Complexity and Cryptography
An Introduction

Cryptography plays a crucial role in many aspects of today's world, from internet banking and ecommerce to email and web-based business processes. Understanding the principles on which it is based is an important topic that requires a knowledge of both computational complexity and a range of topics in pure mathematics. This book provides that knowledge, combining an informal style with rigorous proofs of the key results to give an accessible introduction. It comes with plenty of examples and exercises (many with hints and solutions), and is based on a highly successful course developed and taught over many years to undergraduate and graduate students in mathematics and computer science.

The opening chapters are a basic introduction to the theory of algorithms: fundamental topics such as NP-completeness, Cook's theorem, the P vs. NP question, probabilistic computation and primality testing give a taste of the beauty and diversity of the subject. After briefly considering symmetric cryptography and perfect secrecy, the authors introduce public key cryptosystems. The mathematics required to explain how these work and why or why not they might be secure is presented as and when required, though appendices contain supplementary material to fill any gaps in the reader's background. Standard topics, such as the RSA and ElGamal cryptosystems, are treated. More recent ideas, such as probabilistic cryptosystems (and the pseudorandom generators on which they are based), digital signatures, key establishment and identification schemes are also covered.

JOHN TALBOT has been a lecturer in mathematics, University College London since 2003. Before that he was GCHQ Research Fellow in Oxford.

DOMINIC WELSH is a fellow of Merton College, Oxford where he was Professor of Mathematics. He has held numerous visiting positions including the John von Neumann Professor, University of Bonn. This is his fifth book.

Complexity and Cryptography

An Introduction

JOHN TALBOT
DOMINIC WELSH

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521852319

First published 2006

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

ISBN-13 978-0-521-85231-9 hardback
ISBN-10 0-521-85231-5 hardback

ISBN-13 978-0-521-61771-0 paperback
ISBN-10 0-521-61771-5 paperback

Contents

Preface *page* ix
Notation xi

1 Basics of cryptography 1
1.1 Cryptographic models 2
1.2 A basic scenario: cryptosystems 3
1.3 Classical cryptography 7
1.4 Modern cryptography 8

2 Complexity theory 10
2.1 What is complexity theory? 10
2.2 Deterministic Turing machines 16
2.3 Decision problems and languages 22
2.4 Complexity of functions 30
2.5 Space complexity 33

3 Non-deterministic computation 39
3.1 Non-deterministic polynomial time – NP 39
3.2 Polynomial time reductions 43
3.3 NP-completeness 45
3.4 Turing reductions and NP-hardness 54
3.5 Complements of languages in NP 56
3.6 Containments between complexity classes 60
3.7 NP revisited – non-deterministic Turing machines 62

4 Probabilistic computation 67
4.1 Can tossing coins help? 67
4.2 Probabilistic Turing machines and RP 71

4.3 Primality testing 74
4.4 Zero-error probabilistic polynomial time 80
4.5 Bounded-error probabilistic polynomial time 81
4.6 Non-uniform polynomial time 83
4.7 Circuits 86
4.8 Probabilistic circuits 92
4.9 The circuit complexity of most functions 93
4.10 Hardness results 94

5 Symmetric cryptosystems 99
5.1 Introduction 99
5.2 The one time pad: Vernam's cryptosystem 101
5.3 Perfect secrecy 102
5.4 Linear shift-register sequences 106
5.5 Linear complexity 111
5.6 Non-linear combination generators 113
5.7 Block ciphers and DES 115
5.8 Rijndael and the AES 118
5.9 The Pohlig–Hellman cryptosystem 119

6 One way functions 125
6.1 In search of a definition 125
6.2 Strong one-way functions 129
6.3 One way functions and complexity theory 132
6.4 Weak one-way functions 135

7 Public key cryptography 141
7.1 Non-secret encryption 141
7.2 The Cocks–Ellis non-secret cryptosystem 142
7.3 The RSA cryptosystem 145
7.4 The Elgamal public key cryptosystem 147
7.5 Public key cryptosystems as trapdoor functions 150
7.6 Insecurities in RSA 153
7.7 Finding the RSA private key and factoring 155
7.8 Rabin's public key cryptosystem 158
7.9 Public key systems based on NP-hard problems 161
7.10 Problems with trapdoor systems 164

8 Digital signatures 170
8.1 Introduction 170
8.2 Public key-based signature schemes 171

8.3 Attacks and security of signature schemes 172
8.4 Signatures with privacy 176
8.5 The importance of hashing 178
8.6 The birthday attack 180

9 Key establishment protocols 187
9.1 The basic problems 187
9.2 Key distribution with secure channels 188
9.3 Diffie–Hellman key establishment 190
9.4 Authenticated key distribution 193
9.5 Secret sharing 196
9.6 Shamir's secret sharing scheme 197

10 Secure encryption 203
10.1 Introduction 203
10.2 Pseudorandom generators 204
10.3 Hard and easy bits of one-way functions 207
10.4 Pseudorandom generators from hard-core predicates 211
10.5 Probabilistic encryption 216
10.6 Efficient probabilistic encryption 221

11 Identification schemes 229
11.1 Introduction 229
11.2 Interactive proofs 231
11.3 Zero knowledge 235
11.4 Perfect zero-knowledge proofs 236
11.5 Computational zero knowledge 240
11.6 The Fiat–Shamir identification scheme 246

Appendix 1 Basic mathematical background 250
A1.1 Order notation 250
A1.2 Inequalities 250

Appendix 2 Graph theory definitions 252

Appendix 3 Algebra and number theory 253
A3.1 Polynomials 253
A3.2 Groups 253
A3.3 Number theory 254

Appendix 4 Probability theory 257

Appendix 5 Hints to selected exercises and problems 261

Appendix 6 Answers to selected exercises and problems 268

Bibliography 278
Index 287

Preface

This book originated in a well-established yet constantly evolving course on Complexity and Cryptography which we have both given to final year Mathematics undergraduates at Oxford for many years. It has also formed part of an M.Sc. course on Mathematics and the Foundations of Computer Science, and has been the basis for a more recent course on Randomness and Complexity for the same groups of students.

One of the main motivations for setting up the course was to give mathematicians, who traditionally meet little in the way of algorithms, a taste for the beauty and importance of the subject. Early on in the book the reader will have gained sufficient background to understand what is now regarded as one of the top ten major open questions of this century, namely the $\mathsf{P} = \mathsf{NP}$ question. At the same time the student is exposed to the mathematics underlying the security of cryptosystems which are now an integral part of the modern 'email age'.

Although this book provides an introduction to many of the key topics in complexity theory and cryptography, we have not attempted to write a comprehensive text. Obvious omissions include cryptanalysis, elliptic curve cryptography, quantum cryptography and quantum computing. These omissions have allowed us to keep the mathematical prerequisites to a minimum.

Throughout the text the emphasis is on explaining the main ideas and proving the mathematical results rigorously. Thus we have not given every result in complete generality.

The exercises at the end of many sections of the book are in general meant to be routine and are to be used as a check on the understanding of the preceding principle; the problems at the end of each chapter are often harder.

We have given hints and answers to many of the problems and exercises, marking the question numbers as appropriate. For example 1^{a}, 2^{h}, 3^{b} would indicate that an answer is provided for question 1, a hint for question 2 and both for question 3.

We have done our best to indicate original sources and apologise in advance for any omissions and/or misattributions. For reasons of accessibility and completeness we have also given full journal references where the original idea was circulated as an extended abstract at one of the major computer science meetings two or more years previously.

We acknowledge with gratitude the Institut des Hautes Études Scientifiques and the Department of Mathematics at Victoria University, Wellington where one of us spent productive periods working on part of this book.

It is a pleasure to thank Magnus Bordewich and Dillon Mayhew who have been valued teaching assistants with this course over recent years.

We are also grateful to Clifford Cocks, Roger Heath-Brown, Mark Jerrum and Colin McDiarmid who have generously given most helpful advice with this text whenever we have called upon them.

Notation

$\mathbb{N} = \{1, 2, \dots\}$	the set of natural numbers.
$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$	the set of integers.
$\mathbb{Z}^+ = \{0, 1, 2, \dots\}$	the set of non-negative integers.
$\mathbb{Q}$	the set of rational numbers.
$\mathbb{R}$	the set of real numbers.
$\mathbb{R}^+$	the set of non-negative real numbers.
$\mathbb{Z}[x_1, \dots, x_n]$	the set of polynomials in n variables over $\mathbb{Z}$.
$\lceil x \rceil$	the smallest integer greater than or equal to x.
$\lfloor x \rfloor$	the greatest integer less than or equal to x.
$\log n$	the base two logarithm of n.
$\ln x$	the natural logarithm of x.
$\{0, 1\}^k$	the set of zero–one strings of length k.
$\{0, 1\}^*$	the set of all zero–one strings of finite length.
$\binom{n}{k} = n!/(n-k)!k!$	the binomial coefficient 'n choose k'.
$g = O(f)$	g is of order f.
$g = \Omega(f)$	f is of order g.
$\Theta(f)$	f is of order g and g is of order f.
$\Pr[E]$	the probability of the event E.
$\mathrm{E}[X]$	the expectation of the random variable X.
Σ	an alphabet containing the blank symbol $*$.
Σ_0	an alphabet not containing the blank symbol $*$.
Σ^*	the set of finite strings from the alphabet Σ.
Σ^n	the set of strings of length n from Σ.
$\lvert x \rvert$	the length of a string $x \in \Sigma_0^*$.
$\lvert A \rvert$	the size of a set A.
$\gcd(a, b)$	the greatest common divisor of a and b.
$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$	the residues mod n.
$\mathbb{Z}_n^+ = \{1, \dots, n-1\}$	the non-zero residues mod n.

$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$	the units mod n.
$\vee$	Boolean disjunction (OR).
$\wedge$	Boolean conjunction (AND).
$\neg$	Boolean negation (NOT).
$a \leftarrow b$	a is set equal to b.
$x \in_R A$	x is chosen uniformly at random from the set A.
$a_1, \ldots, a_k \in_R A$	$a_1, \ldots, a_k$ are chosen independently and uniformly at random from A.
$A \leq_m B$	A is polynomially reducible to B.
$f \leq_T g$	f is Turing reducible to g.