Review of the book

"An Introduction to Mathematical Cryptography"

by Jeffrey Hoffstein, Jill Pipher and Joseph Silverman
Springer, 2008

ISBN: 978-0-387-77993-5

Edoardo Persichetti
University of Warsaw
March 2014

1 Summary of the review

In this review I present the book "An Introduction to Mathematical Cryptography" by Hoffstein, Pipher and Silverman. This volume provides a simple but detailed coverage of the most popular areas of modern cryptography, and the mathematics behind them.

2 Summary of the book

Modern-day cryptography has evolved in many interesting direction, a major breakthrough being the development of public-key cryptography. This particular branch is based on a variety of mathematical hard problems such as factoring, computing discrete logarithms, or finding short vectors in a lattice. In this book, the authors aim to provide an introduction to the subject, using a very simple approach and assuming almost no background.

3 Main Review

The volume is divided in eight chapters. Chapter 1 is an introduction to the subject, and begins with "historical" cryptographic concepts such as basic ciphers. The most elementary mathematical background tools are also presented here. These include simple notions of modular arithmetic, prime numbers and factoring, finite fields and so on. The chapter is concluded with a very interesting paragraph about cryptography before the computer age, and a paragraph presenting somewhat rigorous definitions of symmetric and asymmetric schemes.

The whole of Chapter 2 is dedicated to discrete logarithms and related cryptographic schemes. The chapter begins with a short introduction about the birth of public-key cryptography, and then presents the discrete logarithm problem (DLP). Subsequently, two of the most popular schemes based on discrete logarithms are described: the Diffie-Hellman key exchange and the El Gamal cryptosystem. Basic attacks on DLP-based schemes are also presented, such as the Baby Step-Giant Step algorithm and the Pohlig-Hellman method. General mathematical notions are included in this chapter as they will be needed in the rest of the book, namely the Chinese Remainder Theorem, and other notions regarding rings, quotients, polynomials and finite fields.

In a similar way, Chapter 3 is dedicated to integer factorization and RSA. The structure is similar to the previous chapter. First, there is an introductory paragraph featuring relevant mathematical notions, such as Euler's theorem. Then, the RSA encryption scheme is presented. Finally, several attacks on RSA are described. These are only attacks of mathematical nature, i.e. aimed at solving the (harder) factoring problem and independent of the cryptographic nature of RSA as a scheme. These include Pollard's $p-1$ algorithm, Dixon's random squares method, and an introduction to sieves: the quadratic sieve is described in detail while the complicated number field sieve is only hinted at. The chapter is concluded with a paragraph on quadratic residues, and a paragraph introducing probabilistic encryption via the Goldwasser-Micali cryptosystem.

Chapter 4 is an important chapter covering the fundamentals of probability and counting, areas that can't be ignored by anyone seriously interested in the study of cryptography. Besides several crucial probability notions, the chapter includes a description of cryptographic tools of probabilistic nature such as the Vigenere cipher and related cryptanalysis, and Pollard's ρ algorithm. In addition, we find here a paragraph dedicated to basic information theory and a paragraph on complexity theory.

Chapter 5 returns to the trend discussed before, this time with regard to elliptic curves. The vast theory of elliptic curves is greatly compressed and simplified in order to fit into a single chapter. The authors succeed in presenting an introduction to elliptic curves with a focus on applications in cryptography. Therefore, after the basic definitions, the reader is catapulted directly to cryptographic applications of elliptic curves such as elliptic Diffie-Hellman and El Gamal, and Lenstra's factorization algorithm. The chapter also features an interesting paragraph on the development of elliptic curve cryptography in recent times. The remainder of this chapter deals with more complicated objects such as elliptic curves over finite fields of characteristic 2, and pairings.

In Chapter 6, the authors considerably shift the focus, from cryptographic primitives based on "classical" number theory problems (such as DLP or factoring) to cryptographic primitives based on alternative hard problems. The chapter is in fact dedicated to lattices and their applications. The subset sum problem and knapsack cryptosystem are described carefully, introduced by a toy example. After a brief review of vector spaces, lattices are finally introduced,

together with the main problems connected to them, closest vector problem (CVP) and shortest vector problem (SVP), and algorithms for solving those, such as Babai's algorithm. The highlight of the chapter is the presentation of the NTRU encryption scheme, first from a general point of view, and then as a lattice-based cryptosystem. The chapter is concluded with a long and detailed presentation of the LLL lattice reduction algorithm.

Chapter 7 is orthogonal to all the previous chapters, as it focuses on a specific type of primitive, namely digital signatures, rather than the problem on which the primitive is based. Thus, after a short introduction presenting the basic definitions, we find descriptions of RSA signatures, DLP signatures, lattice-based signatures (GGH) and NTRU signatures. The ECDSA algorithm for signatures based on elliptic curves is relegated to the exercises section at the end of the chapter.

The last chapter, Chapter 8, is a "potluck" chapter that briefly presents a variety of additional topics that are fundamental for cryptographic purposes. These include hash functions, pseudorandom generators, zero-knowledge proofs, secret sharing schemes, identification schemes, a survey of the random oracle model and padding schemes, cryptographic protocols, hyperelliptic curves, quantum computing and modern-day symmetric schemes such as DES and AES.

4 Style of the book

The whole book is presented in a very simple fashion and descriptive style. Several extensive examples are provided along each notion, while proofs are often simplified, or just sketched (usually the most complicated ones).
Every chapter is correlated with a good number of exercises, ranging from simple calculations and revisitations of the examples, to more difficult proofs and some purely "descriptive" observations. All the exercises are conveniently divided and organized by the paragraph they refer to. Occasionally (see Chapter 7), these sections are used to cover additional material that was not presented in the main body of the chapter.

5 Would you recommend the book?

While not exactly rigorous, the book very is perfect for whoever is approaching cryptography with very little background. Explanations are easy to follow and the many examples and simplified language are of great help. I personally found it an excellent book and an invaluable tool for preparing my graduate cryptography course. I greatly recommend it.

The reviewer is Assistant Professor at University of Warsaw, Poland.