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.