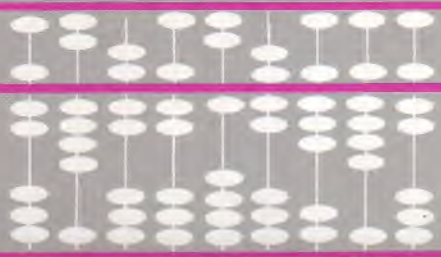
CRYPTOGRAPHY

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

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. Peiprzyk, 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

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