Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

149

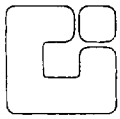
Cryptography

Proceedings of the Workshop on Cryptography
Burg Feuerstein, Germany, March 29 – April 2, 1982

Edited by Thomas Beth

Springer-Verlag
Berlin Heidelberg New York 1983

Editor
Thomas Beth
Friedrich-Alexander Universität Erlangen-Nürnberg
Institut für Mathematische Maschinen und Datenverarbeitung (Informatik 1)
Martensstr. 3, 8520 Erlangen, FRG



Gesellschaft für Informatik e.V.
– Fachausschuß 8 –

Institut für Mathematische
Maschinen und Datenverarbeitung

ARBEITSTAGUNG ÜBER KRYPTOGRAPHIE – BURG FEUERSTEIN – 29. 3. – 2. 4. 82

Diese erste europäische Arbeitstagung über Kryptographie wurde von folgenden Institutionen gemeinsam getragen:

Lehrstuhl I (Prof. Dr. K. Leeb) des Instituts für Mathematische Maschinen und Datenverarbeitung (Informatik) der Universität Erlangen-Nürnberg

Gesellschaft für Informatik e.V. (Fachausschuß 8)

Deutsche Forschungs-Gemeinschaft

CR Subject Classifications (1982): D 3

ISBN 3-540-11993-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-11993-0 Springer-Verlag New York Heidelberg Berlin

Library of Congress Cataloging in Publication Data. Main entry under title: Cryptography: proceedings, Burg Feuerstein, 1982. (Lecture notes in computer science ; 149)
1. Cryptography–Congresses. I. Beth, Thomas, 1949-. II. Series. Z102.5.C78 1983 001.54'36 83-430
ISBN 0-387-11993-0

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2145/3140-543210

Wir werden in der Folge Gelegenheit nehmen, die mancherlei Arten dieses Versteckens näher zu betrachten. Symbolik, Allegorie, Rätsel, Attrape, Chiffrieren wurden in Übung gesetzt. Apprehension gegen Kunstverwandte, Marktschreierei, Dünkel, Witz und Geist hatten alle gleiches Interesse, sich auf diese Weise zu üben und geltend zu machen, so daß der Gebrauch dieser Verheimlichungskünste sehr lebhaft bis in das siebzehnte Jahrhundert hinübergeht und sich zum Teil noch in den Kanzleien der Diplomatiker erhält.

Goethe: Farbenlehre-Historischer Teil,aus:"Lust am Geheimnis"

Preface

This book contains the proceedings of a workshop on cryptography that took place from March 29th to April 2nd , 1982 , at Burg Feuerstein in the lovely surroundings of the Fränkische Schweiz near Erlangen.

Burg Feuerstein is an extensive estate run by the diocese of Bamberg. It serves many purposes , mainly of social character.

Our workshop on cryptography , however , proved to be in the best traditions of these grounds , since the `Burg´ is not a genuine castle : it was built in the early 1940´s as a camouflaged center for communications engineering emphasizing cryptographic research . The unintended coincidence gives a good opportunity to note the changes that cryptographic research has undergone since then. One of the most remarkable was the fact that there were 76 participants from 14 nations.

This volume contains 26 articles altogether. The introduction is an expository survey for non-specialists and places in context the other 25 papers submitted. These are grouped into 10 sections within which they are arranged with regard to content. The editor has refrained judiciously from judging the significance or consistency of all the results. Together with its rather extensive (doubly linked) bibliography the book could be used as a self-contained text. At the back of the book are a list of participants as well as a list of the talks for which no paper was submitted.

The organizer is indebted to the Deutsche Forschungs - Gemeinschaft and to the Gesellschaft für Informatik for supporting the conference.

The advice given by H.J.Beker (Racal-Comsec,Salisbury) , by H.-R. Schuchmann (Siemens-Forschungslaboratorien,München), and by N.J.A. Sloane (Bell Laboratories, Murray Hill) were of substantial help.

Finally it is a pleasure to thank R.Dierstein (DFVLR Oberpfaffenhofen) for his experienced aid in organizing the workshop.

T.B.

Contents