November 28-December 2, 2012. Proceedings

The international conference on Advances in Computing and Information technology (ACITY 2012) provides an excellent international forum for both academics and professionals for sharing knowledge and results in theory, methodology and applications of Computer Science and Information Technology. The Second International Conference on Advances in Computing and Information technology (ACITY 2012), held in Chennai, India, during July 13-15, 2012, covered a number of topics in all major fields of Computer Science and Information Technology including: networking and communications, network security and applications, web and internet computing, ubiquitous computing, algorithms, bioinformatics, digital image processing and pattern recognition, artificial intelligence, soft computing and applications. Upon a strength review process, a number of high-quality, presenting not only innovative ideas but also a founded evaluation and a strong argumentation of the same, were selected and collected in the present proceedings, that is composed of three different volumes.

A Student's Guide to the Study, Practice, and Tools of Modern Mathematics provides an accessible introduction to the world of mathematics. It offers tips on how to study and write mathematics as well as how to use various mathematical tools, from LaTeX and Beamer to Mathematica® and MapleTM to MATLAB® and R. Along with a color insert, the text includes exercises and challenges to stimulate creativity and improve problem solving abilities. The first section of the book covers issues pertaining to studying mathematics. The authors explain how to write mathematical proofs and papers, how to perform mathematical research, and how to give mathematical presentations. The second section focuses on the use of mathematical tools for mathematical typesetting, generating data, finding patterns, and much more. The text describes how to compose a LaTeX file, give a presentation using Beamer, create mathematical diagrams, use computer algebra systems, and display ideas on a web page. The authors cover both popular commercial software programs and free and open source software, such as Linux and R. Showing how to use technology to understand mathematics, this guide supports students on their way to becoming professional mathematicians. For beginning mathematics students, it helps them study for tests and write papers. As time progresses, the book aids them in performing advanced activities, such as computer programming, typesetting, and research.

This work is about implementing Elliptic Curve Cryptography to make ATM working secure and reliable. ECC is advanced Cryptography scheme which is advanced and take less size of keys to implement security and also provide methods to implement customer authentication very well. ATM is Automated Teller Machine with which ECC is combined to make it much secure and reliable. ECDSA algorithm is used to generate signatures for authentication. Elliptic Curves provide much secure keys which is the strongest part of this simulation work.

This two-volume set (CCIS 1229 and CCIS 1230) constitutes the refereed proceedings of the 5th International Conference on Recent Developments in Science, Engineering and Technology, REDSET 2019, held in Gurugram, India, in November 2019. The 74 revised full papers presented were carefully reviewed and selected from total 353 submissions. The papers are organized in topical sections on data centric programming; next generation computing; social and web analytics; security in data science analytics; big data analytics.

How to Count
Guide to Elliptic Curve Cryptography
5th International Conference on Recent Developments in Science, Engineering and Technology, REDSET 2019, Gurugram, India, November 15–16, 2019, Revised Selected Papers, Part I
Algebraic Number Theory
Elliptic Curve Cryptography
Evolutionary Computing and Mobile Sustainable Networks

Bringing the material up to date to reflect modern applications, Algebraic Number Theory, Second Edition has been completely rewritten and reorganized to incorporate a new style, methodology, and presentation. This edition focuses on integral domains, ideals, and unique factorization in the first chapter; field extensions in the second chapter; and

The way information is shared and retained has evolved throughout the years. This progression into the digital age provides longevity and easy accessibility of information, while new advancements keep rolling society into the future. Interdisciplinary Digital Preservation Tools and Technologies addresses the processes that encompass digital conversion and preservation of information into electronic formats. This book provides exhaustive coverage on the details of digital preservation, lists the latest happenings in this field, and spreads awareness of this topic in order to keep the expansion of converting digital ongoing. This publication is a critical reference source for academicians, researchers, and students seeking current research on the impact of digital advancements.

Advances in Computing and Information Technology
Data Science and Analytics
Proceedings of the Second International Conference on Advances in Computing and Information Technology (ACITY) July 13-15, 2012, Chennai, India - Volume 1
Proceedings of ICDTA 21, Fez, Morocco