CRYPTO 81

was sponsored by

The Data and Computer Communications Committees
of the
IEEE Communications Society

with the cooperation of the
Dept. of Electrical and Computer Engineering
University or California, Santa Barbara

The workshop was supported in part by the
National Science Foundation
Award No. ECS81-17145

Organizing Committee

Chairman: Allen Gersho (Univ. Calif., Santa Barbara)
Committee Members:
Leonard Adleman (Univ. Southern Calif.)
Whitfield Diffie (BNR)
Martin Hellman (Stanford)
Ricnard Kemmerer (Univ. Calif., Santa Barbara)
Alan Konheim (IBM)
Raymond Pickholtz (George Washington Univ.)
Brian Schanning (Mitre)
Gus Simmons (Sandia)
Stephen Weinstein (American Express)

ADVANCES IN CRYPTOGRAPHY

Allen Gersho, Editor

A Report on CRYPTO 81

ECE Rept No 82-04

CRYPTO 81
IEEE Workshop on Communications Security
held at
University of California, Santa Barbara
August 24-26, 1981

August 20, 1982
Department of Electrical & Computer Engineering
Santa Barbara, California 93106

Advances in Cryptography

Preface

This report contains information provided by the authors about the papers presented at CRYPTO 81. In some cases only abstracts were available, in a few cases essentially complete papers have been included, and in most cases an extended abstract or summary is provided. The Table of Contents gives the complete program with the original titles. In a few papers, the authors have provided closely related material with different titles.

This report is more an afterthought than a proceedings. The success of the workshop motivated considerable interest in making available some form of record of the event. The report was prepared for the participants of the workshop and for the use of the National Science Foundation whose support was of tremendous value by providing travel funds for several participants who would not otherwise have been able to attend.

Allen Gersho, Editor

Table of Contents

Session A: Theory & Implementation
Ron Rivest, MIT, Chairman

Session B: Algorithms, Techniques, & Funding
Ralph Merkle, ELXSI Int'l, Chairman

Rump Session
Paul S. Henry, Bell Labs, Chairman