

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

Editorial Board

D. Barstow W. Brauer P. Brinch Hansen D. Gries D. Luckham
C. Moler A. Pnueli G. Seegmüller J. Stoer N. Wirth

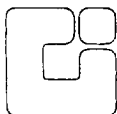
Editor

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)

I. Cryptography—Congresses. I. Beth, Thomas, 1949-. II. Series. Z102.5.C78 1983 001.54'36 83-430
ISBN 0-387-11993-0

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. Under
§ 54 of the German Copyright Law where copies are made for other than private use, a fee is
payable to "Verwertungsgesellschaft Wort", Munich.

© by Springer-Verlag Berlin Heidelberg 1983
Printed in Germany

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 Diplomaten 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

Section 1 : Introduction	1-28
Section 2 : Classical Cryptography	29-68
F.L.Bauer: Cryptology-Methods and Maxims	31
Mechanical Cryptographic Devices	47
A.G.Konheim: Cryptanalysis of a Kryha machine	49
H.-R.Schuchmann: Enigma Variations	65
Section 3 : Mathematical Foundations	69-128
N.J.A.Sloane: Encrypting by Random Rotations	71
Section 4 : Analogue Scrambling Schemes	129-178
H.J.Beker: Analogue Speech Security Systems	130
P.Hess;K.Wirl: A Voice Scrambling System for Testing and Demonstration	147
K.-P.Timmann: The Rating of Understanding in Secure Voice Communication Systems	157
L.Györfi;I.Kerekes: Analysis of Multiple Access Channel Using Multiple Level FSK	165
F.Pichler: Analog Scrambling by the General Fast Fourier Transform	173
Section 5 : Stream Ciphers	179-216
F.C.Piper: Stream Ciphers	181
S.M.Jennings: Multiplexed Sequences: Some Properties of the Minimum Polynomial	189
T.Herlestam: On Using Prime Polynomials in Crypto Generators	207
Section 6 : Cryptography in Large Communication Systems	217-232
M.R.Oberman: Communication Security in Remote Controlled Computer Systems	219
L.Horbach: Privacy and Data Protection in Medicine	228

Section 7 : The Data Encryption Standard	233-279
I.Schaumüller-Bichl: Cryptanalysis of the Data Encryption Standard by the Method of Formal Coding	235
J.A.Gordon;H.Retkin: Are Big S-Boxes Best ?	257
D.W.Davies;G.I.P.Parkin: The Average Cycle Size of the Key Stream in Output Feedback Encipherment	263
Section 8 : Authentication Systems	281-306
M.Davio;J.-M.Goethals;J.-J.Quisquater: Authentication Procedures	283
P.Schöbi;J.L.Massey: Fast Authentication in a Trapdoor -Knapsack Public Key Cryptosystem	289
Section 9 : The Merkle - Hellman - Scheme	307-322
I.Ingemarsson: A New Algorithm for the Solution of the Knapsack Problem	309
R.Eier;H.Lagger: Trapdoors in Knapsack Cryptosystems	316
Section 10: The Rivest - Shamir - Adleman - Scheme	323-375
C.P.Schnorr: Is the RSA -Scheme Safe ?	325
J.Sattler;C.P.Schnorr: Ein Effizienzvergleich der Faktorisierungs- verfahren von Morrison-Brillhart und Schroepfel	331
A.Ecker: Finite Semigroups and the RSA-Cryptosystem	353
M.Mignotte: How to Share a Secret?	371
List of talks for which no paper was submitted	376
Bibliography	377-397
List of Participants	398-402