Preface

Crypto '96, the Sixteenth Annual Crypto Conference, is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara (UCSB). It takes place at UCSB from August 18 to 22, 1996. The General Chair, Richard Graveman, is responsible for local organization and registration.

The scientific program was organized by the 16-member Program Committee. We considered 115 papers. (An additional 15 submissions had to be summarily rejected because of lateness or major noncompliance with the conditions in the Call for Papers.) Of these, 30 were accepted for presentation. In addition, there will be five invited talks by Ernest Brickell, Andrew Clark, Whitfield Diffie, Ronald Rivest, and Cliff Stoll. A Rump Session will be chaired by Stuart Haber.

These proceedings contain the revised versions of the 30 contributed talks. The submitted version of each paper was examined by at least three committee members and/or outside experts, and their comments were taken into account in the revisions. However, the authors (and not the committee) bear full responsibility for the content of their papers.

A successful Crypto conference requires the combined efforts of many people. In the first place I wish to thank the members of the Program Committee, who devoted a tremendous amount of time and energy to reading the papers and making a difficult selection. They are: Mihir Bellare, Josh Benaloh, Matt Blaze, Johannes Buchmann, Don Coppersmith, Joan Feigenbaum, Andrew Klapper, Lars Knudsen, Peter Landrock, Tsutomu Matsumoto, Chris Mitchell, Paul Van Oorschot, Bart Preneel, Rainer Rueppel, and Jacques Stern. They were assisted by the following outside experts, whom I would also like to thank: Martin Abadi, Birgit Baum, Charles Bennett, Antoon Bosselaers, Gilles Brassard, Florent Chabaud, Giovanni Di Crescenzo, Matthew Franklin, Jovan Golic, Louis Granboulan, Russell Impagliazzo, Markus Jacobsson, Thomas Jakobsen, Jack Lacy, Xuejia Lai, Kevin McCurley, Kaisa Nyberg, David Pointcheval, James Reeds, Mike Reiter, Vincent Rijmen, Dan Simon, Doug Stinson, Serge Vaudenay, Michael Waidner, Michael Wiener, Yakov Yakobi. I apologize for any omissions in this list.

I would next like to thank the authors of all the papers (not just the ones that we were able to accept) for their hard work and cooperation. In particular, I very much appreciated the positive spirit with which they complied with the new requirement of a 1-page statement about the oral presentation, even though this was a further imposition on their time. The authors' 1-page statements turned out to be useful to me and the reviewers in several ways: in determining whom to ask to evaluate the paper, in getting an informal

overview (which the authors might not have found appropriate to include in the formal paper), and sometimes in deciding between acceptance and rejection in a borderline case.

Finally, I want to thank a few other individuals who made the job of Program Chair more tractable and rewarding. It was a pleasure to work with the General Chair, Richard Graveman, who was helpful and cooperative beyond the call of duty. Scott Vanstone was an important source of encouragement in the first period after my appointment as Program Chair, when I was afraid that I would do everything wrong. My wife Ann provided some useful suggestions, as well as the reassuring perspective of a historian of science who knows that any damage caused by my mistakes will be of no importance in the next millennium.

Neal Koblitz
June, 1996

CRYPTO '96

University of California, Santa Barbara
August 18-22, 1996

Sponsored by the

International Association for Cryptologic Research

in cooperation with the

IEEE Computer Society Technical Committee on Security and Privacy

and the

Computer Science Department, University of California, Santa Barbara

General Chair

Richard Graveman, Bellcore, USA

Program Chair

Neal Koblitz, University of Washington, Seattle, USA

Program Committee

Mihir Bellare	Univ. of California, San Diego, USA
Josh Benaloh	Microsoft, USA
Matt Blaze	AT&T Bell Laboratories, USA
Johannes Buchmann	Universität de Saarlandes, Germany
Don Coppersmith	IBM T.J. Watson Research Center, USA
Joan Feigenbaum	AT&T Bell Laboratories, USA
Andrew Klapper	University of Kentucky, USA
Lars Knudsen	Ecole Normale Supérieure, France
Peter Landrock	Aarhus University, Denmark
Tsutomu Matsumoto	Yokohama National University, Japan
Chris Mitchell	University of London, UK
Paul Van Oorschot	Bell-Northern Research, Canada
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Rainer Rueppel	R^3 Security Engineering, Switzerland
Jacques Stern	Ecole Normale Supérieure, France