**Springer ISBN-13: 978-1493939381**

# User Manual: An Introduction to Mathematical Cryptography

Model: ISBN-13: 978-1493939381 | Brand: Springer

## 1. Overview and Purpose

This manual provides guidance for engaging with "An Introduction to Mathematical Cryptography," Second Edition. This self-contained text introduces modern cryptography, focusing on the mathematical principles underpinning public key cryptosystems and digital signature schemes. It develops the necessary mathematical tools for constructing and analyzing diverse cryptosystems.

The book is designed for mathematics and computer science students seeking a foundation in the mathematics of modern cryptography. It covers classical constructions, fundamental mathematical tools, and advanced cryptographic innovations.

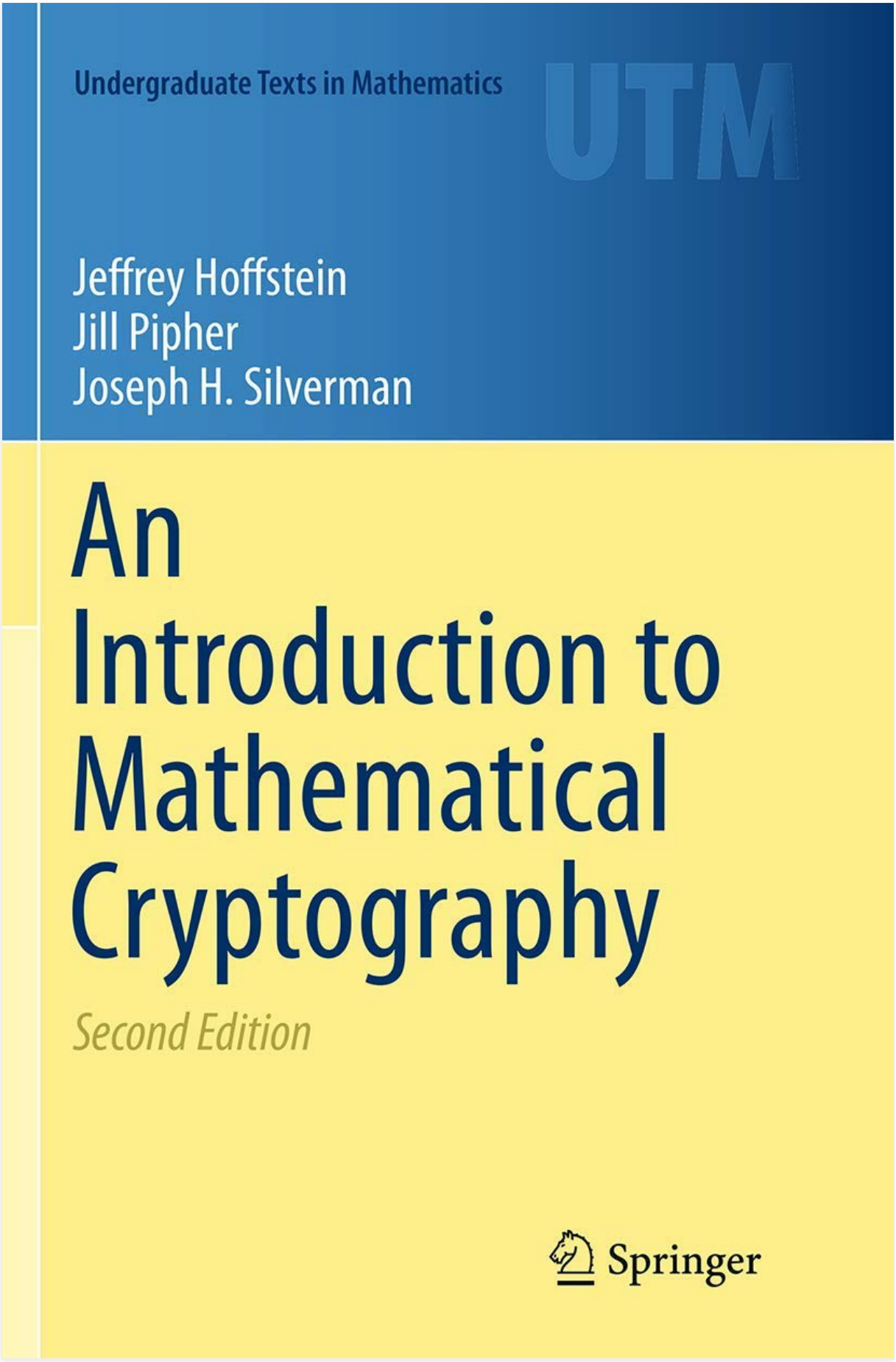


**Figure 1.1:** Front cover of "An Introduction to Mathematical Cryptography." The cover features the title, authors (Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman), and publisher (Springer), along with the series "Undergraduate Texts in Mathematics."

## 2. Prerequisites and Setup

To effectively utilize this textbook, a basic understanding of linear algebra is required. Techniques from algebra, number theory, and probability are introduced and developed within the text as needed.

### 2.1. Recommended Background

- **Basic Linear Algebra:** Familiarity with vector spaces, matrices, and linear transformations.
- **Mathematical Maturity:** An ability to understand and engage with mathematical proofs and abstract concepts.

### 2.2. Supplementary Materials

Supplementary materials, including an extensive bibliography and index, are available online. Refer to the publisher's website or the book's introductory sections for access details.

## 3. Engaging with the Content

The book is structured to guide the reader through various topics in mathematical cryptography.

### 3.1. Key Topics Covered

- **Classical Cryptographic Constructions:** Includes Diffie–Hellmann key exchange, discrete logarithm-based cryptosystems, RSA cryptosystem, and digital signatures.
- **Fundamental Mathematical Tools:** Covers primality testing, factorization algorithms, probability theory, information theory, and collision algorithms.
- **Advanced Cryptographic Innovations:** Explores elliptic curves, elliptic curve and pairing-based cryptography, lattices, lattice-based cryptography, and the NTRU cryptosystem.
- **Second Edition Revisions:** Significant revisions to digital signatures (earlier introduction to RSA, Elgamal, DSA), new material on lattice-based signatures and rejection sampling, expanded sections on information theory, elliptic curves, lattices, digital cash, and homomorphic encryption.

### 3.2. Exercises

Numerous exercises are included at the end of sections to reinforce understanding and provide practice. These exercises are designed to deepen comprehension of the material.

## 4. Care and Preservation

To ensure the longevity of your textbook, follow these general guidelines:

- Store the book in a cool, dry place away from direct sunlight and excessive humidity.
- Avoid bending the spine excessively to prevent damage to the binding.
- Keep the book away from liquids and food to prevent stains and damage.
- Handle pages carefully to avoid tearing or creasing.

## 5. Troubleshooting and Support

This section addresses common inquiries and challenges encountered while studying the material.

### 5.1. Difficulty Understanding Concepts

- **Review Prerequisites:** Ensure a solid understanding of basic linear algebra and mathematical

maturity.

- **Consult References:** The book includes an extensive bibliography. Utilize these resources for deeper dives into specific mathematical topics (e.g., algebra, number theory).
- **Work Through Examples:** The text provides numerous examples. Carefully follow the steps and reasoning presented.

### 5.2. Exercises and Solutions

The book includes exercises for practice. Please note that solutions to these exercises are generally not provided for individual purchasers. For academic settings, instructors may have access to solutions.

### 5.3. Cross-Referencing Issues

If you find it challenging to locate cross-referenced propositions or theorems, ensure you are referring to the correct chapter and section. The book's index can assist in navigating specific terms and concepts.

## 6. Product Specifications

| Attribute | Detail |
|---|---|
| **Title** | An Introduction to Mathematical Cryptography |
| **Authors** | Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman |
| **Publisher** | Springer |
| **Publication Date** | September 10, 2016 |
| **Edition** | Second Edition 2014 |
| **Language** | English |
| **Print Length** | 555 pages |
| **ISBN-10** | 1493939386 |
| **ISBN-13** | 978-1493939381 |
| **Item Weight** | 1.7 pounds |
| **Dimensions** | 6.1 x 1.26 x 9.25 inches |
| **Series** | Undergraduate Texts in Mathematics |

## 7. Publisher Information and Support

### 7.1. Publisher

This book is published by **Springer**.

### 7.2. Contact and Errata

For inquiries regarding the content, potential errata, or supplementary materials, please refer to the official Springer website or contact their customer support. Specific contact details may be found within the book's front matter or on the publisher's academic resources page.
**Visit Springer's Official Website**