



Introduction to Cryptography with Coding Theory (2nd Edition)

By Wade Trappe, Lawrence C. Washington

Download now

Read Online ➔

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.

↓ [Download Introduction to Cryptography with Coding Theory \(2 ...pdf](#)

📄 [Read Online Introduction to Cryptography with Coding Theory ...pdf](#)

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

 [Download Introduction to Cryptography with Coding Theory \(2 ...pdf](#)

 [Read Online Introduction to Cryptography with Coding Theory ...pdf](#)

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.

Excerpt. © Reprinted by permission. All rights reserved.

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.

Excerpt. © Reprinted by permission. All rights reserved.

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:

Brenda Schweiger:

What do you concerning book? It is not important together with you? Or just adding material when you want something to explain what your own problem? How about your extra time? Or are you busy person? If you don't have spare time to complete others business, it is gives you the sense of being bored faster. And you have time? What did you do? Everybody has many questions above. They need to answer that question mainly because just their can do this. It said that about publication. Book is familiar in each person. Yes, it is proper. Because start from on guardería until university need this specific Introduction to Cryptography with Coding Theory (2nd Edition) to read.

Tara Carlson:

The feeling that you get from Introduction to Cryptography with Coding Theory (2nd Edition) could be the more deep you searching the information that hide within the words the more you get enthusiastic about reading it. It doesn't mean that this book is hard to recognise but Introduction to Cryptography with Coding Theory (2nd Edition) giving you joy feeling of reading. The author conveys their point in specific way that can be understood simply by anyone who read the item because the author of this e-book is well-known enough. This kind of book also makes your current vocabulary increase well. Making it easy to understand then can go together with you, both in printed or e-book style are available. We advise you for having this Introduction to Cryptography with Coding Theory (2nd Edition) instantly.

Rita Carter:

Many people spending their time by playing outside along with friends, fun activity along with family or just

watching TV 24 hours a day. You can have new activity to shell out your whole day by examining a book. Ugh, do you consider reading a book can definitely hard because you have to take the book everywhere? It okay you can have the e-book, delivering everywhere you want in your Mobile phone. Like Introduction to Cryptography with Coding Theory (2nd Edition) which is having the e-book version. So , try out this book? Let's find.

James Hibner:

As a student exactly feel bored for you to reading. If their teacher expected them to go to the library as well as to make summary for some book, they are complained. Just minor students that has reading's soul or real their passion. They just do what the trainer want, like asked to the library. They go to presently there but nothing reading really. Any students feel that reading through is not important, boring in addition to can't see colorful photographs on there. Yeah, it is for being complicated. Book is very important in your case. As we know that on this time, many ways to get whatever we wish. Likewise word says, ways to reach Chinese's country. So , this Introduction to Cryptography with Coding Theory (2nd Edition) can make you really feel more interested to read.

Download and Read Online Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington #HC6W4TMIXLY

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

Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington books to read online.

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

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

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

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

HC6W4TMIXLY: Introduction to Cryptography with Coding Theory (2nd Edition) By Wade Trappe, Lawrence C. Washington