Review of the book

"Algorithmic Cryptanalysis"

by Antoine Joux

CRC Press, Taylor & Francis Group, 2009

ISBN: 978-1-4200-7002-6

Joppe W. Bos
NXP Semiconductors

1 Summary of the review

As the title clearly indicates, this book is about *algorithmic cryptanalysis*. In an easy to follow manner this book outlines the various popular and efficient algorithms used to assess the security of the theoretic foundations in both symmetric and asymmetric cryptography. This book introduces the algorithms from an applied computational point of view; often accompanying the algorithms with C-code which implement these algorithms. This book can serve both as a course book for computer science or mathematic students with an interest in cryptanalysis but I would also highly recommended this as a reference work for any professional who has to deal cryptanalytic algorithms.

2 Summary of the book

This book consists of fifteen chapters divided over three parts.

① **Background.** The first two chapters serve as the required background. The first chapter is concerned with how security is defined in cryptography while the second chapter recalls the required elementary number theory to understand the remainder of the book. Joux introduces the reader in an easy-to-follow manner to the greatest common divisor (including its variants), modular arithmetic, the concept of finite fields, vector spaces, and the RSA and Diffie-Hellman cryptosystems.

② **Algorithms.** The second and main part of the book consists of nine chapters. With these nine chapters Joux manages to cover an impressive range of different algorithms which are commonly used to cryptanalyze commonly-used problems. Algorithms to target both problems in symmetric and asymmetric cryptography are presented. The topics range from brute-force type of algorithms to algorithms which use the birthday paradox to sieve algorithms to lattice reductions to Gröbner base computations. All these topics are interesting research areas by themselves and the topics are well-explained. The presented algorithms are always presented with pseudo-code or working C-code such that the applied cryptanalyst can immediately get a feeling how the presented approached are computed in practice.

③ **Applications.** The third part of the book consists of four chapters. In this part the applications of the previously described algorithms are described. The four areas of focus are attacks on stream ciphers, lattice based cryptography, elliptic curve and pairings and various index calculus algorithms.

Every chapter ends with a list of interesting and challenging exercises. Unfortunately, no solutions are provided in the book. Some basic hints are provided on the website of the book for the exercises marked with an "h" but I hope full solutions will appear in the (near) future.

3 What is the book like (style)?

The book is very well-written and easy to follow. The required theoretical results are stated in the form of theorems, next the implications of these results are explained in more detail which eases the understanding of these results. Besides the motivation behind the algorithms also a (very helpful) run-time analysis is performed such that the reader gets a good feeling for why these algorithms are efficient.

4 Would you recommend this book?

Yes, I would highly recommend this book to (under)graduate students with an interest in cryptanalysis. Furthermore, every cryptographer who is thinking about designing new cryptographic algorithms should be familiar with the appropriate chapters from this book in order to be aware of the state-of-the-art in cryptanalysis. For the professional cryptologists this book is a perfect reference work to check the specific (run-time) details and background of the various popular techniques and algorithms used in cryptanalysis.

The reviewer is a cryptographic researcher at NXP Semiconductors, Leuven, Belgium