WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY (SAC '95)

May 18 – 19, 1995

WORKSHOP RECORD

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

Preface

SAC '95 is the 2nd in a series of annual workshops on Selected Areas in Cryptography. The first workshop was held at Queen's University in Kingston on May 5 and 6, 1994. The purpose of the workshop is to bring together researchers in cryptography and present new work on selected areas of current interest. It is hoped that by focusing on chosen topics more opportunity will exist for in-depth discussion. This year's topics include

Key Establishment
Cryptogrphic Protocols
Hashing and Message Authentication
Cryptanalysis of Symmetric Ciphers
Block Cipher Design

as well as a panel session on "The role of block ciphers: Today and Tomorrow".

A subset of the papers accepted for SAC '95 will be invited for submission to a special issue of "Designs, Codes and Cryptography", to be refereed in accordance with the standard process for that journal.

The worshop is sponsored by the School of Computer Science - Carleton University and Bell-Northern Research/Northern Telecom Secure Networks, in cooperation with the International Association for Cryptologic Research (IACR). Many thanks to Rosemary Carter and Barbara Coleman for their assistance in the organization of the workshop.

On behalf of the program committee

Carlisle Adams (Bell-Northern Research)
Josh Benaloh (Microsoft Corp.)
Evangelos Kranakis (Carleton University)
Danny Krizanc (Carleton University)
Henk Meijer (Queen's University)
Paul Van Oorschot (Bell-Northern Research)
Stafford Tavares (Queen's University)

we would like to welcome you to SAC '95.

M. Just, E. Kranakis, D. Krizanc, and P. Van Oorschot
Ottawa, May 1995

SAC '95 PROGRAM

All lectures will take place in room 3120 of the Herzberg Building.

THURSDAY, MAY 18, 1995

8:40-8:55 **Opening Remarks & Introduction of Invited Speaker,** *Paul Van Oorschot*

8:55-9:40 **Invited Talk:** *Doug Stinson* 1

"On Some Methods For Unconditionally Secure Key Distribution and Broadcast Encryption"

9:40-10:00 **Break**

10:00-11:30 **Key Establishment** 2

"On One-Pass Authenticated Key Establishment Schemes", *Kaisa Nyberg*

"Server-Aided Secret Key Exchange", *Chae Hoon Lim, Pil Joong Lee*

"Some New Key Agreement Protocols Providing Implicit Authentication", *Alfred Menezes, Minghua Qu, Scott Vanstone*

11:30-1:00 **Lunch**

1:00-2:00 **Cryptographic Protocols** 35

"Automated Security Analysis of Cryptographic Protocols Using Coloured Petri Net Specifications", *Eric Doyle, Stafford Tavares, Henk Meijer*

"An Efficient and Secure Authentication Protocol Using Uncertified Keys", *I-Lung Kao, Randy Chow*

2:00-2:20 Break

2:20-3:20 Hashing & Message Authentication 58

"Practical and Secure Message Authentication", *S. Bakhtiari, R. Safavi-Naini, J. Pieprzyk*

"The Compression Function of MD2 is not Collision Free", *Nathalie Rogier, Pascal Chauvaud*

3:20-3:40 Break

3:40-3:45 Introduction of Invited Speaker

3:45-4:30 Invited Talk: *Bart Preneel* 89

"Software performance of block ciphers and hash functions"

4:30-5:30 Panel Session

"The role of block ciphers: Today and Tomorrow"

7:00-7:30 Social Gathering

7:30-9:00 Dinner

FRIDAY, MAY 19, 1995

8:30-8:45 Introduction of Invited Speaker

8:45-9:30 Invited Talk: *Kaisa Nyberg*

"Chosen Plaintext in Linear Cryptanalysis"

9:30-10:00 Break