



# ADVANCES IN CRYPTOGRAPHY

Allen Gersho, Editor

A Report on CRYPTO 81

ECE Rept No 82-04



**DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING**

UNIVERSITY OF CALIFORNIA    SANTA BARBARA, CALIFORNIA 93106

# 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

## 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 of 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)  
Richard Kemmerer (Univ. Calif., Santa Barbara)  
Alan Konheim (IBM)  
Raymond Pickholtz (George Washington Univ.)  
Brian Schanning (Mitre)  
Gus Simmons (Sandia)  
Stephen Weinstein (American Express)