

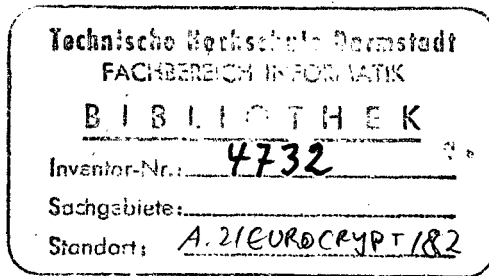
Lecture Notes in Computer Science

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



Fachbereichsbibliothek Informatik
TU Darmstadt



Springer-Verlag
Berlin Heidelberg New York 1983

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