Review of the book

"Algorithmic Cryptanalysis" by Antoine Joux CRC Press, Taylor & Francis Group, 2009

ISBN: 978-1-4200-7002-6

Julia Borghoff
Technical University of Denmark

1 What the book is about

The book is divided into three parts: Background, Algorithms and Applications. The first part (Background) starts with a bird's-eye view of modern cryptography (Chapter 1). As the name suggests this chapter gives a very short introduction to concepts like symmetric and public key encryption, distinguishers and applications of cryptographic primitives such as signatures, MAC etc.

Chapter 2 (Elementary number theory and algebra background) gives a quick summary of the number theoretical and algebraic concepts which are needed in cryptography, such as GCD, modular arithmetic, univariate polynomials, finite fields and vector spaces. Also the first cryptosystems based on number theory are introduced: RSA and the Diffie-Hellman key exchange. Of particular interest for me was the mathematical description of an LFSR and the Berlekamp-Massey algorithm in Section 2.5. This chapter is very useful to refresh your knowledge especially because it comes with a pseudo code of many useful algorithms. However, if the reader is unfamiliar with these topics I would point him to more introductory books in this field because in my opinion the chapter is not meant for studying these topic for the first time as the description of the topics is very compact and lacks examples.

The second part of the book is called "Algorithms" and focuses on, as the name implies, algorithms and optimized implementations of those.

Chapter 3 (Linear Algebra) starts with a simple matrix multiplication as an introductory example. Step by step is explained how to achieve an optimized implementation in C with respect to running time and memory starting from the elementary matrix multiplication. This example points out nicely what a programmer has to consider when optimizing an implementation. It is followed by a section about dense matrix multiplication which focuses on Strassen's algorithm with a slightly too long performance analysis (for my taste), an explanation of the Gauss elimination and the difficulties that might occur while implementing it. The last section of this chapter treats sparse matrix operations which are due to the different way of storing the matrices quite different from dense matrix operations. Here, iterated approaches such as Wiedemann's and Lanczos's algorithm are introduce and different variants of structure Gauss elimination are sketched.

Chapter 4 (Sieve Algorithms) treats two topic: Sieving for primes and sieving for smooth composites. In the section about primes mainly Eratosthenes's sieve and different improvement of the naive implementation are considered. The drawback of this section is that either improvement is well described but a pseudo code or C code is missing as it is the case for the wheel or a full code is given (segmented sieve) which is hard to read because of the too short explanation and missing comments in the code. However, the section closes with the sieving algorithm of Atkin and Bernstein and gives therefore a nice overview of efficient sieving for primes. The second part of this chapter considers sieving for small numbers. In my opinion it is hard to follow the description of the different methods also because some of the terms e.g norm are not defined from the beginning.

Chapter 5 (Brute force cryptanalysis) starts with dictionary attacks as an introductory example where amongst other the difference between an online and an offline attack is explained. The next section focuses on DES and here especially on the different implementation for either fast encryption or a fast brute force search. The section ends with sketching the main ideas of a bit-sliced implementation. In the following section the collision search for SHA-0 is described from the linear model to a guided brute force over messages which gives the reader a very good impression how such an attack works.

The following three chapters are devoted to the birthday paradox. Chapter 6 (The birthday paradox: Sorting or not?) explains the birthday paradox on the example of the CBC mode. After analyzing the bounds of the birthday paradox the chapter continues with a discussion which is often omitted in other books. It answers the question of how to actually find a collision in a given set. In this section also a good overview over different sorting algorithms including their pros and cons is given and hash tables and binary trees are discussed. A broad answer is given and different solutions are offered to the question of how to find a collision in a given set. The chapter concludes with the Pohlig-Hellman algorithm for the discrete logarithm.

Chapter 7 (Birthday-based algorithms for functions) deals with the problem of reducing the memory requirements for algorithms that find collisions. If the sets, in which we search for a collision, can be generated by a recursive formula we can use cycle finding algorithms. Different algorithms such as Floyd's, Brent's and Nivasch's algorithms are introduced and compared. After general properties of random functions are discussed, concrete applications of these cycle finding algorithms are given: Pollard's rho factoring and discrete logarithms as number-theoretic examples and the block wise security of CBC mode as a cryptographic example. It is nice that here the example of Chapter 6 is picked up again which gives the reader a deeper understanding of the risk which CBC encryption might carry and emphasizes the strength and weaknesses of the different approaches. The next section considers collisions in hash function and focuses in particularly on the problem of how to parallelize collision search as cycle finding algorithms are sequential. The chapter concludes with Hellman's time memory trade off.

In Chapter 8 (Birthday attacks through quadrisection) algorithms with medium memory requirements are described. The main idea is to consider 4 lists instead of the 2 lists in the classical birthday problem. As an introductory example the knapsack problem together with an algorithm of Shamir and Schroeppel is described which is followed by several generalizations of the approach as well as a list of problems where no memory reduction is possible. Finally some applications are given such as the noisy CRT and plain variants of RSA and ElGamal.

In Chapter 9 (Fourier and Hadamard-Walsh transforms) first an algorithm for the Hadamard-Walsh transform is introduced and it is shown how it can be used to efficiently calculate linear and differential characteristics for an S-box. Also a comparison of the complexities between algorithms using the Hadamard-Walsh transform and classical algorithms for differential or linear characteristics is made. Amongst others a generalization of the Walsh transform to GF(p) is outlined. The chapter concludes with fast algorithms for the Fourier transform. While the section about the Fourier transform was quite clear for me I think the chapter lacks a clear definition of the Wash and Moebious transform in the first part of the section. Also the motivation for using these transformations could be stressed more in my opinion.

Chapter 10 (Lattice reduction) starts with a couple of definitions from lattice theory and continues with explaining lattice reduction in two dimensions before the lattice reduction algorithms for higher dimensions such as the LLL-algorithm are introduced. This first part is built up nicely and makes it easy to understand the lattice reduction in higher dimensions. In the next section the shortest vector problem and corresponding algorithms are discussed. The chapter concludes with the notions of dual and orthogonal lattices. The chapter gives a good summary of lattice reduction and nicely explains the mathematical ideas behind the algorithms, nevertheless, also practical issues like floating point vs rational representation of the number are addressed.

Chapter 11 (Polynomial systems and Gröbner base computations) deals with the problem of solving non-linear multivariate equation systems. The resultant method is introduced for the special case of bivariate systems and an extension to the general case is outlined. The main part of this chapter focuses on Gröbner bases, Buchberger's algorithm as well as F4 and F5 are discussed and the HFE cryptosystem completes the chapter as an example for the power of Gröbner bases in cryptography. The chapter gives a very nice overview over Gröbner bases, however, it is not meant to cover this very complex topic completely.

The third part of the book is called "Applications" and shows how the theory and algorithms we have seen in the chapters before are applied in cryptanalysis.

The main topic in Chapter 12 (Attacks on stream ciphers) are keystream generators based on LFSR with non-linear filter functions. The mainly considered attack type are correlation attacks which are based on the modeling of the keystream generator as a noisy binary channel. Furthermore, the extension of this attack to NFSR, algebraic attacks, cube attacks and time-memory trade-offs are examined.

In Chapter 13 (Lattice-based cryptanalysis) two main classes of lattice-based cryptanalysis are addressed: direct attacks, where the cryptanalytic problem can directly be expressed as a lattice reduction problem and Coppersmith's based attacks, which rely on several algorithms that can recover small roots of polynomial systems of equations using lattice reduction. The direct attacks focus on short dependence relations, applications are amongst others knapsack problems, finding minimal polynomials, NTRU lattices and Damgård's hash function. The section on Coppersmith's small roots attacks begins with introducing Howgrave-Graham's variant of the attack for univariate modular polynomials and continues with the Coppersmith's method for univariate and bivariate modular polynomials and an extension for finding rational roots. The chapter concludes with the application of Coppersmith's method on the security of RSA. I like this chapter because Coppersmith's method and it's application to RSA is rather new and cannot be found in many books.

Chapter 14 (Elliptic curves and pairings) focuses in the first part on the Weil pairing. The chapter is self-contained and starts therefore with an introduction to elliptic curves and gives important definitions in order to define the group structure of elliptic curves. All theorems stated in this part are proven using theory which has been introduced earlier in the book. The part concludes with Miller's algorithms for the Weil pairing. The second part of the chapter considers the elliptic curve factoring method (ECM) and points out the similarity between Pollard's $p-1$ factoring method and ECM.

Chapter 15 (Index calculus algorithms) is the last chapter of the book and it is devoted to the index calculus method. The method is introduced over finite fields, where the general description of the method is followed by a thorough analysis of the complexity and a toy example. Later also the regular function field sieve and the number field sieve are described. The book concludes with a section on smoothness probability for polynomials and integers.

2 What is this book about (summary)?

On the rear page of the book it says "Illustrating the power of algorithms, Algorithmic Cryptanalysis describes algorithmic methods with cryptographically relevant examples. Focusing on both private- and public-key cryptographic algorithms, it presents each algorithm either as a textual description, in pseudo-code, or in a C code program...". This is already a very good summary. The book clearly focuses on the algorithmic part of cryptanalysis and on efficient implementation. Therefore also topics are covered which are often omitted in other cryptography books such as sieving algorithms or algorithms that find a collision using the birthday paradox (such include sorting algorithms and cycle finding). Another example for the focus on the efficient implementation is the chapter about brute force search. The complexity of brute force in O-notation is well known, however when actually implementing it the algorithm can be sped up using different tricks.

The book is divided into three parts. The first part (Background) begins with a short introduction to cryptography and a background chapter on elementary number theory and algebra. The next part is called "Algorithms". Each chapter deals with a specific topic which is often illustrated with simple cryptographic applications. The part starts with a section on linear algebra with a focus on efficient implementations, continues with sieving algorithms, brute force cryptanalysis, followed by three chapter which are dedicated to the birthday paradox. The last three chapter of this part consider Fourier and Hadamard-Walsh transforms, lattice reduction and polynomial systems and Gröbner base computations. The last part is dedicated to applications. It starts with a chapter on attacks on LFSR-based stream ciphers, continues with lattice-based cryptanalysis and elliptic curves and pairing and finally concludes with a chapter on index calculus algorithms.

3 What is the book like (style)?

The author mentions in the preface that the idea of this book stemmed from a master's degree course given at the University of Versailles, where most students come from a mathematical background. Therefore the recapitulation of the mathematical concepts is kept quite short and sometimes even omitted. The mathematical basic are outside the scope of the book.

The book focuses on the algorithmic side of cryptanalysis. Therefore many (almost all) algorithms describe in the book are either given as pseudo code or C-program in the book. Longer programs can be found on the book's website. I personally missed comments in the code itself explaining the important steps of the algorithms.

Apart from that the book is mainly written as continuous text, which means that definition, theorems etc often are given within the text instead of stating them as a clear definition, theorem etc. (However there are some definition etc in the book). This is a matter of taste, many people prefer this writing style because it is easier to read a continuous text. However, I, as a mathematician, prefer the style "Motivation, Definition, Theorem, Proof, Explanation, Example", when possible. The drawback of a continuous text is clearly that it makes it difficult to go back and look up a definition etc.

At many points the author points out cryptanalytic problems to motivate or explain an approach/algorithm. This is very nice to see the connection between cryptography and the different algorithms. Unfortunately the book lacks more concrete examples in the book which would make it easier to understand a certain concept or definition (small examples containing concrete numbers, so that the reader can follow step by step what happens).

A convenient extra of the book are the good references. As the book tries to cover quite a large field, it is impossible to go into all details of the different topics. However, for each topic the reader can find several references in the book, which enable him/her to read more about the topic without having to do a literature search him/herself.

To sum this section up, even though the content of the book is quite interesting, it is not written in my preferred style but that is a matter of taste.

4 Would you recommend this book?

"Algorithmic Cryptanalysis" is a high level book that covers many interesting topics.

Yes, I would recommend this book for graduate students with a strong mathematical background, a cryptographic background, knowledge in C-programming and an interest in implementing cryptanalytic attacks. As mentioned before the book covers interesting topics when it comes to implementing an attack which I haven't seen in any other book before in this combination. However, the reader should be able to read pseudo and C-code without problems. Furthermore, the book contains just a short recap about the mathematical bases, so that it might be necessary for the reader to consult a corresponding mathematical textbook. Also a certain knowledge in cryptology is assumed.

I would not recommend the book for someone who is looking for an introduction to cryptanalysis because the book is not an introductory book to cryptography but requires a certain level of knowledge.

It is difficult to say if the book can serve as a self-study, here the missing examples are a drawback because it makes it hard for a student to check if he/she really understood the content. That could be fixed by making full solutions of the exercises available online.

The reviewer is a Ph.D. student in Symmetric Cryptology at the Department of Mathematics at the Technical University of Denmark.