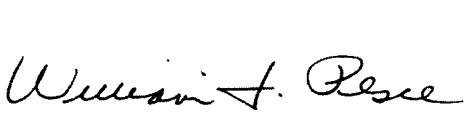
APPLIED CRYPTANALYSIS

THE WILEY BICENTENNIAL–KNOWLEDGE FOR GENERATIONS

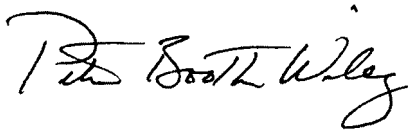
Each generation has its unique needs and aspirations. When Charles Wiley first opened his small printing shop in lower Manhattan in 1807, it was a generation of boundless potential searching for an identity. And we were there, helping to define a new American literary tradition. Over half a century later, in the midst of the Second Industrial Revolution, it was a generation focused on building the future. Once again, we were there, supplying the critical scientific, technical, and engineering knowledge that helped frame the world. Throughout the 20th Century, and into the new millennium, nations began to reach out beyond their own borders and a new international community was born. Wiley was there, expanding its operations around the world to enable a global exchange of ideas, opinions, and know-how.

For 200 years, Wiley has been an integral part of each generation's journey, enabling the flow of information and understanding necessary to meet their needs and fulfill their aspirations. Today, bold new technologies are changing the way we live and learn. Wiley will be there, providing you the must-have knowledge you need to imagine new worlds, new possibilities, and new opportunities.

Generations come and go, but you can always count on Wiley to provide you the knowledge you need, when and where you need it!



WILLIAM J. PESCE
PRESIDENT AND CHIEF EXECUTIVE OFFICER



PETER BOOTH WILEY
CHAIRMAN OF THE BOARD

APPLIED CRYPTANALYSIS

Breaking Ciphers in the Real World

Mark Stamp
Richard M. Low

San Jose State University
San Jose, CA

WILEY-INTERSCIENCE
A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Stamp, Mark.
Applied cryptanalysis : breaking ciphers in the real world / Mark Stamp, Richard M. Low.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-11486-5 (pbk.)
1. Computer security. 2. Data encryption (Computer science) 3. Cryptography. I. Low, Richard M., 1967– II. Title.
QA76.9.A25S687 2007
005.8'2—dc22 2007001277

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

To Melody, Austin, and Miles — MSS

To Amy — RML

This Page Intentionally Left Blank

Contents

This Page Intentionally Left Blank

Preface

To paraphrase Barbie, "cryptanalysis is hard" [6]. Unfortunately, many cryptanalysis papers seem to be written in their own impenetrable secret code, making the subject appear to be even more difficult than it really is.

In this book, we strive to present applied cryptanalytic attacks in an accessible form. Here, we are focused on practical attacks that actually break real-world systems, not attacks that merely indicate some theoretical weakness in a cipher. Consequently, we consider real ciphers and, primarily, modern ciphers. Many attacks that satisfy our criteria are scattered throughout the literature.[1] With a few notable exceptions, these papers require a Herculean effort to digest and understand. One of our goals is to lift this unintentional veil on the exciting and fascinating field of cryptanalysis.

Most of the topics presented in this book require only a modest mathematical background. Some of the public key topics are inherently more mathematical, but in every case we have strived to minimize the advanced mathematics. We also believe that we have provided enough background information so that the book is essentially self-contained. Some of the more advanced mathematical topics are treated briefly in the Appendix. Any motivated upper-division undergraduate student—in any technical field of study—should be able to tackle this book. Some of the material is not easy, but those who persist will be rewarded with a solid understanding of cryptanalysis, as well as the knowledge, tools, and experience to confidently explore cutting-edge cryptanalytic topics.

We have provided an extensive set of problems for each chapter. A few of these problems are relatively easy, but most range from moderate to somewhat challenging. Generally, we have tried to avoid obvious problems of the "implement such-and-such attack" variety. Of course, it is useful and instructive to implement an attack, but the problems are intended to reinforce and expand on material presented in the text, without placing an overwhelming burden on the reader. A fairly complete solutions manual is available to instructors directly from your Wiley representative.

[1] A large percentage of the cryptanalysis literature is informal in the sense that many papers never receive any formal peer review. Although the academic peer-review process suffers from a multitude of sins, no peer review is no better.

To really understand the material in this book, it is necessary to work a significant number of the problems. Cryptanalysis is definitely not a spectator sport. We believe that the computer is an essential cryptanalytic tool. It is not coincidental that many of the homework problems require some computer programming.

For the terminally cryptanalytically insane, we have created a collection of challenge problems. These problems, which are posted on the textbook website at

`http://cs.sjsu.edu/faculty/stamp/crypto/`

consist primarily of cryptanalytic challenges based on the ciphers and attacks presented in the text. A few research-oriented problems are also included. Each problem carries a difficulty rating so that you will have some idea of what you might be getting into. For each challenge problem, a small prize[2] is offered to the first solver. We promise to update the website as the challenge problems are solved. The website includes source code and test vectors for many of the ciphers discussed here. In addition, a complete set of quality PowerPoint slides is available.

The text is organized around four major themes, namely, classic ciphers (Chapters 1 and 2), symmetric ciphers (Chapters 3 and 4), hash functions (Chapter 5), and public key crypto (Chapters 6 and 7). The specific topics covered in each chapter are summarized below:

Chapter	Topics
1. Classic Ciphers	Pen-and-paper systems
2. World War II Ciphers	Enigma, Purple, Sigaba
3. Stream Ciphers	Shift registers, correlation attacks, ORYX, RC4, PKZIP
4. Block Ciphers	Block cipher modes, MAC, Hellman's TMTO, CMEA, Akelarre, FEAL
5. Hash Functions	HMAC, birthday attacks, Nostrasamus attack, MD4, MD5
6. Public Key Systems	Knapsack, Diffie-Hellman, Arithmetica, RSA Rabin, NTRU, ElGamal
7. Public Key Attacks	Factoring, discrete log, RSA timing attacks, RSA glitching attack

[2]The emphasis here is on "small."

The first author wrote Chapters 2 through 5 and 7, while the second author wrote the majority of Chapters 1 and 6. The first author extensively edited all chapters to give the book a more consistent "look and feel." The first author did his best to resist including too many bad jokes, but some proved irresistible. Most of these have, mercifully, been relegated to footnotes.

The majority of the book consists of a series of cryptanalytic vignettes, organized by topic. Chapters 3, 4, and 5 each begin with a relatively generic method of attack (correlation attacks, Hellman's TMTO and birthday attacks, respectively). These attacks are interesting in their own right, but each also serves as an introduction to the type of cipher under consideration. Each of these chapters then segues into the cryptanalysis of specific ciphers.

For public key crypto, the introductory material has been expanded to an entire chapter. In Chapter 6, several public key systems are introduced and discussed from the perspective of relatively straightforward attacks or implementation issues that can lead to weaknesses. Then selected public key attacks are covered in depth in Chapter 7.

The chapters are highly independent of each other, as are many of the sections within chapters. The most dependent chapters are 6 and 7, which cover public key crypto. In addition, some familiarity with hashing (Chapter 5) would be useful before diving into the public key material. The terminology and background covered in Chapter 1 is used throughout the text. Regardless of your background in cryptography, we recommend that you read Chapter 1 first, since terminology is not consistent throughout the crypto world. Not only is crypto terminology inconsistent, but notation is even worse. Notationwise, we have tried to be as internally consistent as possible. Consequently, our notation often differs from the original source.

The first author's information security textbook [142] covers four major topics, one of which is cryptography. The only significant overlap between [142] and this book is Hellman's time-memory trade-off attack, discussed here in Section 4.4. A brief section on the knapsack attack is also included in both books; here, in Section 6.2.

Finally, we apologize in advance for the inevitable "bugs" in this book. Any computer program of sufficient size has bugs and it is more difficult to debug a textbook than a program, since there is at least some hope of getting a program to misbehave during testing. There is no method to "exercise" a textbook other than to proofread it and to teach from it—the more times the better. The first author has taught virtually all of the material in this text, and several careful proofreadings have been done. Nevertheless, it is a sure bet that errors remain. Please tell us of any bugs you find. We would also appreciate any other comments you have regarding this book.

Mark Stamp
Richard M. Low
San Jose State University

This Page Intentionally Left Blank

About the Authors

Mark Stamp has an extensive background in information security in general and cryptography in particular, having spent more than seven years as a Cryptologic Mathematician at the National Security Agency. His other relevant experience includes two years as Chief Cryptologic Scientist at a small Silicon Valley startup company. Since the demise of his startup company in 2002, he has been a faculty member in the department of computer science at San Jose State University, where he primarily teaches courses in information security. In 2005, Dr. Stamp published his first textbook, *Information Security: Principles and Practice* (Wiley Interscience).

Richard M. Low has a PhD in mathematics and is a faculty member in the department of mathematics at San Jose State University. His research interests include cryptography, combinatorics and group theory. In addition to teaching mathematics, he has conducted a popular cryptography seminar at SJSU.

Acknowledgments

I want to thank the following San Jose State University students who contributed significantly to the indicated sections: Heather Kwong (Enigma); Thang Dao (Purple); Wing On Chan and Ethan Le (Sigaba); Thuy Nguyenphuc (ORYX); Bevan Jones and Daniel Tu (Akelarre); Tom Austin, Ying Zhang, and Narayana Kashyap (MD5); Ramya Venkataramu (RSA timing attack); Natalia Khuri (RSA); Edward Yin (Chapter 2 solutions).

As always, thanks to my PhD advisor, Clyde F. Martin. Clyde is the one who introduced me to cryptography.

Richard Low deserves credit for enthusiastically signing on to this project and for convincing me to persevere at a couple of points where I was ready to throw in the towel. He also tolerated my occasional rants very well.

A very special thanks to Wan-Teh Chang for his careful reading of most sections of this book. Wan-Teh has an excellent eye for detail and he provided numerous corrections and useful suggestions.

Thanks are due to all of the people at Wiley who were involved with this book. In particular, I want to thank Paul Petralia, Whitney A. Lesch, and Kellsee Chu who were extremely helpful throughout.

Last but certainly not least, thanks to my lovely wife, Melody, and my two boys, Austin and Miles, for their patience during the seemingly endless hours I spent working on this project.

— MSS

My love of mathematics was cultivated by many of my former math teachers (from junior high school to graduate school). Those that come particularly to mind include: Joseph Buckley, Gary Chartrand, Daniel Goldston, Doug Harik, Philip Hsieh, Sin-Min Lee, John Martino, John Mitchem, Thomas Richardson, Gerhard Ringel, Jerome Schroeder, Michael Slack, Arthur Stoddart, Sandra Swanson, Arthur White, Gregg Whitnah, and Kung-Wei Yang. Thank you for showing me the way.

— RML