

INTERNATIONAL CENTRE FOR MECHANICAL SCIENCES

COURSES AND LECTURES - No. 279



# SECURE DIGITAL COMMUNICATIONS

EDITED BY  
G. LONGO  
UNIVERSITA' DI TRIESTE



SPRINGER-VERLAG WIEN GMBH

This volume contains 118 illustrations.

This work is subject to copyright.  
All rights are reserved,  
whether the whole or part of the material is concerned  
specifically those of translation, reprinting, re-use of illustrations,  
broadcasting, reproduction by photocopying machine  
or similar means, and storage in data banks.  
© 1983 by Springer-Verlag Wien  
Originally published by Springer Verlag Wien-New York in 1983

ISBN 978-3-211-81784-1

ISBN 978-3-7091-2640-0 (eBook)

DOI 10.1007/978-3-7091-2640-0

## PREFACE

*The necessity of keeping certain information secret is as old as human communication. At the same time the advantages to be gained in intercepting secret messages was soon realized. This has led to a century-long battle between the “codemakers” and the “codebreakers”, the battle being fought in the everchanging arena of communication media.*

*The concept of secure communication itself has evolved through the ages, as the traditional communication systems — like the mail and courier services — were supplemented by more technical media — radio, telephone, television, data links, etc. The amount of protection needed also vary depending both on the importance of the message contents and on the determination of the interceptor to understand and use the information.*

*The most common forms of communication are highly insecure, since they are easily intercepted and understood. Probably the use of a courier is the safest way to exchange messages, but this is seldom possible in our present society, which is so much dependent on large amounts of information exchanged at very high rate. One possibility is then to make information (almost) non-interceptible by concealing the messages via a suitable transformation before transmission. A cipher system is precisely a more or less sophisticated way of doing this, and the “art” (some would prefer “science”) of designing cipher systems is named cryptology (from two Greek words meaning “discourse on hiding”).*

*It has to be emphasized that the revolution of microelectronics has led both to ever-increasing capabilities of and to ever increasing dependence upon data processing and data transmission systems. This results in a tremendous growth of the need for protection against unauthorized access and misuse of the data. While the general public is increasingly alarmed by frauds in this area, professional cryptologists are well aware of the weaknesses of present-day security and of the difficulties of their task.*

*The aim of this book is to give a broad survey of the problem of secure communication. Some contributions are introductory, some are more advanced, but the interested reader can benefit from reading all of them as different chapters on one single topic of increasing importance.*

*I wish to thank all the participants and all the lecturers, whose generous effort make it possible to publish this book.*

*Giuseppe Longo*

*Udine, November 1983.*

## CONTENTS

	page
Preface . . . . .	I
Contents . . . . .	III
<i>Elements of Cryptology</i>	
by M. Davio and J.M. Goethals	
1. Classical Approach and Shannon Theory . . . . .	1
2. Block Ciphers. . . . .	12
3. Substitution Networks . . . . .	15
4. Basic Protocols in Modern Cryptology . . . . .	27
5. Knapsack Trapdoor Functions: An Introduction . . . . .	41
6. The RSA Trapdoor Function: An Analysis of Some Attacks . . . . .	51
References . . . . .	57
<i>Simple Substitution Ciphers</i>	
by A. Sgarro	
1. Introduction . . . . .	61
2. Mathematical Preliminaries . . . . .	62
3. Key Equivocation and Message Equivocation . . . . .	68
4. The Probability-of-Error Approach . . . . .	72
5. Final Remarks . . . . .	75
References . . . . .	76
<i>Stream Ciphers</i>	
by T. Beth	
1. Introduction . . . . .	79
2. Definitions and Notations . . . . .	81
3. A First Look at Secure Stream Ciphers . . . . .	85
4. An Excursion to Algebra . . . . .	89
5. How to Break a Stream Cipher which is Generated by a LFSR-Sequence . . . . .	92
6. An Analysis of Binary Deterministic Finite State Machines . . . . .	94
7. How to Construct "Good" P-R Generators? . . . . .	96
8. References . . . . .	103

	Page
<i>Secret Sharing Systems</i>	
by S. Harari . . . . .	105
<i>Key Management in Data Banks</i>	
by S. Harari . . . . .	111
<i>Electronic Signature Functions</i>	
by S. Harari . . . . .	117
<i>Primality Testing – A Deterministic Algorithm</i>	
by S. Harari . . . . .	121
<i>Communication in the Presence of Jamming – An Information Theory Approach</i>	
by R.J. McEliece . . . . .	
1. Introduction . . . . .	127
2. A Game-Theoretic Formulation . . . . .	128
3. A Pseudo-Random Scrambler . . . . .	135
4. Some Saddlepoints . . . . .	139
5. Spread-Spectrum Communication: The Results of Houston and Viterbi-Jacobs . . . . .	154
6. Acknowledgements . . . . .	163
References . . . . .	164
<i>Conflict Resolution Protocols for Secure Multiple-Access Communication Systems</i>	
by T. Berger and N. Mehravari	
1. Introduction . . . . .	168
2. Confusion Resolution Algorithm for Infinite User Model . . . . .	181
3. Confusion Resolution Algorithm for Finite User Model and Generalized Group Testing . . . . .	189
References . . . . .	227
<i>Security in Distributed Mobile-User Radio Networks</i>	
by A. Ephremides	
Preface . . . . .	231
1. Introduction . . . . .	232
2. The Capture Phenomenon . . . . .	241
3. Acknowledgements and Feedback Information . . . . .	248
4. A Case Study . . . . .	257
5. Inherent Network Security . . . . .	270

	Page
Conclusion . . . . .	277
References . . . . .	278
 <i>Fast Decoding Algorithms for Reed-Solomon Codes</i>	
by R.E. Blahut	
I. Introduction . . . . .	281
II. Decoding of Reed-Solomon Codes . . . . .	282
III. The Berlekamp-Massey Algorithm . . . . .	287
IV. Fast Convolution Algorithms . . . . .	288
V. The Winograd Fast Fourier Transform . . . . .	296
VI. A Fast Berlekamp-Massey Algorithm . . . . .	306
VII. Accelerated Decoding of BCH Codes . . . . .	313
References . . . . .	316
 <i>Pseudo-Random Sequences with A Priori Distribution</i>	
by J.H. Rabinowitz	
1. Introduction and Summary of Results . . . . .	318
2. De Bruijn Sequences and Necklace Graphs . . . . .	319
3. Atomic Sequences . . . . .	325
4. Link Hypergraphs and Realizable Atomic Distributions . . . . .	327
References . . . . .	331
List of Contributors . . . . .	332