

IST 2848

STUDENT MATHEMATICAL LIBRARY
Volume 18

Cryptography: An Introduction

V. V. Yaschenko
Editor



BIBLIOTHEQUE DU CRIST

Editorial Board

David Bressoud, Chair

Carl Pomerance

Robert Devaney

Hung-Hsi Wu

Daniel L. Goroff

Под редакцией В. В. Ященко

ВВЕДЕНИЕ В КРИПТОГРАФИЮ

МШМО ЧеРо, Москва 1998, 2000

Translated from the Russian by Sergei Lando

2000 *Mathematics Subject Classification*. Primary 94-01, 94A60;
Secondary 11T71, 68P25.

Library of Congress Cataloging-in-Publication Data

Vvedenie v kriptografiu. English.

Cryptography : an introduction / V. V. Yaschenko, editor.

p. cm. — (Student mathematical library. ISSN 1520-9121 ; v. 18)

Includes bibliographical references.

ISBN 0-8218-2986-6 (acid-free paper)

I. Computer security. 2. Cryptography. I. IAschenko, V. V. II. Title.
III. Series.

QA76.9.A25 V85 2002

005.8'2- dc21

2002027740

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

© 2002 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Printed in the United States of America.

⊗ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 07 06 05 04 03 02

Contents



Preface	vii
Chapter 1. Main Notions	1
§1. Introduction	1
§2. The subject of cryptography	3
§3. Mathematical basis	10
§4. New directions	13
§5. Conclusion	19
Chapter 2. Cryptography and Complexity Theory	21
§1. Introduction	21
§2. Cryptography and the $P \neq NP$ conjecture	24
§3. One-way functions	26
§4. Pseudorandom generators	29
§5. Zero-knowledge proofs	32
Chapter 3. Cryptographic Protocols	39
§1. Introduction	39

§2. Integrity. Authentication and electronic signature protocols	42
§3. Untraceability. Electronic money	60
§4. Coin flipping by telephone protocols	68
§5. More about secret sharing	74
§6. Playing building blocks, or Election protocols	77
§7. Beyond standard assumptions. Confidential message transmission	83
§8. In place of a conclusion	86
Chapter 4. Algorithmic Problems of Number Theory	87
§1. Introduction	87
§2. The RSA cryptosystem	89
§3. Complexity of number-theoretic algorithms	93
§4. How to distinguish between a composite and a prime number	99
§5. How to construct large prime numbers	102
§6. How to test primality of a large number	105
§7. How to factorize a composite number	110
§8. Discrete logarithms	114
§9. Conclusion	120
Chapter 5. Mathematics of Secret Sharing	121
§1. Introduction	121
§2. Secret sharing for arbitrary access structures	123
§3. Linear secret sharing	127
§4. Ideal secret sharing and matroids	129
Chapter 6. Cryptography Olympiads for High School Students	135

Contents

v

§1. Introduction	135
§2. Substitution ciphers	139
§3. Transposition ciphers	152
§4. Periodic polyalphabetic substitution ciphers	159
§5. Problems	165
§6. Answers, hints, solutions	184
Bibliography	225