



CRYPTOGRAPHERS TRACK

THE 1997 RSA DATA SECURITY CONFERENCE

1996: THE CRYPTOGRAPHIC YEAR IN REVIEW

- Dr. Yiquin Lisa Yin, RSA Laboratories

THE CRYPTOGRAPHY OF LAW ENFORCEMENT

- Dr. Taher ElGamal, Netscape Communications Corporation

HANDLING CRYPTO BOTTLENECKS

- Dr. Yacov Yacobi, Microsoft Corporation

SDSI - A SIMPLE DISTRIBUTED SECURITY INFRASTRUCTURE

- Dr. Ron Rivest, Massachusetts Institute of Technology

SYMMETRIC CIPHER DESIGN & IMPLEMENTATION

- Dr. Michael Wiener, Entrust Technologies

BACK TO THE DARK AGES

- Dr. Richard Pinch, University of Cambridge, Queen's College

RECENT DEVELOPMENTS IN HASH FUNCTIONS

- Dr. Matt Robshaw, RSA Laboratories

TRANSFERABLE AND ONLINE SECRET SHARING

- Dr. Richard Pinch, University of Cambridge, Queen's College

A SECURITY FLAW IN THE X.509 STANDARD

- Santosh Chokhani, CygnaCom Solutions, Inc.

PROACTIVE SECURITY: RECOVERING FROM PENETRATIONS

- Amir Herzberg, IBM Research

SUBLIMINAL CHANNELS

- Dr. Gustavus Simmons

RECENT TRENDS IN THE DESIGN OF CRYPTOGRAPHIC ALGORITHMS

- Dr. Bart Preneel, Katholieke Universiteit, Leuven

EFFICIENT CERTIFICATE REVOCATION AND CERTIFIED E-MAIL WITH TRANSPARENT POST OFFICES

- Dr. Silvio Micali, Massachusetts Institute of Technology

PART 1: CRYPTOGRAPHIC ARCHITECTURE BASED ON CONTROL VECTORS

PART 2: IBM'S KEY RECOVERY INITIATIVE

- Dr. Stephen M. Matyas, IBM Corporation

ECDSA: AN ENHANCED DSA

- Don B. Johnson, Certicom

THE EXACT SECURITY OF DIGITAL SIGNATURES: HOW TO SIGN WITH RSA AND RABIN.

- Mihir Bellare, University of California, San Diego