
The Cryptoclub

Using Mathematics to Make and Break Secret Codes



Janet Beissinger
Vera Pless

Daria Tsoupikova, Artist



A K Peters
Wellesley, Massachusetts

Foreword

The Cryptoclub is a wonderful introduction to cryptography for middle-school students. As a research mathematician with a long-standing interest in this subject, I am very favorably impressed by the accuracy, clarity, and relevance of the material presented. I believe that this book offers a great opportunity to introduce students to applications of mathematics that are both exciting and also play a major if sometimes hidden role in our daily activities. Encryption of information is used not only by students and governments to keep communications secret but also by banks and other businesses to secure sensitive information. With the growing number of transactions taking place over the Internet, cryptography is of ever-increasing importance.

Many people have the mistaken impression that mathematics is a static subject, one in which everything has been known for hundreds of years. Cryptography acts as a window to the open questions and evolving nature of mathematics and, in particular, to number theory, often considered an amusing playground for mathematicians with little relevance to the real world. In this book, we are shown why this view now has been completely reversed.

By incorporating various mathematical skills (factoring, exponentiation, modular arithmetic, etc.) and using them in a concrete way, the authors motivate students; by testing the efficiency of different encryption techniques, they stimulate critical algorithmic thinking and a sense of practicality. I believe that by telling a continuous story, the authors are able to engage the students and keep their interest throughout the entire project.

This book will without a doubt be a very attractive addition to the curriculum for middle-school students.

It certainly would have benefited me when I was in middle school.

Ronald L. Graham

University of California at San Diego