Review of the book

"Understanding and Applying Cryptography and Data Security"

by Adam J. Elbirt

Taylor & Francis, 2009

ISBN-13: 978-1-4200-6160-4

Olivier Blazy
ENS/CNRS/INRIA, France

2009-11-01

1 What the book is about

As explains the author, Adam J. Elbirt, this book aims to describe cryptography and data security from the "How do I implement the algorithm" point of view. At the first glance the idea seems really good, it can help understand another side of Cryptography which might be forgotten when working only on theoretical experiments.

The author tries to give a large overview of the field of Cryptology, or at least Cryptography.

- He begins with a short history to show where and why cryptography is needed in our modern world.
- Then he focuses on Symmetric-Key Cryptography, reexplaining the basic notions used (modulo, gcd, $\mathbb{Z}_p$, ...), introducing the different kind of ciphers (substitution, stream, block) with different examples of real-world application (LSFR, DES, triple DES, AES, and some classical attacks.
- Later in the book, he speaks about Public-Key Cryptography, introducing its purpose, the concept of One-Way Functions, while explaining how RSA works he reminds some notions in arithmetic (Chinese reminder theorem, Karatsuba Multiplication Algorithm...). He also try to emphasize Cryptography based on the discrete logarithms problem and later on based on Elliptic Curves.
- The last two sections are wider. The first one presents signatures, hash functions and MAC, each time with some concrete examples and some characteristic about the

actual efficient implementations. The last one is about protocols and tries to briefly summarize how a PKE works and gives some examples like PGP and SSL.

2 What the book is like

When looking at the table of content of the book you can see that the author want to cover a large area of the field while keeping some organization. This way, you might use the book as a handbook where you'll find quickly the precise information you were looking for. The style is quite pleasant, with few embellishment without being excessively compact.

The book is divided into main sections each around a global theme (Symmetric Cryptography, Public-Key, ...), and each of them follow the same organization.

First you begin with mathematical basis. In this part the author explains how the different fundamental tools work. there you can find several examples here to strengthen the different notions shown. Most of the time they are really well chosen, however some of them are not always progressive enough or may even comport mistakes, like the one explaining how to use the DES S-Boxes ...

Then the author speaks about real and practical implementation of those concept, as the book is here to help people with implementation you can find examples in assembly, C, VHDL and Verilog throughout the sections, and you can also find a lot of figures; as for everything, some is a good idea, but too much ruins the whole thing, and at the end you may end up totally skipping them; some of them are simple and help but on the other hand some are just unnecessary and might frighten the reader. ...

At the end of the different sections, you can also find several homework, which are quite progressive and, are effective to help understanding the notions previously explained... Last exercises always ask to implement things or to understand examples in C or hardware description languages. It really helps to feel the complexity of some basic crypto problems and feel the time needed by some computation ...

One also has to mention the very detailed references given by the author during each chapter. The final bibliography comports more than 300 references showing the work accomplished by the author to let his book have a real scientific background.

3 Recommendation

Actually I don't really know to whom I'd recommend this book. From a mathematical point of view, you really start from scratch as the author explains everything and details (too much) his numerical examples. (The worst is a 11 pages numerical example in the elliptic curves chapter ..., to stress the problem, I'm not sure that half way through the books, you really need 5 steps to compute $7(7-2)-9 \mod 11$....)

However teaching cryptography was not the original purpose of the book, it was made to explain how to implement things and which actual implementation may be chosen in a specific case. And I think that this goal is achieved. I can't say you don't need any

programming background, because implementation performance tables are given with very few information. But at least you will be able to find the information you were looking for but maybe not fully understanding what it exactly does which may seem kinda dangeourous in term of security...

I do believe that students may benefit from this book however. It's easy to read, and you have many references if you need precise and detailed information.

In a general point of view, the book is interesting, but some examples, parts might have been skipped or drasticaly shortened in order to make it more attractive, because there are many very nice explanations and they are quite hidden by the rest.

The reviewer is a Ph.D. student at the Ecole Normale Supérieure, Paris, France.