

CRYPTOGRAPHY

An Introduction
to

Computer Security

JENNIFER SEBERRY

JOSEF PIEPRZYK

Advances in Computer Science Series



Richard P. Brent – Editor

CRYPTOGRAPHY:

An Introduction to Computer Security

I said it in Hebrew - I said it in Dutch -
I said it in German and Greek:
But I wholly forgot (and it vexes me much)
That English is what you speak!

from *The Hunting of the Snark*
Lewis Carroll

'What does it mean by *speak, friend and enter?*' asked Merry.
'That is plain enough,' said Gimili. 'If you are a friend, speak the
password, and the doors will open, and you can enter.'
'Yes,' said Gandalf, 'these doors are probably governed by words ...'

from *The Lord of the Rings*
J. R. R. Tolkien

© 1989 by Prentice Hall of Australia Pty Ltd

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without permission of the publisher.

Printed and bound in Australia by Impact Printing, Brunswick, Vic.

1 2 3 4 5 93 92 91 90 89
ISBN 0 7248 0274 6 (paperback)
ISBN 0-13-194986-1 (hardback)

**National Library of Australia
Cataloguing-in-Publication Data**

Seberry, Jennifer, 1944—
Cryptography : an introduction to computer security.

Bibliography.
Includes index.
ISBN 0 7248 0274 6.

1. Computers—Access control. 2. Cryptography.
I. Pieprzyk, Josef, 1949— . II. Title.

005.8

**Library of Congress
Cataloguing-in-Publication Data**

Seberry, Jennifer, 1944—
Cryptography : an introduction to computer security/by Jennifer
Seberry and Josef Pieprzyk.

p. cm.
Bibliography: p.
ISBN 0-13-194986-1

1. Computers—Access control. 2. Cryptography.
I. Pieprzyk, Josef, 1949— . II. Title.

QA76.9.A25S37 1988

005.8—dc19

87-27026
CIP

Prentice Hall, Inc., *Englewood Cliffs, New Jersey*
Prentice Hall Canada, Inc., *Toronto*
Prentice Hall Hispanoamericana, S.A., *Mexico*
Prentice Hall of India Private Ltd, *New Delhi*
Prentice Hall International, Inc., *London*
Prentice Hall of Japan, Inc., *Tokyo*
Prentice Hall of Southeast Asia Pty Ltd, *Singapore*
Editora Prentice Hall do Brasil Ltda, *Rio de Janeiro*



PRENTICE HALL

A division of Simon & Schuster

CONTENTS

Preface	vii
Chapter 1. Introduction	1
Chapter 2. Background theory	7
2.1 Mathematical methods	7
2.2 Complexity theory	25
2.3 Complexity of selected problems used in cryptology	34
2.4 Information theory	45
Chapter 3. Encryption methods of information protection	61
3.1 Classical ciphers	61
3.2 Symmetric algorithms and DES	77
3.3 Asymmetric algorithms or public key cryptosystems	88
Chapter 4. Authentication methods	131
4.1 Elementary methods of message authentication	131
4.2 Subliminal channel	145
4.3 Digital signatures	154
4.4 Other authentication techniques	171
4.5 Summary	179
Chapter 5. Cryptography in computer network security	196
5.1 Information protection in computer networks	196
5.2 Key management issues	208
5.3 Electronic funds transfer (EFT)	218
5.4 Summary	225
Chapter 6. Application of cryptography in databases	233
6.1 Database model	234
6.2 Cryptographic transformation preserving data structure	236
6.3 Application of cryptography to protection of information during processing	246
6.4 Privacy homomorphisms	253
6.5 Summary	258

Chapter 7. Other cryptographic techniques	268
7.1 Linear feedback shift registers	268
7.2 One-way ciphers and passwords	271
7.3 Smart cards and information cards	272
7.4 Unforgeable ID cards using smart cards	273
7.5 Summary	279
Chapter 8. Security in operating systems	280
8.1 Access control in computer systems	280
8.2 Implementations of access control systems	284
8.3 Rationale for security evaluation classes	287
8.4 Summary	293
Chapter 9. Minimum knowledge systems	294
9.1 An introduction to the minimum knowledge concept	294
9.2 More on the Fiat-Shamir smart card protocol	296
9.3 Subliminal free verification using minimum knowledge protocols	298
9.4 Conclusion	299
Appendix A	300
A.1 Frequencies of occurrences of characters in languages	300
A.2 Frequencies of occurrences of pairs of letters in languages	304
Appendix B	321
B.1 DES code	321
B.2 Key representation for DES	337
Appendix C	340
Vigenere, Beauford or Variant Beauford code	340
Bibliography	344
Index	366

CRYPTOGRAPHY

An Introduction to Computer Security

JENNIFER SEBERRY and JOSEF PIEPRZYK

This book presents the mathematical and computer science background to cryptography in an easy-to-read, stimulating fashion. It includes numerous worked examples, diagrams and problems. Theory is applied to the most recent developments in computer security, including the following:

- minimum knowledge proof theorem
- unforgeable I.D. cards using smart cards
- the new classification system for secure operating systems

Also in the Advances in Computer Science Series:

Gough & Mohay: *Modula-2: A Second Course in Programming*
Hille: *Data Abstraction and Program Development Using Pascal*
Hille: *Data Abstraction and Program Development Using Modula-2*
Rankin: *Computer Graphics Software Construction*

ISBN 0-13-194986-1