MATHEMATICAL WORLD • VOLUME 25

MATHEMATICAL CIPHERS

from Caesar to RSA

Anne L. Young

AMS
AMERICAN MATHEMATICAL SOCIETY

http://dx.doi.org/10.1090/mawrld/025

MATHEMATICAL WORLD • VOLUME 25

MATHEMATICAL CIPHERS

from Caesar to RSA

Anne L. Young

AMS
American Mathematical Society
www.ams.org

2000 *Mathematics Subject Classification.* Primary 11-01, 11T71, 94-01, 94A60.

For additional information and updates on this book, visit
www.ams.org/bookpages/mawrld-25

Library of Congress Cataloging-in-Publication Data

Young, Anne L., 1946–
Mathematical ciphers : from Caesar to RSA / Anne L. Young.
p. cm. — (Mathematical world, ISSN 1055-9426 ; v. 25)
Includes bibliographical references and index.
ISBN-13: 978-0821-3730-6
1. Ciphers. 2. Cryptography. 3. Number theory. I. Title. II. Series.

Z104.Y68 2006
652′.8–dc22 2006042991

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to `reprint-permission@ams.org`.

© 2006 by the American Mathematical Society. All rights reserved.
The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 11 10 09 08 07 06

To my husband, David

This page intentionally left blank

Contents

Preface		vii
Chapter 1.	Introduction	1
Chapter 2.	Caesar Cipher	3
Chapter 3.	Terminology and Results from Number Theory	9
Chapter 4.	Modular Arithmetic	17
Chapter 5.	Describing the Caesar Cipher Mathematically	27
Chapter 6.	Cryptanalysis for the Caesar Cipher	31
Chapter 7.	Multiplication Cipher	37
Chapter 8.	Cryptanalysis for the Multiplication Cipher	47
Chapter 9.	Multiplication-Shift Cipher	51
Chapter 10.	Cryptanalysis for the Multiplication-Shift Cipher	59
Chapter 11.	Non-Mathematical Substitution Ciphers	69
Chapter 12.	Preparing to Generalize	75
Chapter 13.	Finding Inverses Modulo n	81
Chapter 14.	General Multiplication-Shift Cipher	89
Chapter 15.	Security of the General Multiplication-Shift Cipher	93
Chapter 16.	Introduction to the Exponential Cipher	103
Chapter 17.	Deciphering the Exponential Cipher	111
Chapter 18.	Cryptanalysis for the Exponential Cipher	119
Chapter 19.	Mathematical Basis for the Exponential Cipher	123
Chapter 20.	Public Key Ciphers	127
Chapter 21.	RSA Cipher	131

Chapter 22. Signatures 133

Chapter 23. Security and Implementation of the RSA Cipher 143

Chapter 24. Computer Programs 149

Chapter 25. Further Reading 151

Chapter 26. Answers to Selected Exercises 153

Index 157

Preface

A cipher is a scheme for creating coded messages. The purpose of using a cipher is to exchange information securely. Throughout history, many different coding schemes have been devised. Those discussed in this book have a mathematical basis. One of the oldest and simplest mathematical systems was used by Julius Caesar. This is where we will begin our study. Building on that simple system, we will then consider more complicated schemes, ultimately ending with the RSA cipher, which is used to provide security for the Internet. In addition to developing various encryption schemes and the underlying mathematics, this book has several other goals. One is to introduce the reader to number theory, the area of mathematics that concerns integers and their properties. Consequently, some mathematical concepts are presented in greater detail than is needed to understand and implement a cipher. In addition, proofs of some theorems are included for those readers who are interested in learning more about this aspect of mathematics.

The book is structured differently from most mathematics texts. It does not begin with a mathematical topic, but rather with a cipher. The mathematics is developed only as it is needed; the applications motivate the mathematics. The following conventions are used throughout. The first time that a term is introduced, it appears in *italic* type and the sentence or paragraph in which it appears contains the definition of the term. Messages, plain or coded, are written in capital letters in a special font. For example, `EXAMPLE` and `TBQDHST`. Occasionally, equations or phrases containing symbols are set off from the body of the text. When it is necessary to refer to these statements later in the chapter, they are numbered consecutively within the chapter. For example, if we were considering the equation

$$x + 5 = 11, \tag{1}$$

we might say "solving for x in (1) gives $x = 6$." It is traditional in mathematics to mark the end of examples and proofs with a special symbol. In this text, these are indicated by $\bullet$.

As is typical in mathematics textbooks, most chapters end with exercises. Many of these problems are similar to solved examples and are designed to assist the reader in mastering the basic material. Answers to these routine problems are contained in Chapter 26. A few of the exercises are one-of-a-kind, intended to challenge the interested reader.

Implementing encryption schemes is considerably easier with the use of the computer. There are JavaScript programs, which are available from the webpage for this book and run on the user's computer, for all the ciphers introduced in this book. Information about these programs is contained in Chapter 24.

This book is based on materials that I use in my course, Topics in Modern Math: Ciphers and Codes, at Loyola College in Maryland. The course, which has no prerequisites, satisfies Loyola's core mathematical sciences requirement and is taken primarily by humanities majors. The course was originally developed in the early 1990s with the support of a Loyola College Summer Teaching Grant and was significantly enhanced by a year-long College sabbatical in 1998–99. I am grateful for that support. Each time I have taught the course, I have found ways to improve the course materials using comments and suggestions from my students. It was their voices that I heard in the background and which I have tried to keep in mind as I prepared this book.

I am thankful to many people who have contributed to my development as a teacher of mathematics. I have been fortunate to have spent my career at two institutions that value teaching, Hamilton College and Loyola College in Maryland. I have learned much from my departmental colleagues at both institutions. Sadly, two of the most influential colleagues, John T. Anderson and George Mackiw, are no longer living; both were broadly-read mathematicians who cared deeply about their students. It was Gordon Pritchett who first taught me how to write mathematics.

Several people played significant roles in the development of this book and I am grateful to them. John Hennessey first suggested the basic approach to the course, that the "story line comes first," preceding the mathematics. Erica Flappan, one of my first students at Hamilton and now a published author herself, encouraged me to submit my materials for publication. David Haddad supported adding this project to my administrative responsibilities. Edward Dunne, Editor for the Book Program at the American Mathematical Society, made many valuable suggestions as well as provided general encouragement. Emilie Kulis read the entire manuscript, worked the exercises, checked the computer programs, made many excellent suggestions for improvement, and assisted me in so many other ways, going well beyond her responsibilities as my executive administrative assistant. I could not have completed the project on time without her help. Finally, my wonderful husband David gave me his unwavering support and encouragement all along the way, as he always does.

If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

A cipher is a scheme for creating coded messages for the secure exchange of information. Throughout history, many different coding schemes have been devised. One of the oldest and simplest mathematical systems was used by Julius Caesar. This is where *Mathematical Ciphers* begins. Building on that simple system, Young moves on to more complicated schemes, ultimately ending with the RSA cipher, which is used to provide security for the Internet.

Photo by Bob Stockfield, courtesy of Loyola College

This book is structured differently from most mathematics texts. It does not begin with a mathematical topic, but rather with a cipher. The mathematics is developed as it is needed; the applications motivate the mathematics. As is typical in mathematics textbooks, most chapters end with exercises. Many of these problems are similar to solved examples and are designed to assist the reader in mastering the basic material. A few of the exercises are one-of-a-kind, intended to challenge the interested reader.

Implementing encryption schemes is considerably easier with the use of the computer. For all the ciphers introduced in this book, JavaScript programs are available from the Web.

In addition to developing various encryption schemes, this book also introduces the reader to number theory. Here, the study of integers and their properties is placed in the exciting and modern context of cryptology. *Mathematical Ciphers* can be used as a textbook for an introductory course in mathematics for all majors. The only prerequisite is high school mathematics.

ISBN 0-8218-3730-3

9 780821 837306

MAWRLD/25

For additional information and updates on this book, visit

www.ams.org/bookpages/mawrld-25

AMS on the Web
www.ams.org