Two days of technical colloquia covering the latest advances in the cryptographic sciences.

RSA Laboratories®

A Division of RSA Data Security

THE 1997 RSA LABORATORIES SEMINAR SERIES

August 14-15, 1997

Claremont Resort

Oakland, California

RSA Laboratories Seminar Series

As awareness of the importance of cryptography and security becomes more widespread, the connections among researchers in academia and the developers and designers of cryptographic products grow increasingly significant.

Held annually, the RSA Laboratories Seminar Series seeks to provide a forum for the frank discussion and free exchange of information among technical professionals in the cryptographic sciences from academia, government and industry.

In a change from previous years, the 1997 Seminar Series will concentrate in large part on emerging trends within the cryptographic sciences: new directions in research, the latest applications and techniques, and their effects on industry standards.

Towards this end, we offer some of the top cryptographic experts presenting their perspectives on the leading edges of cryptography— not just the state-of-the-art, but the state-of-the-art to come… two, or five, or even ten years into the future.

Taking place during the week that directly precedes the annual IACR *CRYPTO* conference, the 1997 RSA Laboratories Seminar Series offers a wonderful opportunity to get right to the heart of current cryptographic research, and to map out its future directions.

Who should attend:

The Seminar Series is aimed primarily at developers and engineers who have a good working knowledge and a basic understanding of cryptographic issues. While the seminars will not be particularly mathematical in nature, we anticipate that they will be most beneficial to those already familiar with many of today's cryptographic techniques.

Scheduled Speakers

We are very fortunate to be able to bring to this year's Seminar Series the skills and experiences of many cryptographic experts. Each speaker will provide an overview of his or her own particular field of expertise and attendees will have the unique opportunity to ask each researcher direct questions about the future practical significance of some of the latest research work.

Our scheduled speakers include:

Mihir Bellare
Assistant Professor, University of California, San Diego

Dan Boneh
Research Scientist, Bellcore

John Brainard
Principal Research Engineer, RSA Laboratories East

Walter Fumy
Siemens A.G., Germany

Rosario Gennaro
Research Staff Member, IBM Corporation

Jon Grantham
Research Staff Member, Institute for Defense Analyses

Ari Juels
Research Scientist, RSA Laboratories East

Burt Kaliski
Chief Scientist, RSA Laboratories East

Prof. Jean-Jacques Quisquater
Université Catholique de Louvain, Belgium

Prof. Ron Rivest
Massachusetts Institute of Technology

Matt Robshaw
Principal Research Scientist, RSA Laboratories West

Phillip Rogaway
Assistant Professor, University of California, Davis

Prof. Claus Schnorr
Universität Frankfurt a.M., Germany

Ray Sidney
Research Scientist, RSA Laboratories West

Bob Silverman
Senior Research Scientist, RSA Laboratories East

Thursday August 14, 1997

Provisional Schedule

morning

Jean-Jacques Quisquater:
Preventing Hardware Attacks

(TBA):
Proactive and Threshold Techniques

break

Ron Rivest:
SPKI / SDSI 2.0

lunch

afternoon

Walter Fumy:
ISO Update

Burt Kaliski:
IEEE P1363 Status Report

Ray Sidney:
PKCS Developments

break

John Brainard:
Cryptographic Security Services Protocol

Bob Silverman:
Standards for RSA Key Generation

Matt Robshaw:
AES: the Successor to DES

banquet

Friday August 15, 1997

Provisional Schedule

morning

Phillip Rogaway:
Target Collision-Resistant Hashing

Mihir Bellare:
Symmetric Encryption: Security of the DES Modes of Operation

break

Claus Schnorr:
Lattice Cryptosystems & Cryptanalysis

Jon Grantham:
Primality Testing

lunch

afternoon

Rosario Gennaro:
Secure Voting

Ari Juels:
Survey of Electronic Payment Systems

Dan Boneh:
Cryptographic Watermarking

Information and Registration Details

The 1997 RSA Laboratories Seminar Series will take place at the Claremont Resort, located in the Oakland foothills adjacent to the University of California, Berkeley.

The number of attendees at this year's Seminar Series will be limited in order to maintain an informal atmosphere conducive to freeranging discussions. Those interested in attending are advised to register as soon as possible. Registration for the Seminar Series is $995 and the chief registration period is from July 7 to August 3. Should space be available after August 3, registrants will be charged an additional fee of $300.

The registration fee includes a copy of the Seminar Series proceedings as well as invitations to the welcome reception on the evening of August 13 and the Seminar Series Banquet on August 14. Breakfast and lunch on both August 14 and August 15 will be included.

Payment can be made by major credit card or check. Please make checks payable in U.S. funds to RSA Data Security, Inc.

Please note that accommodation is not included in the registration fee. Instead a limited number of rooms are being held at the Claremont Resort at $145 per night. To reserve rooms at the Claremont Resort, please call 510-843-3000 and mention RSA Laboratories when booking your room.

Please mail the registration form and any required enclosures to:

RSA Laboratories Seminar Series Registration
100 Marine Parkway, Suite 500
Redwood City, CA 94065-1031
415/595-7703 (voice); 415/595-4126 (fax)
E-mail: rsa-labs@rsa.com

Registration Form

Contact Information:

First Name:	Last Name:	
Position/Title:	Organization:	
Address/Mail Stop:		
City:	Zip Code + 4:	State/Province:
Work Phone:	Work Fax:	Country:
E-mail:		

☐ I require vegetarian meals

☐ I do not want my information to appear in the attendees list

Payment Information:

Check ☐	Mastercard ☐	VISA ☐	Exp. Date:
Account No.			
Cardholder Name:	Cardholder Signature:		

Registration Fees:

Standard rate registration — $995	☐
Late registration (after August 3) — $1295	☐
Total Fee:	

There will be a $75 charge for cancellation up to two weeks before the Seminar Series; after that time registration fees will be non-refundable. Registrations may be transferred within the same organization.

RSA Laboratories®

A Division of RSA Data Security

100 Marine Parkway, Suite 500
Redwood City, CA 94065-1031

Tel 415/595-7703
Fax 415/595-4126

rsa-labs@rsa.com
http://www.rsa.com/rsalabs/

FIRST CLASS
U.S. POSTAGE
PAID
MMS, INC.