# WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY (SAC '97)

**August 11 – 12, 1997**

## WORKSHOP RECORD

School of Computer Science
Carleton University
Ottawa, Ontario
Canada
K1S 5B6

# Preface

SAC '97 is the fourth in a series of annual workshops on Selected Areas in Cryptography. SAC '94 and SAC '96 were held at Queen's University and SAC '95 was held at Carleton University. The purpose of the workshop is to bring together researchers in cryptography and present new work on selected areas of interest. By concentrating on several selected areas we hope to facilitate a more comfortable atmosphere, allowing for increased interaction and in-depth discussion. The themes for this year's workshop are

- Efficiency in Cryptographic Systems,
- Symmetric Cipher Design & Implementation, and
- Protocols and Techniques for Web Security.

Of the 31 papers submitted to SAC '97, 20 were accepted for presentation at the workshop. We would like to thank the program committee members, Howard Heys, Henk Meijer, Stafford Tavares and Michael Wiener, who along with ourselves, participated in the selection process. As well, we would like to thank the following external reviewers for their help with the selections: Zhi-Guo Chen, Eric De Win, Václav Matyáš Jr., Serge Mister, Doug Stinson, Amr Youssef and Rob Zuccherato.

Complementing the Workshop Record that is made available to participants, this is the first year that the presented papers are available online. We thank the authors for the timely return of their papers in postscript form. The papers are available from the official SAC webpage located at `http://adonis.ee.queensu.ca:8000/sac/sac.html`.

SAC '97 is sponsored by the School of Computer Science at Carleton University, Entrust Technologies and the Interac Association. We would especially like to thank Rosemary Carter of the School of Computer Science for her assistance in every aspect of the organization of the workshop. As well, we would like to thank Richard Outerbridge for initiating the partnership between SAC '97 and the Interac Association. We also thank the International Association for Cryptologic Research (IACR) for their cooperation.

On behalf of the Organizing Committee, we welcome you to SAC '97, Carleton University and Ottawa.

Mike Just
Carlisle Adams
Ottawa, August 1997

# Table of Contents

## Stream Ciphers



## Working in GF($2^n$)



## Symmetric Ciphers II

## Invited Talk III



## Cryptanalysis



## Public-Key Cryptography