

**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, Pascal 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.

© 2006 Springer Science+Business Media, Inc.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, Inc., 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America.

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

[springeronline.com](http://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	xiii
1. PREHISTORY OF CRYPTOGRAPHY	1
Exercises	1
Exercise 1	Mappings, etc. 1
Exercise 2	A Simple Substitution Cryptogram 4
Exercise 3	Product of Vigenère Ciphers 5
Exercise 4	★One-Time Pad 5
Exercise 5	★Latin Squares 6
Exercise 6	Enigma 6
Solutions	8
2. CONVENTIONAL CRYPTOGRAPHY	17
Exercises	17
Exercise 1	Weak Keys of DES 17
Exercise 2	Semi-Weak Keys of DES 17
Exercise 3	Complementation Property of DES 17
Exercise 4	3DES Exhaustive Search 18
Exercise 5	2DES and Two-Key 3DES 18
Exercise 6	★Exhaustive Search on 3DES 19
Exercise 7	An Extension of DES to 128-bit Blocks 20
Exercise 8	Attack Against the OFB Mode 21
Exercise 9	★Linear Feedback Shift Registers 22
Exercise 10	★Attacks on Cascade Ciphers 23
Exercise 11	Attacks on Encryption Modes I 24
Exercise 12	Attacks on Encryption Modes II 28
Exercise 13	★A Variant of A5/1 I 29

Exercise 14	★A Variant of A5/1 II	31
Exercise 15	★Memoryless Exhaustive Search	32
Solutions		34
3. DEDICATED CONVENTIONAL CRYPTOGRAPHIC PRIMITIVES		57
Exercises		57
Exercise 1	Collisions in CBC Mode	57
Exercise 2	Collisions	57
Exercise 3	Expected Number of Collisions	58
Exercise 4	Multicollisions on Hash Functions	58
Exercise 5	Weak Hash Function Designs	60
Exercise 6	Collisions on a Modified MD5	62
Exercise 7	First Preimage on a Modified MD5	62
Exercise 8	★Attacks on Yi-Lam Hash Function	62
Exercise 9	MAC from Block Ciphers	63
Exercise 10	CFB-MAC	64
Exercise 11	★Universal Hashing	64
Solutions		66
4. CONVENTIONAL SECURITY ANALYSIS		81
Exercises		81
Exercise 1	The SAFER Permutation	81
Exercise 2	★Linear Cryptanalysis	81
Exercise 3	★Differential and Linear Probabilities	82
Exercise 4	★Feistel Schemes	82
Exercise 5	★Impossible Differentials	84
Exercise 6	★Attacks Using Impossible Differential	84
Exercise 7	★Multipermutations	86
Exercise 8	★Orthomorphisms	87
Exercise 9	★Decorrelation	88
Exercise 10	★Decorrelation and Differential Cryptanalysis	89
Exercise 11	★Decorrelation of a Feistel Cipher	89
Exercise 12	★A Saturation Attack against IDEA	89
Exercise 13	★Fault Attack against a Block Cipher	94
Solutions		97

5. SECURITY PROTOCOLS WITH CONVENTIONAL CRYPTOGRAPHY	125
Exercises	125
Exercise 1   Flipping a Coin by Email	125
Exercise 2   Woo-Lam Protocol	126
Exercise 3   MicroMint I	127
Exercise 4   MicroMint II	127
Exercise 5   Bluetooth Pairing Protocol	128
Exercise 6   UNIX Passwords	128
Exercise 7   Key Enlargement	128
Solutions	130
6. ALGORITHMIC ALGEBRA	135
Exercises	135
Exercise 1   Captain's Age	135
Exercise 2   Roots in $\mathbf{Z}_{77}^*$	135
Exercise 3   ★When is $\mathbf{Z}_n^*$ Cyclic?	135
Exercise 4   Finite Fields and AES	137
Exercise 5   ★A Special Discrete Logarithm	138
Exercise 6   ★Quadratic Residues	138
Exercise 7   ★Cubic Residues	139
Exercise 8   ★Generating Generators for $\mathbf{Z}_p^*$	139
Exercise 9   ★Elliptic Curves and Finite Fields I	140
Exercise 10  ★Elliptic Curves and Finite Fields II	141
Solutions	142
7. ALGORITHMIC NUMBER THEORY	159
Exercises	159
Exercise 1   ★Rho Method and Distinguished Points	159
Exercise 2   ★Factorization	160
Exercise 3   ★Prime Numbers	161
Exercise 4   ★Factoring $n = p \cdot q$	161
Exercise 5   Strong Prime Numbers	161
Exercise 6   Complexity of Eratosthenes Sieve	161
Exercise 7   ★Hash Function Based on Arithmetics	164
Solutions	165

8. ELEMENTS OF COMPLEXITY THEORY	175
Exercises	175
Exercise 1   ★Regular Language	175
Exercise 2   ★Finite State Automaton	175
Exercise 3   ★Turing Machine	175
Exercise 4   ★Graph Colorability I	176
Exercise 5   ★Graph Colorability II	176
Solutions	177
9. PUBLIC KEY CRYPTOGRAPHY	181
Exercises	181
Exercise 1   ★Okamoto-Uchiyama Cryptosystem	181
Exercise 2   RSA Cryptosystem	182
Exercise 3   RSA for Paranoids	182
Exercise 4   RSA - Common Moduli	183
Exercise 5   Networked RSA	183
Exercise 6   Repeated RSA Encryption	184
Exercise 7   Modified Diffie-Hellman	184
Exercise 8   ★Rabin Cryptosystem	184
Exercise 9   ★Paillier Cryptosystem	185
Exercise 10  ★Naccache-Stern Cryptosystem	186
Solutions	188
10. DIGITAL SIGNATURES	199
Exercises	199
Exercise 1   Lazy DSS	199
Exercise 2   ★DSS Security Hypothesis	199
Exercise 3   DSS with Unprotected Parameters	200
Exercise 4   Ong-Schnorr-Shamir Signature	201
Exercise 5   Batch Verification of DSS Signatures	201
Exercise 6   Ring Signatures	203
Solutions	205
11. CRYPTOGRAPHIC PROTOCOLS	211
Exercises	211
Exercise 1   Breaking the RDSA Identification Scheme	211
Exercise 2   ★A Blind Signature Protocol for a Variant of DSA	213



<i>Contents</i>		xi
Exercise 3	★Fiat-Shamir Signature I	215
Exercise 4	★Fiat-Shamir Signature II	216
Exercise 5	★Authenticated Diffie-Hellman Key Agreement Protocol	216
Exercise 6	Conference Key Distribution System	217
Solutions		220
12. FROM CRYPTOGRAPHY TO COMMUNICATION SECURITY		231
Exercises		231
Exercise 1	A Hybrid Cryptosystem Using RSA and DES	231
Exercise 2	SSL/TLS Cryptography	233
Exercise 3	Secure Shell (SSH)	235
Exercise 4	Attack against RC5-CBC-PAD	236
Exercise 5	Wired Equivalent Privacy (WEP)	237
Exercise 6	Forging X.509 Certificates	238
Solutions		240
References		249

# 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!