PREFACE

This book contains the proceedings of EUROCRYPT 84, held in Paris in 1984, April 9-11, at the University of Paris, Sorbonne.

EUROCRYPT is now an annual international European meeting in cryptology, intended primarily for the international community of researchers in this area. EUROCRYPT 84 was following previous meetings held at Burg Feuerstein in 1982 and at Udine in 1983. In fact EUROCRYPT 84 was the first such meeting being organized under IACR (International Association of Cryptology Research). Other sponsors were the well-known French association on cybernetics research called AFCET, the LITP (Laboratoire d'Informatique théorique et de Programmation), which is a laboratory of computer science associated with CNRS, and the department of mathematics and computer science at the University René Descartes, Sorbonne.

EUROCRYPT 84 was very successful, with about 180 participants from a great variety of foreign countries and close to 50 papers addressing all aspects of cryptology, applied as well as theoretical. It also had a special feature, i.e. a special session on smart cards particularly welcome at the time, since France was then carrying on an ambitious program on smart cards.

EUROCRYPT 84 was a great experience. We like to thank all the sponsors and all the authors for their submission of papers.


Norbert COST
CONTENTS

SECTION I: GENERAL THEORY, CLASSICAL METHODS

Cryptology and Complexity Theories................................. 3
G. RUGGIU

On Cryptosystems based on Polynomials and Finite Fields........ 10
R. LIDL

Algebraical Structures of Cryptographic Transformations....... 16
J.P. PIEPRZYK

Non-linear, Non-Commutative Functions for Data Integrity...... 25
S. HARA RI

Wire-Tap Channel II.................................................... 33
L.H. OZAROW, A.D. WYNER

Equivocations for Homophonic Ciphers.............................. 51
A. SGARRO

Propagation Characteristics of the DES........................... 62
M. DAVID, V. DESMEDT, J.J. QUISQUATER

Linear Ciphers and Random Sequence Generators with Multiple
Clocks............................................................................. 74
J.L. MASSEY, R.A. RUEPEL

The Stop-and-go Generator............................................. 88
T. BÉTH, F.C. PIPER

Pseudo Random Properties of Cascade Connections of Clock
Controlled Shift Registers............................................. 93
D. GOLLHAN

On the Linear Complexity of Cascaded Sequences............... 99
R. VOGEL

SECTION II: PUBLIC-KEY SYSTEMS

RSA-Bits are $0.5 + \varepsilon$ Secure.................................. 115
C.P. SCHNÖRR, W. ALEXI

On the Number of Close-and-equal Pairs of Bits in a String.... 127
O. GOLDBEICH
Fast Cryptanalysis of the Matsumoto-Imai Public Key Scheme
V. DESMEUT, P. DELSARTE, A. ODLYZKO, P. PIRET

A New Trapdoor Knapsack Public-Key Cryptosystem
R.M.F. GOODMAN, A.J.MC AULEY

RSA Chips (Past/Present/Future)
R. RIVEST

SECTION III: NUMBER THEORETICAL PAPERS

The Quadratic Sieve Factoring Algorithm
C. POMERANCE

Status Report on Factoring (At the Sandia National Labs)
J.A. DAVIS, D.B. HOLDRIDGE, G.J. SIMMONS

Strong Primes are Easy to Find
J.A. GORDON

Discrete Logarithms in Finite Fields and their Cryptographic Significance
A.M. ODLYZKO

SECTION IV: CHANNELS, NETWORKS, KEY DISTRIBUTION, PROTOCOLS

User Functions for the Generation and Distribution of Encipherment Keys
R.W. JONES

An Optimal Class of Symmetric Key Generation Systems
R. BLUM

On the Use of the Binary Multiplying Channel in a Private Communication System
E.J.M. SHEETS

Secrecy and Privacy in a Local Area Network Environment
G.B. AGNEW

The Subliminal Channel and Digital Signatures
G.J. SIMMONS

A Provably Secure Oblivious Transfer Protocol
R. BERGER, R. PERALTA, T. TEDRICK

On Concurrent Identification Protocols
O. GOLDREICH
SECTION V: APPLICATIONS

Time-division Multiplexing Scramblers: Selecting Permutations and Testing the Systems ........................ 399
A. ECKER

Security of Transportable Computerized Files ........................................ 416
A. BOUCKAERT

Encryption and Key Management for the ECS Satellite Service .... 420
S.C. SERPELL, C.B. BROOKSON

An Encryption and Authentification Procedure for Tele-surveillance Systems .............................. 437
W. WOLFOWICZ, O. BRUGIA, S. IMPROTA

A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques ....... 446
I. SCHAUMUELLER, E. PILLER

SECTION VI: SMART CARDS

Introductory Remarks ................................................................. 457
A. TURBAT

Smart Card Applications in Security and Data Protection ................ 459
J. GOUTAY

Bull CP8 Smart Card Uses in Cryptology ........................................... 464
V. GIRARDOT

Estimation of Some Encryption Functions Implemented into Smart Cards ........................................... 470
H. GROSCOT

Smart Cards and Conditional Access .............................................. 480
L. GUILLOU

AUTHOR INDEX ................................................................. 491