Review of the book

"Number Theory and Cryptography"

by J. H. Loxton

Cambridge University Press, 1990

ISBN: 978-0-521-39877-0

Constantinos Patsakis
Research fellow
Distributed Systems Group
School of Computer Science and Statistics
Trinity College

1 Summary of the review

The book is a selection of papers from a wide variety of topics in Cryptography and Number Theory, presented at the 33rd Annual Meeting of the Australian Mathematical Society and at the Workshop on Number Theory and Cryptography in Telecommunications in 1989. The book is composed of three parts that focus on a range of topics such as stream ciphers, applications of cryptography, number theory, integer factorization algorithms and authentication mechanisms, to name a few.

2 Summary of the book

The book consists of three parts. The first part is dedicated to the number theoretic aspects of Cryptology. A wide range of topics, from integer factorization algorithms and Quadratic fields, to number sieves and continued fractions are being discussed.

The first paper offers an insight on the advances of that period in Cryptography with number theoretic tools. More precisely it presents the Weiner attack for RSA with short private exponent, an alternative to the classical Diffie-Hellman key distribution scheme by McCurley and the connection between linear complexity profiles and continued fraction expansions.

The second paper, discusses how quadratic fields can be used in Cryptography. After a short introduction to quadratic fields, the authors illustrate a problem in quadratic fields that can be used for creating one-way functions. Moreover, a key exchange system based on quadratic fields and a Public encryption scheme are being described, proving that quadratic fields can be a very useful tool in Cryptography. The authors finish with several very good remarks and questions for future work.

Given the fact that nowadays we have multicore CPUs and GPUs in our computers, the next paper is quite important, because it contains a very good analysis of the most well-known integer factorization algorithms, specially, the ones that can be parallelized, like Pollard's "rho" and "p-1" algorithms, ECM and quadratic sieve.

The forth paper is a very good introduction to sieving. From its roots to the implementation of OASiS (Open Architecture Sieve System), the authors illustrate the needs, the problems and their solutions. Apart from the theoretical results, the authors give a very good description of Lehmer's bicycle chain and photoelectric sieves. It is worth going through the specs of OASiS and its architecture, to appreciate the results that people got from such machines at that time.

The following paper is illustrating several algorithms, deterministic and probabilistic in finite fields. Some of these algorithms are still being used today, with several modifications. Their scope is for testing whether a polynomial is irreducible in a finite field, or find its factorization.

The last paper of the first part focuses on continued fractions. The reader may consider that the notes will be aiming for the continued fraction factorization method, after all continued fractions are mostly used for integer factorization. However, the author shows the connection between them and recurrence sequences and uses this connection to show that encryption schemes based on non-linear combinations of recurrence sequences can be cryptanalyzed.
The second part consists of 9 papers which focus on cryptographic devices and applications of cryptography.
The first paper of this part clearly shows the big boom of the Internet in the 90's, note that the paper was published in 1990. The paper tries to summarize the methods that are going to be used in securing communications the next decade, however the whole new world of Internet/WWW even as words are missing. The general ideas of the paper might seemed good, X.509 can be found as a recommendation quite interestingly, yet the technological advances and the growth of telecommunications in that decade were so quick and to that extend, that couldn't be guessed by anyone, set aside their security aspects.
The second paper gives an introduction, of the well-known linear feedback shift registers (LFSRs) and stream ciphers, describing their structure, their properties and their applications.
The third paper illustrates several results on randomness tests to block ciphers, more precisely, FEAL 4 and 8 and Madryga. The tests that are applied here are a prelude to the upcoming Marsaglia's diehard tests and NIST's statistical test suite.
The following paper describes an application of Reed-Muller codes to creating pseudo-random sequences with the use of structured noise. However, as the authors note, despite the nice properties that the generators might have, they are not secure to be used for stream ciphers and should only be used as an efficient alternative to applications where security is not needed, eg simulations.
The next paper, examines the security and privacy issues of a MACNET, a shared fiber access network and how they can be treated with several cryptographic methods.
The sixth paper of this part provides a gentle introduction to authentication mechanisms, based on cryptographic methods.
After several attempts to "fix" the knapsack-based cryptosystems the system has been proved to be insecure. In the seventh paper, the author presents the encryption scheme, the method to break it and a very good example, discussing all the needed steps and how to circumvent several difficulties when implementing the attack.
The eighth paper of the second part proposes three solutions to the tactical frequency management problem. Apart from a known manual solution, the author presents two novel methods, one using heuristic search and one using simulated annealing.
The last paper of this part is rather a note on Reed-Salomon codes and how they can be extended to complex fields.
The last part of the book deals with problems mainly in Diophantine Analysis and normal numbers.
The first paper of this part, deals with several results on a very well-known problem by Gauss, the class problem. The authors focus on real quadratic fields, providing several good criteria and interesting results.
The second paper is providing solutions to four number theoretic problems, mainly on normal numbers. Quite delicate proofs for some hard mathematical problems, which involve multiplicative independent integers.
Since normality is a very good statistical property of the digits of real numbers, the third paper of this part is focused on providing sever results for a special class of normal numbers.
The following paper is a note containing several theorems on normal numbers that can be used in order to construct new normal numbers, from existing ones.
The fifth paper deals a set of famous mathematical equations, Thue equations and connects them with multiplicatively independent numbers. This work, for specific cases of Thue equations, provides several bounds on their solutions. However, the provided bounds, improve previous results for with the same assumptions.
The sixth paper of the third part provides an Dyson-type crank based on 24-coloured partitions. The core of the problem is highly connected to several problems in string theory, more precisely, to its roots with open bosonic strings.
The last paper of the book provides an overview on how to determine a special class of universal abelian varieties, the Mordell-Weil groups. The not only tries to illustrate most important results on this area,

but tries to illustrate the techniques that are being used in proofs as well. Therefore, provides the reader a more solid overview of the theory and how it can be used.

3 What is the book like (style)?

Since the book is a collection of papers from a workshop and a meeting, it deals with several topics, which has a very bad impact to its homogeneity. The same applies to the depth of several articles as well. For example, some go too deep and some are very shallow, some of them are just notes, on a very specific topic, or some of them provide a now deprecated view of security in telecommunications. Moreover, some articles are too general, like stream ciphers and LFSRs. Given the variety of good books nowadays in cryptography, I can hardly think of someone getting this book today to learn about integer factorization, LFSRs or even authentication mechanisms.
Since the book is on number theory and cryptography, as the title says, one would imagine a more-applied-to-cryptography version, however this is not the case. Of course one could find links between normal numbers and pseudo-random generators, yet the authors clearly do not have such intensions, as it is clear that these papers were from the mathematical society meeting.

4 Would you recommend this book?

The audience of this book is academia and researchers and I can say that I hardly know many people that I would recommend this book. The main reason is that you will end up getting this book only if you need a very-very specific result. Since it was published in the 90s several ideas have been surpassed, or when it comes to its introductory articles, modern textbooks in cryptography can provide better information by far, in terms of comprehension, depth, examples and illustration.

The reviewer is a post-doc research fellow at the Distributed Systems Group, School of Computer Science and Statistics, Trinity College, Dublin, Ireland