# A CLASSICAL INTRODUCTION TO CRYPTOGRAPHY EXERCISE BOOK

# A CLASSICAL INTRODUCTION TO CRYPTOGRAPHY EXERCISE BOOK

by

**Thomas Baignères**
*EPFL, Switzerland*

**Pascal Junod**
*EPFL, Switzerland*

**Yi Lu**
*EPFL, Switzerland*

**Jean Monnerat**
*EPFL, Switzerland*

**Serge Vaudenay**
*EPFL, Switzerland*

Springer

Thomas Baignères
EPFL - I&C - LASEC
Lausanne, Switzerland

Pascal Junod
Lausanne, Switzerland

Yi Lu
EPFL - I&C - LASEC
Lausanne, Switzerland

Jean Monnerat
EPFL-I&C-LASEC
Lausanne, Switzerland

Serge Vaudenay
Lausanne, Switzerland

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

A CLASSICAL INTRODUCTION TO CRYPTOGRAPHY EXERCISE BOOK
by Thomas Baignères, Palcal Junod, Yi Lu, Jean Monnerat and Serge Vaudenay

ISBN-10: 0-387-27934-2 e-ISBN-10: 0-387-28835-X
ISBN-13: 978-0-387-27934-3 e-ISBN-13: 978-0-387-28835-2

Printed on acid-free paper.



Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11514411, 11552901

springeronline.com

*To Valérie and my parents*

*To Mimi and Chloé*

*To my parents*

*To Susan and my parents*

*To Christine and Emilien*

# Contents

# Foreword

As a companion book of Vaudenay's *A Classical Introduction to Cryptography*, this exercise book contains a carefully revised version of most of the material used in teaching by the authors or given as examinations to the undergraduate students of the *Cryptography and Security* lecture at EPFL from 2000 to mid-2005. It covers a majority of the subjects that make up today's cryptology, such as symmetric or public-key cryptography, cryptographic protocols, design, cryptanalysis, and implementation of cryptosystems.

Exercises do not require a large background in mathematics, since the most important notions are introduced and discussed in many of the exercises. We expect the readers to be comfortable with basic facts of discrete probability theory, discrete mathematics, calculus, algebra, as well as computer science. Following *A Classical Introduction to Cryptography*, exercises related to the more advanced parts of the textbook are marked with a star.

The difficulty of the exercises covers a broad spectrum. In some the student is expected to simply apply basic facts, while in others more intuition and reflexion will be necessary to find the solution. Nevertheless, the solutions accompanying the exercises have been written as clearly as possible. Some exercises are clearly research-oriented, like for instance the ones dedicated to decorrelation theory or to very recent results in the field of hash functions. The idea was to give to our readers a taste of this exciting research world.

Chapter 1 is dedicated to the prehistory of cryptology, exposing the design and the cryptanalysis of very simple and/or historical ciphers. Chapter 2 investigates basic facts of modern symmetric cryptography, focusing on the Data Encryption Standard, modes of operations, and stream ciphers. Chapter 3 handles the hash functions topic, while Chapter 4 describes some more involved notions of cryptanalysis of block ci-

phers. Chapter 5 considers protocols based on symmetric cryptography. Chapter 6 is based on some basic facts of algebra and on the algorithms used to compute within the usual algebraic structures used in cryptology, while Chapter 7 is devoted to number theory with a strong emphasis put on its algorithmic aspects. Chapter 8 is built around some elements of complexity theory. Chapter 9 treats the important subject of public-key encryption schemes and Chapter 10 contains exercises centered around the notion of digital signatures. Chapter 11 exposes some protocols using public-key cryptography, and Chapter 12 handles the case of hybrid protocols, combining both symmetric and public-key schemes.

A website (`http://www.intro-to-crypto.info`) has been set up as a companion of this book. It will contain inevitable errata as well as other material related to this book, like challenging tests and more exercises.

Finally, the authors would like to thank Gildas Avoine, Matthieu Finiasz, and all the EPFL students who attended at least one of our lectures, as well as the Springer-Verlag staff for having provided us so many useful comments on these exercises, their solutions, and on the textbook.

We wish the reader a wonderful trip in the exciting world of cryptology!