IST 2848

STUDENT MATHEMATICAL LIBRARY
Volume 18

Cryptography: An Introduction

V. V. Yaschenko
Editor

AMS
American Mathematical Society

BIBLIOTHEQUE DU CERIST

1717

Editorial Board

David Bressoud, Chair
Robert Devaney
Daniel L. Goroff
Carl Pomerance
Hung-Hsi Wu

Под редакцией В. В. Ященко

ВВЕДЕНИЕ В КРИПТОГРАФИЮ

МЦНМО 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 kriptografiiu. 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)
1. Computer security. 2. Cryptography. I. IAshchenko, V. V. II. Title. III. Series.

QA76.9.A25V85 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

BIBLIOTHEQUE DU CERIST

Contents

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST