Preface

SAC'99 was the sixth in a series of annual workshops on Selected Areas in Cryptography. Previous workshops were held at Carleton University in Ottawa (1995 and 1997) and at Queen's University in Kingston (1994, 1996, and 1998). The intent of the annual workshop is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The themes for the SAC'99 workshop were:

- Design and Analysis of Symmetric Key Cryptosystems
- Efficient Implementations of Cryptographic Systems
- Cryptographic Solutions for Web/Internet Security

The timing of the workshop was particularly fortuitous as the announcement by NIST of the five finalists for AES coincided with the first morning of the workshop, precipitating lively discussion on the merits of the selection!

A total of 29 papers were submitted to SAC'99 and, after a review process that had all papers reviewed by at least 3 referees, 17 were accepted and presented. As well, two invited presentations were given: one by Miles Smid from NIST entitled "From DES to AES: Twenty Years of Government Initiatives in Cryptography" and the other by Mike Reiter from Bell Labs entitled "Password Hardening with Applications to VPN Security".

The program committee for SAC'99 consisted of the following members: Carlisle Adams, Tom Cusick, Howard Heys, Lars Knudsen, Henk Meijer, Luke O'Connor, Doug Stinson, Stafford Tavares, and Serge Vaudenay. As well, additional reviewers were: Christian Cachin, Louis Granboulan, Helena Handschuh, Julio Lopez Hernandez, Mike Just, Alfred Menezes, Serge Mister, Guillaume Poupard, Victor Shoup, Michael Wiener, and Robert Zuccherato.

The organizers are very grateful for the financial support for the workshop received from Entrust Technologies, the Department of Electrical and Computer Engineering at Queen's University, and Communications and Information Technology Ontario (CITO). Special thanks to Stafford and Henk must be given for, once again, hosting SAC and being responsible for all the local arrangement details. The organizers would also like to thank Sheila Hutchison of the Department of Electrical and Computer Engineering at Queen's University for administrative and secretarial help and Yaser El-Sayed from the Faculty of Engineering at Memorial University of Newfoundland for help in preparing the workshop proceedings.

On behalf of the SAC'99 organizing committee, we thank all the workshop participants for making SAC'99 a success!

November 1999 Howard Heys and Carlisle Adams

Organization

Program Committee

Howard Heys (co-chair)	Memorial University of Newfoundland
Carlisle Adams (co-chair)	Entrust Technologies, Ottawa
Tom Cusick	SUNY, Buffalo
Lars Knudsen	University of Bergen
Henk Meijer	Queen's University at Kingston
Luke O'Connor	IBM, Zurich
Doug Stinson	University of Waterloo
Stafford Tavares	Queen's University at Kingston
Serge Vaudenay	Ecole Normale Supérieure, Paris

Local Organizing Committee

Stafford Tavares	Queen's University at Kingston
Henk Meijer	Queen's University at Kingston