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.


**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