



# THE 1997 RSA DATA SECURITY CONFERENCE

## SPEAKER BIOGRAPHY

### CRYPTOGRAPHERS' TRACK

Speaker: **Bart Preneel**

Dr. Engineer

Katholieke Universiteit,

Leuven c/o Utimaco De vunt 9 Holsbeek,

B-3220Belgium

Phone: 32-1644-0135

Fax: 32-1644-0140

### Presentation Overview:

This talk offers a general perspective on the design and evaluation of fast cryptographic algorithms (block ciphers, stream ciphers, hash functions). We will focus on engineering aspects such as: hardware vs. software, use of memory (tables, registers, cache) word size and parameter size, parallelism, speed vs. provable security against certain attacks. Algorithms whose design principles will be compared include: Blowfish, IDEA, DES, RC-5, SAFER, SEAL, SHA-1 SHARK, Tiger, etc. We will also address the issue of proprietary (confidential) algorithms vs. public algorithms.

### Speaker Background:

Bart Preneel is a postdoctoral researcher, sponsored by the National Fund for Scientific Research Belgium, (N.F.W.O). During the academic year 1993-1994, he was a research fellow of the EECS Department of the University of California at Berkeley. His main research interests are cryptography and wireless communications.

**PRESENTATION**