Springer 1441926747

User Manual: An Introduction to Mathematical Cryptography

Model: 1441926747

1. Introduction to the Text

This book, "An Introduction to Mathematical Cryptography," provides a comprehensive introduction to the theory of public key cryptography and the mathematical principles underpinning it. It covers the historical context of public key cryptography, including the seminal work by Diffie and Hellman in 1976 and the subsequent RSA cryptosystem by Rivest, Shamir, and Adleman in 1978. The text emphasizes the importance of these cryptographic systems in modern computing and internet security.

The book is designed to be self-contained, developing necessary mathematical concepts from various fields such as number theory, abstract algebra, probability, and information theory. It aims to equip students with a solid understanding of the mathematical foundations required for both constructing and analyzing the security of cryptographic schemes.

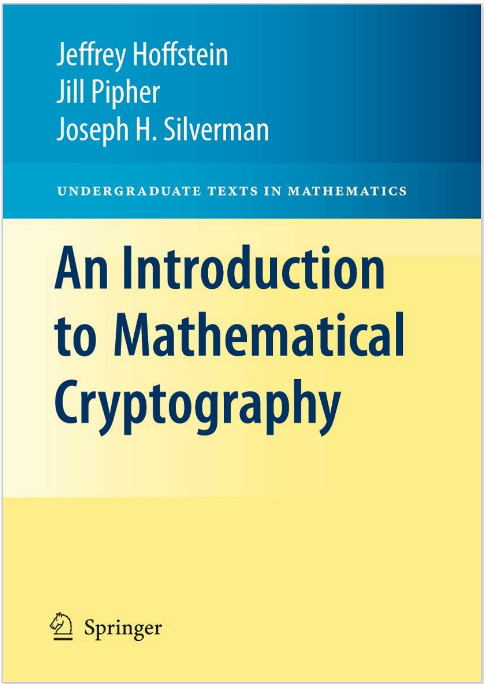
Jeffrey Hoffstein
Jill Pipher
Joseph H. Silverman
UNDERGRADUATE TEXTS IN MATHEMATICS
An Introduction to Mathematical Cryptography
Springer

Figure 1.1: Front cover of "An Introduction to Mathematical Cryptography" by Hoffstein, Pipher, and Silverman. The cover features the title prominently against a yellow and blue background, with the authors' names and publisher logo visible.

2. Key Topics Covered

The book focuses primarily on public key cryptosystems and digital signature schemes, offering an in-depth exploration of the required mathematics. Key topics include:

- **Classical Cryptographic Constructions:** This includes detailed discussions on Diffie-Hellmann key exchange, discrete logarithm-based cryptosystems, the RSA cryptosystem, and various digital signature methods.
- **Fundamental Mathematical Tools:** Essential mathematical concepts for cryptography are introduced, such as primality testing, factorization algorithms, probability theory, information theory, and collision algorithms.
- **Recent Cryptographic Innovations:** The text covers advanced topics like elliptic curves, elliptic curve and pairing-based cryptography, lattices, lattice-based cryptography, and the NTRU cryptosystem.

3. Target Audience and Prerequisites

This textbook is intended for advanced undergraduate or beginning graduate students in mathematics and computer science. The only formal prerequisite is a first course in linear algebra. Students with stronger mathematical backgrounds can proceed directly to cryptographic applications and advanced topics.

The self-contained nature of the book ensures that all necessary mathematical concepts are introduced and developed within the text, making it accessible to students who may not have extensive prior exposure to number theory or abstract algebra.

4. Structure and Organization

The book is structured to guide the reader through the theoretical underpinnings of modern cryptography. Each topic is presented with sufficient detail, including examples and exercises at the end of each chapter to reinforce understanding. The progression of topics is logical, moving from foundational mathematical concepts to their application in various cryptographic schemes.

The text includes an extensive bibliography for further reading and an index for easy reference. Supplementary materials may be available online, as noted in the book's description.

5. Authors

Jeffrey Hoffstein

Professor at Brown University since 1989. His research focuses on number theory, automorphic forms, and cryptography. He has authored over 50 publications.

Jill Pipher

Professor at Brown University since 1989. Her research areas include harmonic analysis, elliptic PDE, and cryptography. She has authored over 40 publications and received numerous awards.

J.H. Silverman (Joseph Silverman)

Professor at Brown University since 1988, and former Chair of the Brown Mathematics department. His research interests include number theory, arithmetic geometry, elliptic curves, dynamical systems, and cryptography. He has authored over 120 publications and mentored more than 20 doctoral students.

6. Specifications

Attribute	Detail
Publisher	Springer
Publication Date	December 1, 2010
Edition	Softcover reprint of hardcover 1st ed. 2008
Language	English
Print Length	540 pages
ISBN-10	1441926747
ISBN-13	978-1441926746
Item Weight	1.6 pounds
Dimensions	6.1 x 1.22 x 9.25 inches

7. Setup: Approaching the Text

To effectively engage with "An Introduction to Mathematical Cryptography," consider the following approach:

1. **Review Prerequisites:** Ensure a foundational understanding of linear algebra. While the book is self-contained, a solid grasp of basic mathematical concepts will facilitate smoother progress.
2. **Chapter-by-Chapter Study:** The material is structured to build knowledge incrementally. It is recommended to follow the chapters sequentially to fully appreciate the development of concepts.
3. **Engage with Examples:** The text includes numerous examples. Work through these examples to see the theoretical concepts applied in practice.
4. **Utilize Exercises:** Each chapter concludes with exercises. Attempting these exercises is crucial for consolidating understanding and developing problem-solving skills in cryptography.

8. Operating: Using the Book for Study

This book serves as an excellent resource for both classroom learning and independent study:

- **Classroom Use:** Instructors can use this book as a primary textbook for courses in mathematical cryptography, leveraging its clear explanations and structured progression.
- **Self-Study:** Individuals interested in learning the mathematical foundations of cryptography can use this book independently. The detailed explanations and self-contained nature support self-paced learning.
- **Reference:** The comprehensive coverage of topics and extensive bibliography make it a valuable reference for researchers and practitioners in the field.

9. Maintenance: Caring for Your Book

To ensure the longevity and readability of your copy, consider the following maintenance tips:

- **Storage:** Store the book in a cool, dry place away from direct sunlight and excessive humidity to prevent paper degradation and cover warping.
- **Handling:** Handle with clean hands to avoid transferring oils and dirt to the pages. Avoid bending the spine excessively to preserve its integrity.

- **Protection:** If transporting, place the book in a protective bag or sleeve to prevent damage to the cover and pages.

10. Troubleshooting: Addressing Learning Challenges

Understanding advanced mathematical concepts can present challenges. Here are some strategies for troubleshooting common learning difficulties:

- **Revisit Foundations:** If a concept is unclear, review the preceding sections or chapters that introduce the foundational mathematical tools.
- **Consult External Resources:** While the book is self-contained, supplementary online resources, academic papers, or other textbooks can offer alternative perspectives or additional examples.
- **Collaborate:** Discuss challenging topics with peers or instructors. Explaining concepts to others or hearing different explanations can often clarify difficult points.
- **Practice Regularly:** Consistent engagement with the exercises is key. If stuck, try a similar problem or break down the problem into smaller, manageable steps.

11. Warranty and Support

As a textbook, this product typically does not come with a manufacturer's warranty in the traditional sense for electronic devices or appliances. For issues related to printing errors, binding defects, or missing pages, please contact the publisher, Springer, or the retailer from whom the book was purchased. Support for academic content is generally provided through educational institutions or direct communication with the authors via their academic affiliations.