Information Security and Cryptography

More information about this series at http://www.springer.com/series/4752

Nigel P. Smart

Cryptography Made Simple

Springer

Nigel P. Smart
University of Bristol
Bristol, UK

ISSN 1619-7100 ISSN 2197-845X (electronic)
Information Security and Cryptography
ISBN 978-3-319-21935-6 ISBN 978-3-319-21936-3 (eBook)
DOI 10.1007/978-3-319-21936-3

Library of Congress Control Number: 2015955608

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

This is a reworking of my earlier book "Cryptography: An Introduction" which has been available online for over a decade. In the intervening years there have been major advances and changes in the subject which have led me to revisit much of the material in this book. In the main the book remains the same, in that it tries to present a non-rigorous treatment of modern cryptography, which is itself a highly rigorous area of computer science/mathematics. Thus the book acts as a stepping stone between more "traditional" courses which are taught to undergraduates around the world, and the more advanced rigorous courses taught in graduate school.

The motivation for such a bridging book is that, in my view, the traditional courses (which deal with basic RSA encryption and signatures, and perhaps AES) are not a suitable starting point. They do not emphasize the importance of what it means for a system to be secure; and are often introduced into a curriculum as a means of demonstrating the applicability of mathematical theory as opposed to developing the material as a subject in its own right. However, most undergraduates could not cope with a full-on rigorous treatment from the start. After all one first needs to get a grasp of basic ideas before one can start building up a theoretical edifice.

The main differences between this version and the Third Edition of "Cryptography: An Introduction" is in the ordering of material. Now security definitions are made central to the discussion of modern cryptography, and all discussions of attacks and weaknesses are related back to these definitions. We have found this to be a good way of presenting the material over the last few years in Bristol; hence the reordering. In addition many topics have been updated, and explanations improved. I have also made a number of the diagrams more pleasing to the eye.

Cryptography courses are now taught at all major universities; sometimes these are taught in the context of a Mathematics degree, sometimes in the context of a Computer Science degree, and sometimes in the context of an Electrical Engineering degree. Indeed, a single course often needs to meet the requirements of all three types of students, plus maybe some from other subjects who are taking the course as an "open unit". The backgrounds and needs of these students are different; some will require a quick overview of the algorithms currently in use, whilst others will want an introduction to current research directions. Hence, there seems to be a need for a textbook which starts from a low level and builds confidence in students until they are able to read the texts mentioned at the end of this Preface.

The background I assume is what one could expect of a third or fourth year undergraduate in computer science. One can assume that such students have already met the basics of discrete mathematics (modular arithmetic) and a little probability. In addition, they will have at some point done (but probably forgotten) elementary calculus. Not that one needs calculus for cryptography, but the ability to happily deal with equations and symbols is certainly helpful. Apart from that I introduce everything needed from scratch. For those students who wish to dig into the mathematics a little more, or who need some further reading, I have provided an appendix which covers most of the basic algebra and notation needed to cope with modern cryptosystems.

It is quite common for computer science courses not to include much of complexity theory or formal methods. Many such courses are based more on software engineering and applications of computer science to areas such as graphics, vision or artificial intelligence. The main goal of such courses is to train students for the workplace rather than to delve into the theoretical aspects of

the subject. Hence, I have introduced what parts of theoretical computer science I need, as and when required.

I am not mathematically rigorous at all steps, given the target audience, but aim to give a flavour of the mathematics involved. For example I often only give proof outlines, or may not worry about the success probabilities of many of the reductions. I try to give enough of the gory details to demonstrate why a protocol or primitive has been designed in a certain way. Readers wishing for a more in-depth study of the various points covered or a more mathematically rigorous coverage should consult one of the textbooks or papers in the Further Reading sections at the end of each chapter.

On the other hand we use the terminology of groups and finite fields from the outset. This is for two reasons. Firstly, it equips students with the vocabulary to read the latest research papers, and hence enables students to carry on their studies at the research level. Secondly, students who do not progress to study cryptography at the postgraduate level will find that to understand practical issues in the "real world", such as API descriptions and standards documents, a knowledge of this terminology is crucial. We have taken this approach with our students in Bristol, who do not have any prior exposure to this form of mathematics, and find that it works well as long as abstract terminology is introduced alongside real-world concrete examples and motivation.

I have always found that when reading protocols and systems for the first time the hardest part is to work out what is public information and which information one is trying to keep private. This is particularly true when one meets a public key encryption algorithm for the first time, or one is deciphering a substitution cipher. Hence I have continued with the colour coding from the earlier book. Generally speaking items in red are secret and should never be divulged to anyone. Items in blue are public information and are known to everyone, or are known to the party one is currently pretending to be.

For example, suppose one is trying to break a system and recover some secret message m; suppose the attacker computes some quantity b. Here the red refers to the quantity the attacker does not know and blue refers to the quantity the attacker does know. If one is then able to write down, after some algebra,

$$b = \cdots = m,$$

then it is clear something is wrong with our cryptosystem. The attacker has found out something he should not. This colour coding will be used at all places where it adds something to the discussion. In other situations, where the context is clear or all data is meant to be secret, I do not bother with the colours.

To aid self-study each chapter is structured as follows:

- A list of items the chapter will cover, so you know what you will be told about.
- The actual chapter contents.
- A summary of what the chapter contains. This will be in the form of revision notes: if you wish to commit anything to memory it should be these facts.
- Further Reading. Each chapter contains a list of a few books or papers from which further information can be obtained. Such pointers are mainly to material which you should be able to tackle given that you have read the prior chapter.

There are no references made to other work in this book; it is a textbook and I did not want to break the flow with references to this, that and the other. Therefore, you should not assume that ANY of the results in this book are my own; in fact NONE are my own. Those who wish to obtain pointers to the literature should consult one of the books mentioned in the Further Reading sections.

The book is clearly too large for a single course on cryptography; this gives the instructor using the book a large range of possible threads through the topics. For a traditional cryptography course within a Mathematics department I would recommend Chapters 1, 2, 3, 7, 11, 12, 13, 14, 15, 16

and 17. For a course in a Computer Science department I would recommend Chapters 1, 11, 12, 13, 14, 15 and 16, followed by a selection from 18, 19, 20, 21 and 22. In any course I *strongly* recommend the material in Chapter 11 should be covered. This is to enable students to progress to further study, or to be able to deal with the notions which occur when using cryptography in the real world. The other chapters in this book provide additional supplementary material on historical matters, implementation aspects, or act as introductions to topics found in the recent literature.

Special thanks go to the following people (whether academics, students or industrialists) for providing input over the years on the various versions of the material: Nils Anderson, Endre Bangerter, Guy Barwell, David Bernhard, Dan Bernstein, Ian Blake, Colin Boyd, Sergiu Bursuc, Jiun-Ming Chen, Joan Daemen, Ivan Damgård, Gareth Davies, Reza Rezaeian Farashahi, Ed Geraghty, Florian Hess, Nick Howgrave-Graham, Ellen Jochemsz, Thomas Johansson, Georgios Kafanas, Parimal Kumar, Jake Longo Galea, Eugene Luks, Vadim Lyubashevsky, David McCann, Bruce McIntosh, John Malone-Lee, Wenbo Mao, Dan Martin, John Merriman, Phong Nguyen, Emmanuela Orsini, Dan Page, Christopher Peikert, Joop van de Pol, David Rankin, Vincent Rijmen, Ron Rivest, Michal Rybar, Berry Schoenmakers, Tom Shrimpton, Martijn Stam, Ryan Stanley, Damien Stehle, Edlyn Teske, Susan Thomson, Frederik Vercauteren, Bogdan Warinschi, Carolyn Whitnall, Steve Williams and Marcin Wójcik.

Nigel Smart
University of Bristol

Further Reading

After finishing this book if you want to know more technical details then I would suggest the following books:

A.J. Menezes, P. van Oorschot and S.A. Vanstone. *The Handbook of Applied Cryptography.* CRC Press, 1997.

J. Katz and Y. Lindell. *Introduction to Modern Cryptography: Principles and Protocols.* CRC Press, 2007.

Contents