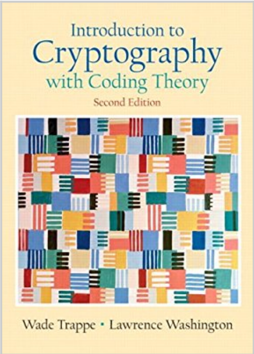

Introduction to Cryptography with Coding Theory (2nd Edition)

By Wade Trappe, Lawrence C. Washington

Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington

With its conversational tone and practical focus, this text mixes applied and theoretical aspects for a solid introduction to cryptography and security, including the latest significant advancements in the field. Assumes a minimal background. The level of math sophistication is equivalent to a course in linear algebra. Presents applications and protocols where cryptographic primitives are used in practice, such as SET and SSL. Provides a detailed explanation of AES, which has replaced Feistel-based ciphers (DES) as the standard block cipher algorithm. Includes expanded discussions of block ciphers, hash functions, and multicollisions, plus additional attacks on RSA to make readers aware of the strengths and shortcomings of this popular scheme. For engineers interested in learning more about cryptography.

Introduction to Cryptography with Coding Theory (2nd Edition)

By Wade Trappe, Lawrence C. Washington

Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington

With its conversational tone and practical focus, this text mixes applied and theoretical aspects for a solid introduction to cryptography and security, including the latest significant advancements in the field. Assumes a minimal background. The level of math sophistication is equivalent to a course in linear algebra. Presents applications and protocols where cryptographic primitives are used in practice, such as SET and SSL. Provides a detailed explanation of AES, which has replaced Feistel-based ciphers (DES) as the standard block cipher algorithm. Includes expanded discussions of block ciphers, hash functions, and multicollisions, plus additional attacks on RSA to make readers aware of the strengths and shortcomings of this popular scheme. For engineers interested in learning more about cryptography.

Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington Bibliography

- Sales Rank: #654306 in Books
- Brand: Trappe, Wade/ Washington, Lawrence C.
- Published on: 2005-07-25
- Ingredients: Example Ingredients
- Original language: English
- Number of items: 1
- Dimensions: 9.40" h x 1.40" w x 7.20" l, 2.16 pounds
- Binding: Hardcover
- 592 pages

Editorial Review

From the Back Cover
This book assumes a minimal background in programming and a level of math sophistication equivalent to a course in linear algebra. It provides a flexible organization, as each chapter is modular and can be covered in any order. Using Mathematica, Maple, and MATLAB, computer examples included in an Appendix explain how to do computation and demonstrate important concepts. A full chapter on error correcting codes introduces the basic elements of coding theory. Other topics covered: Classical cryptosystems, basic number theory, the data encryption standard, AES: Rijndael, the RSA algorithm, discrete logarithms, digital signatures, e-commerce and digital cash, secret sharing schemes, games, zero knowledge techniques, key establishment protocols, information theory, elliptic curves, error correcting codes, quantum cryptography. For professionals in cryptography and network security.

This book is based on a course in cryptography at the upper level undergraduate and beginning graduate level that has been given at the University of Maryland since 1997. When designing the course, we decided on the following requirements.

* The course should be up-to-date and cover a broad selection of topics from a mathematical point of view.
* The material should be accessible to mathematically mature students having little background in number theory and computer programming.
* There should be examples involving numbers large enough to demonstrate how the algorithms really work.

We wanted to avoid concentrating solely on RSA and discrete logarithms, which would have made the course mostly a number theory course. We also did not want to teach a course on protocols and how to hack into friends' computers. That would have made the course less mathematical than desired.

There are numerous topics in cryptology that can be discussed in an introductory course. We have tried to include many of them. The chapters represent, for the most part, topics that were covered during the different semesters we taught the course. There is certainly more material here than could be treated in most one-semester courses. The first eight chapters represent the core of the material. The choice of which of the remaining chapters are used depends on the level of the students.

The chapters are numbered, thus giving them an ordering. However, except for Chapter 3 on number theory, which pervades the subject, the chapters are fairly independent of each other and can be covered in almost any reasonable order. Although we don't recommend doing so, a daring reader could possibly read Chapters 4 through 17 in reverse order, with only having to look ahead/behind a few times.

The chapters on Information Theory, Elliptic Curves, (quantum Methods, and Error Correcting Codes are somewhat more mathematical than the others. The chapter on Error Correcting Codes was included, at the suggestion of several reviewers, because courses that include introductions to both cryptology and coding theory are fairly common.

Computer examples. Suppose you want to give an example for RSA. You could choose two one-digit primes and pretend to be working with fifty-digit primes, or you could use your favorite software package to do an actual example with large primes. Or perhaps you are working with shift ciphers and are trying to decrypt a message by trying all 26 shifts of the ciphertext. This should also be done on a computer. At the end of the book are appendices containing Computer Examples written in each of Mathematica®, Maple®, and MATLAB® that show how to do such calculations. These languages were chosen because they are user friendly and do not require prior programming experience. Although the course has been taught successfully without computers, these examples are an integral part of the book and should be studied, if at all possible. Not only do they contain numerical examples of how to do certain computations but also they demonstrate important ideas and issues that arise. They were placed at the end of the book because of the logistic and aesthetic problems of including extensive computer examples in three languages at the ends of chapters.

Programs available in each of the three languages can be downloaded from the Web site prenhall/washington

In a classroom, all that is needed is a computer (with one of the languages installed) and a projector in order to produce meaningful examples as the lecture is being given. Homework problems (the Computer Problems in various chapters) based on the software allow students to play with examples individually. Of course, students having more programming background could write their own programs instead.

This book is based on a course in cryptography at the upper level undergraduate and beginning graduate level that has been given at the University of Maryland since 1997. When designing the course, we decided on the following requirements.

- The course should be up-to-date and cover a broad selection of topics from a mathematical point of view.
- The material should be accessible to mathematically mature students having little background in number theory and computer programming.
- There should be examples involving numbers large enough to demonstrate how the algorithms really work.

We wanted to avoid concentrating solely on RSA and discrete logarithms, which would have made the course mostly a number theory course. We also did not want to teach a course on protocols and how to hack into friends' computers. That would have made the course less mathematical than desired.

There are numerous topics in cryptology that can be discussed in an introductory course. We have tried to include many of them. The chapters represent, for the most part, topics that were covered during the different semesters we taught the course. There is certainly more material here than could be treated in most one-semester courses. The first eight chapters represent the core of the material. The choice of which of the remaining chapters are used depends on the level of the students.

The chapters are numbered, thus giving them an ordering. However, except for Chapter 3 on number theory, which pervades the subject, the chapters are fairly independent of each other and can be covered in almost any reasonable order. Although we don't recommend doing so, a daring reader could possibly read Chapters 4 through 17 in reverse order, with only having to look ahead/behind a few times.

The chapters on Information Theory, Elliptic Curves, (quantum Methods, and Error Correcting Codes are somewhat more mathematical than the others. The chapter on Error Correcting Codes was included, at the suggestion of several reviewers, because courses that include introductions to both cryptology and coding theory are fairly common.

Computer examples. Suppose you want to give an example for RSA. You could choose two one-digit primes and pretend to be working with fifty-digit primes, or you could use your favorite software package to do an actual example with large primes. Or perhaps you are working with shift ciphers and are trying to decrypt a message by trying all 26 shifts of the ciphertext. This should also be done on a computer. At the end of the book are appendices containing Computer Examples written in each of Mathematica®, Maple®, and MATLAB® that show how to do such calculations. These languages were chosen because they are user friendly and do not require prior programming experience. Although the course has been taught successfully without computers, these examples are an integral part of the book and should be studied, if at all possible. Not only do they contain numerical examples of how to do certain computations but also they demonstrate important ideas and issues that arise. They were placed at the end of the book because of the logistic and aesthetic problems of including extensive computer examples in three languages at the ends of chapters.

Programs available in each of the three languages can be downloaded from the Web site **www.prenhall.com/washington**

In a classroom, all that is needed is a computer (with one of the languages installed) and a projector in order to produce meaningful examples as the lecture is being given. Homework problems (the Computer Problems in various chapters) based on the software allow students to play with examples individually. Of course, students having more programming background could write their own programs instead.

Users Review

From reader reviews:

Frances Feist:

This Introduction to Cryptography with Coding Theory (2nd Edition) tend to be reliable for you who want to be described as a successful person, why. The main reason of this Introduction to Cryptography with Coding Theory (2nd Edition) can be one of many great books you must have is usually giving you more than just simple examining food but feed you with information that perhaps will shock your prior knowledge. This book is handy, you can bring it everywhere you go and whenever your conditions in the e-book and printed people. Beside that this Introduction to Cryptography with Coding Theory (2nd Edition) forcing you to have an enormous of experience for example rich vocabulary, giving you test of critical thinking that we realize it useful in your day activity. So , let's have it and revel in reading.

Jeremy Smith:

Often the book Introduction to Cryptography with Coding Theory (2nd Edition) will bring someone to the new experience of reading a new book. The author style to spell out the idea is very unique. In the event you try to find new book to study, this book very suitable to you. The book Introduction to Cryptography with Coding Theory (2nd Edition) is much recommended to you you just read. You can also get the e-book from your official web site, so you can quickly to read the book.

Tony Paulson:

The book untitled Introduction to Cryptography with Coding Theory (2nd Edition) contain a lot of information on it. The writer explains the girl idea with easy technique. The language is very clear and understandable all the people, so do not really worry, you can easy to read that. The book was written by famous author. The author brings you in the new time of literary works. You can actually read this book because you can continue reading your smart phone, or program, so you can read the book in anywhere and anytime. In a situation you wish to purchase the e-book, you can open up their official web-site and also order it. Have a nice read.

Doris Stone:

What is your hobby? Have you heard that question when you got scholars? We believe that that problem was given by teacher with their students. Many kinds of hobby, Every person has different hobby. Therefore you know that little person like reading or as studying become their hobby. You need to understand that reading is very important in addition to book as to be the thing. Book is important thing to increase you knowledge, except your teacher or lecturer. You discover good news or update in relation to something by book. A substantial number of sorts of books that can you decide to try be your object. One of them are these claims Introduction to Cryptography with Coding Theory (2nd Edition).

Read Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington for online ebook