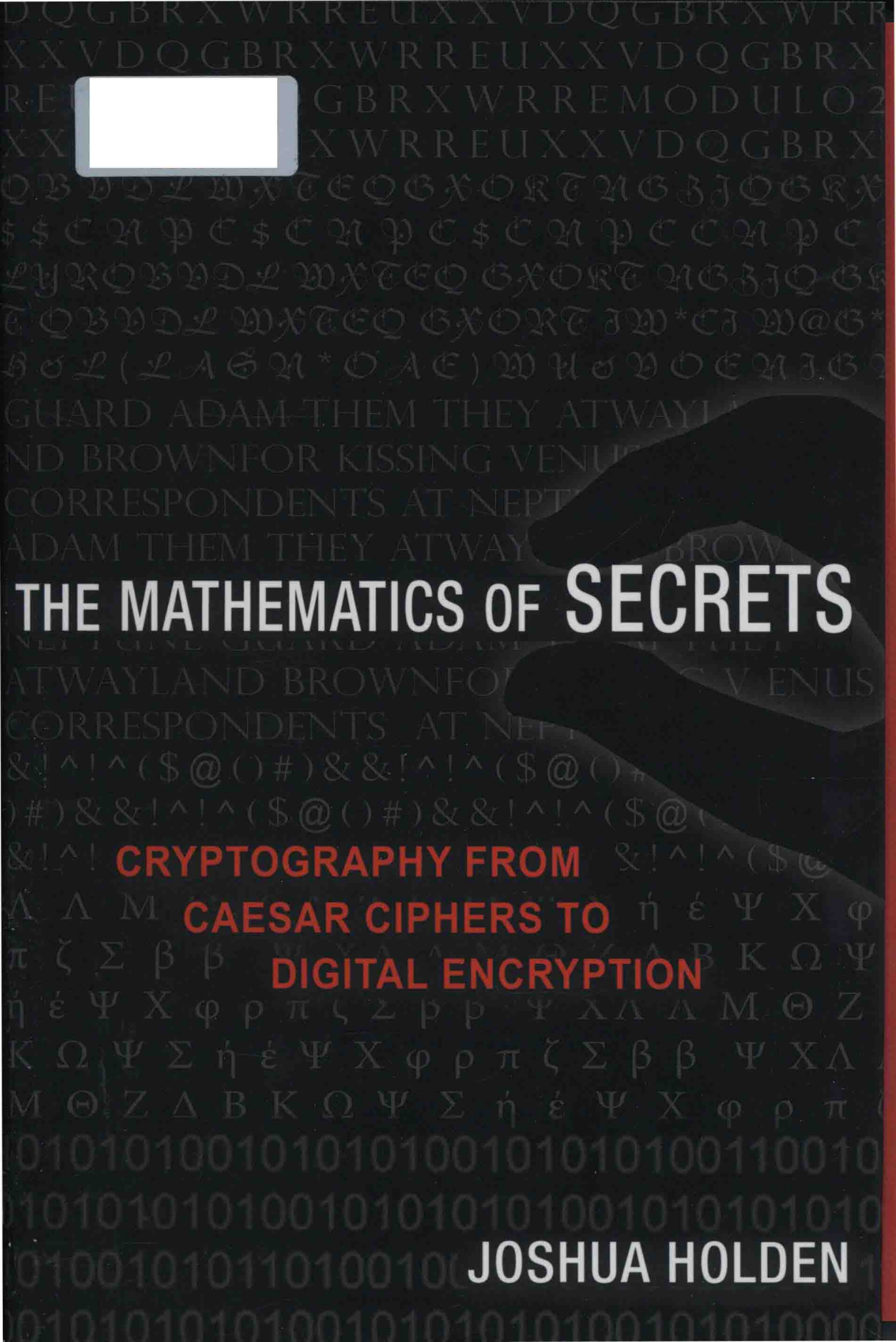
THE MATHEMATICS OF SECRETS
CRYPTOGRAPHY FROM CAESAR CIPHERS TO DIGITAL ENCRYPTION
JOSHUA HOLDEN

# THE MATHEMATICS OF SECRETS

## CRYPTOGRAPHY FROM CAESAR CIPHERS TO DIGITAL ENCRYPTION

■ ■ ■

JOSHUA HOLDEN

■ ■ ■

PRINCETON UNIVERSITY PRESS
PRINCETON AND OXFORD

Published by Princeton University Press, 41 William Street,
Princeton, New Jersey 08540
In the United Kingdom: Princeton University Press, 6 Oxford
Street, Woodstock, Oxfordshire OX20 1TR

press.princeton.edu

Jacket image courtesy of Shutterstock; design by Lorraine Betz Doneker



Library of Congress Cataloging-in-Publication Data

Names: Holden, Joshua, 1970– author.
Title: The mathematics of secrets : cryptography from Caesar
ciphers to digital encryption / Joshua Holden.
Description: Princeton : Princeton University Press, [2017] |
Includes bibliographical references and index.
Identifiers: LCCN 2016014840 | ISBN 9780691141756
(hardcover : alk. paper)
Subjects: LCSH: Cryptography—Mathematics. | Ciphers. |
Computer security.
Classification: LCC Z103 .H664 2017 | DDC 005.8/2—dc23 LC
record available at https://lccn.loc.gov/2016014840

British Library Cataloging-in-Publication Data is available

This book has been composed in Linux Libertine
Printed on acid-free paper. ∞

Printed in the United States of America

1 3 5 7 9 10 8 6 4 2

# THE MATHEMATICS OF SECRETS

*To Lana and Richard for their love and support*

# ■ ■ ■ PREFACE ■ ■ ■

This book is about the mathematics behind the modern science of sending secret messages, or cryptography. Modern cryptography *is* a science, and like all modern science, it relies on mathematics. Without the mathematics, you can only go so far in understanding cryptography. I want you to be able to go farther, not only because I think you should know about cryptography, but also because I think the particular kinds of mathematics the cryptographers use are really pretty, and I want to introduce you to them.

In *A Brief History of Time*, Stephen Hawking says that someone told him that each equation he included in the book would halve the sales. I hope that's not true of this book, because there are lots of equations. But I don't think the math is necessarily that hard. I once taught a class on cryptography in which I said that the prerequisite was high school algebra. Probably I should have said that the prerequisite was high school algebra and a willingness to think really hard about it. There's no trigonometry here, no calculus, no differential equations. There are some ideas that don't usually come up in an algebra course, and I'll try to walk you through them. If you want to really understand these ideas, you can do it without any previous college-level math—but you might have to think hard. (The math in some of the sidebars is a little harder, but you can skip those and still understand the rest of the book just fine.)

Mathematics isn't all there is to cryptography. Unlike most sciences, cryptography is about intelligent adversaries who are actively fighting over whether secrets will be revealed. Ian Cassels, who was both a prominent mathematician at Cambridge and a former British cryptanalyst from World War II, had a good perspective on this. He said that "cryptography is a mixture of mathematics and muddle, and without the muddle the mathematics can be used against you." In this book I've removed some of the muddle in order to focus on the mathematics. Some

professional cryptographers may take issue with that, because I am not really showing you the most secure systems that I could. In response, I can say only that this book for those interested in learning about a particular part of cryptography, namely, the mathematical foundations. There are many additional books in *Suggestions for Further Reading* and the Bibliography that you should read if you want to become a well-rounded professional.

Here is where I have drawn my personal line: I have tried not to say anything false in this book in the name of simplification, but I have left things out. I have left out some details of how to use the systems most securely, and I have left out some systems that I don't feel contribute to the mathematical story I want to tell. When possible, I have tried to present systems that have actually been used to protect real secrets. However, I have included some that were made up by me or another academic type when I feel that they best illustrate a point.

Computer technology has changed both the types of data with which cryptographers work and the techniques that are feasible. Some of the systems for protecting data that I discuss are either no longer applicable or no longer secure in today's world, even if they were in the past. Likewise, some of the techniques I discuss for breaking these systems are no longer effective in the forms presented here. Despite this, I feel that all the topics in this book illustrate issues that are still important and relevant to modern cryptography. I have tried to indicate how the principles are still used today, even when the actual systems are not. "Looking Forward" at the end of each chapter gives you a preview of how the chapter you just finished relates to the chapters yet to come or to future developments that I think are possible or likely.

A lot of the chapters follow the historical development of their topic, because that development is often a logical progression through the ideas I'm describing. History is also a good way to tell a story, so I like to use it when it fits. There's lots more about the history of cryptography out there, so if you would like to know more, definitely check out *Suggestions for Further Reading.*

I tell my students that I became a math professor because I like math and I like to talk. This book is me talking to you about a particular application of mathematics that I really like. My hope is that by the end of the book, you will really like it too.

# ■ ■ ■ ACKNOWLEDGMENTS ■ ■ ■

I wish I could individually thank everyone with whom I have ever had a good conversation about math or cryptography, but obviously I can't. I do want to single out some of the people who have particularly helped with my teaching of cryptography: by letting me sit in on their classes, by encouraging me, by teaching with me, or by sharing relevant materials. In roughly chronological order, these include David Hayes, Susan Landau (from whom I learned the "cosmic ray" principle, among many other cryptographic things), Richard Hain, Stephen Greenfield, Gary Sherman (from whom I learned the "shoes and socks" principle), and David Mutchler. I apologize if I've left anyone out.

Thank you to all the attendees of the Algorithmic Number Theory Symposia, particularly Carl Pomerance, Jon Sorenson, Hugh Williams, and all the members of Hugh's "posse" at (or formerly at) the University of Calgary. I'd also like to thank Brian Winkel, Craig Bauer, and the present and past members of the Editorial Board of *Cryptologia*. Without the friendship and encouragement of all of you, I'm sure my cryptography research would never have gotten off of the ground. And thanks go to all my research students at Rose-Hulman and at the Rose-Hulman Summer Research Experience for Undergraduates, who gave me the best reason to keep my research going.

This book has been in progress for a long time and many people have reviewed various drafts of it over the years. Many of you I don't know personally, and I don't even know some of your names, but thank you to all of you. Two people I particularly would like to thank are Jean Donaldson and Jon Sorenson. Jean volunteered to read a very early draft despite my being unable to offer any personal or professional incentive whatsoever. Not being a professional mathematician or cryptographer, she was the perfect audience and everything she said was immensely useful. Jon Sorenson likewise read an early draft and made encouraging

and helpful comments. In addition to being a reviewer, Jon has been a colleague and a friend for many years and has helped my career in numerous ways. Paul Nahin, David Kahn, and John MacCormick are also among those who gave me encouraging and helpful reviews.

The staff at Rose-Hulman's Logan Library have been invaluable through this process. Amy Harshbarger has come up with articles and technical reports through Interlibrary Loan that I thought would never be found. And Jan Jerrell let me keep library books far beyond the limits of a reasonable circulation policy. I thank them both, and everyone else at the library, profusely. Speaking of the library, Heather Chenette and Michelle Marincel Payne helped organize the "Shut Up and Write" group that met there and got me through the final revisions.

I could not have done this without the support and tolerance of my wife, Lana, our housemate, Richard, and the cats, who "tolerated" the occasional late dinner. You've put up with a lot through this process. I really appreciate it.

Finally, thank you to everyone at Princeton University Press, especially my editor, Vickie Kearn. Vickie first approached me about writing a cryptography book 12 years ago, and in all that time she never lost faith that it would happen some day. I can't believe it's finally finished. Thanks so much.

# THE MATHEMATICS OF SECRETS

# ■ ■ ■ CONTENTS ■ ■ ■