

TVOFISH
SERPENT
SAFEPR
BUNDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFEPR
BUNDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

Special Report on the First AES Conference

Miles Smid

Morris Dworkin

NIST

WELCOME!

**The First
Advanced Encryption Standard (AES)
Candidate Conference**

August 20-22, 1998

Double Tree Hotel
Ventura, California

“It’s time for those 128-, 192-, and 256-bit keys”

TRIOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TRIOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

TRIOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TRIOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

AES1 Conference Overview

- Formal presentation of candidate algorithms and design philosophies
- Distribution of CD-1: Documentation
- Call for analysis
- Discussion
- Announcement of Second AES Conference

Note: To obtain CD-2 see <http://www.nist.gov/aes>

TVOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

Selecting the Candidates

- Twenty-one packages received
- NIST verified that legal documents were completed
- NIST verified that responses were provided for all items
- NIST attempted to run code and verify Known Answer Tests
- Six packages found to be incomplete
- No cryptanalysis performed

Candidate Algorithms

- Australia
 - LOKI97 Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
- Belgium
 - RIJNDAEL Joan Daemen, Vincent Rijmen
- Canada
 - CAST-256 Entrust Technologies, Inc.
 - DEAL Outerbridge, Knudsen
- Costa Rica
 - FROG TecApro Internacional S.A.
- France
 - DFC Centre National pour la Recherche Scientifique (CNRS)
- Germany
 - MAGENTA Deutsche Telekom AG

TVOFISH
SERPENT
SAFEPR
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFEPR
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Candidate Algorithms

- Japan
 - E2 Nippon Telegraph and Telephone Corporation (NTT)
- Korea
 - CRYPTON Future Systems, Inc.
- USA
 - HPC Rich Schroepel
 - MARS IBM
 - RC6 RSA Laboratories
 - SAFER+ Cylink Corporation
 - TWOFISH Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
- UK, Israel, Norway
 - SERPENT Ross Anderson, Eli Biham, Lars Knudsen

TWOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TWOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

Based on Previous Schemes

- CAST-256 CAST-128
- DEAL DEA
- LOKI97 LOKI 89,91
- RC6 RC5
- SAFER+ SAFER

TV0FISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TV0FISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

Feistel Networks

<u>Algorithm</u>	<u>Rounds</u>
DEAL	6,6,8
DFC	8
E2	12
LOKI97	16
MAGENTA	6,6,8
TWOFISH	16

TWOFISH
SERPENT
SAFER+
BUNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TWO FISH
SERPENT
SAFER+
BUNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

Modified Feistel Networks

<u>Algorithm</u>	<u>Rounds</u>	<u>Cycles</u>
CAST-256	48	12
MARS	32	16
RC6	20	10

TRIOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TRIOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

SP Networks

<u>Algorithm</u>	<u>Rounds</u>
CRYPTON	12
Rijndael	10,12,14
SAFER+	8,12,16
SERPENT	32

TVOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

Other Algorithms

<u>Algorithm</u>	<u>Rounds</u>	<u>Type</u>
FROG	8	Key Interp.
HPC	8?	Omni

TVOFISH
SERPENT
SAFER+
BUNDAEL
RC6
MARS
MAGENTA
LOH197
HPC
FROG
E2
DPC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFER+
BUNDAEL
RC6
MARS
MAGENTA
LOH197
HPC
FROG
E2
DPC
DEAL
CRYPTON
CAST-256

Cryptanalysis

- LOKI97
 - Rijmen and Knudsen
 - Differential: 2^{56} chosen plaintexts
 - Linear: 2^{56} known plaintexts
- FROG
 - Wagner, Ferguson, and Schneier
 - Differential: 2^{58} chosen plaintext
 - Linear: 2^{56} known plaintexts

TVOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Cryptanalysis

- Magenta
 - Biham, Biryukov, Ferguson, Knudsen, Schneier, Shamir
 - 2^{64} chosen plaintexts, 2^{64} steps
 - 2^{33} known plaintexts, 2^{97} steps
- DEAL
 - Lucks
 - 2^{70} chosen plaintexts

TVOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOH97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFEPR
BLINDAEL
RC6
MARS
MAGENTA
LOH97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

Other Factors

- Provable security against classes of attacks (DFC)
- Cost/Efficiency
 - Software
 - Hardware
- Architectures 8/32/64 bits
- Intellectual Property

TRIVIAL
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TRIVIAL
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

Next Steps

- NIST to establish informal discussion group at www.nist.gov/aes for each candidate
- Public review of candidates, Aug. 20 - April 15, 1999
- Submissions of analysis for AES2, Feb 1, 1999
- Second AES conference, March 22-23, 1999
- Formal submissions of analysis for Round 1, April 15, 1999
- Announcement of (about) five finalists
- Public Review of finalists, 6-9 months
- Third AES Conference
- Selection of AES Algorithm
- Making AES a FIPS

TV0FISH
SERPENT
SAFE+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TV0FISH
SERPENT
SAFE+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

Formal Comments Requested

- How well algorithms meet criteria
 - Security, Cost, and Implementation Characteristics
- Any related intellectual property
- Cross-cutting analysis of multiple algorithms
- Overall recommendations and rationale
- e-mail: AESFIRST_ROUND@nist.gov

TVOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFER+
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256

AES

Second AES Candidate Conference

TV0FISH
SERPENT
SAFEPR
BLINDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TV0FISH
SERPENT
SAFEPR
BLINDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

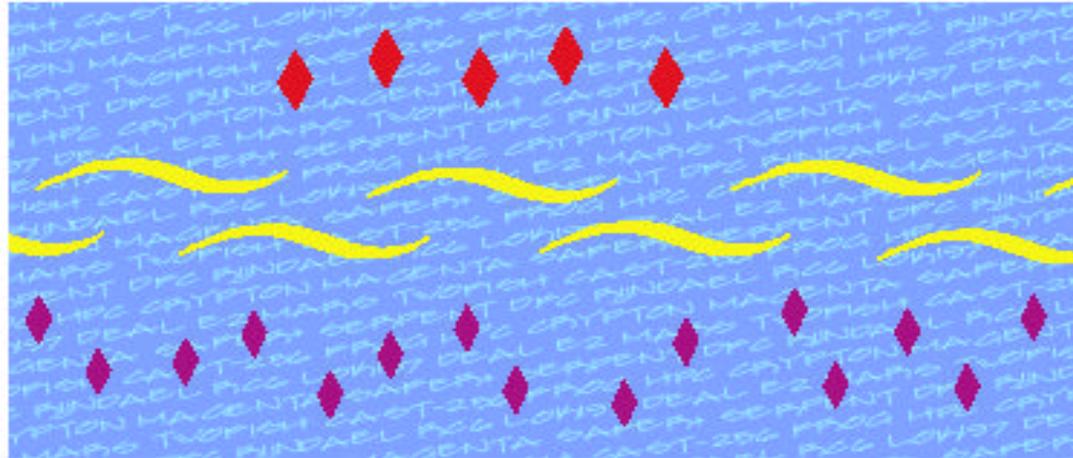
Rome, Italy

March 22-23,
1999



AES

A Crypto Algorithm for the Twenty-first Century . . .



THE SECOND
ADVANCED ENCRYPTION STANDARD
CANDIDATE CONFERENCE

MARCH 22-23, 1999

HOTEL QUIRINALE
ROME, ITALY

SPONSORED BY:
INFORMATION TECHNOLOGY LABORATORY
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

TVOPISH
SERPENT
SAFE
BUNDAEL
PCG
MAGS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TVOPISH
SERPENT
SAFE
BUNDAEL
PCG
MAGS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

Issues/Questions



TVOFISH
SERPENT
SAFEPR
BUNDAEL
PCG
MAGS
MAGENTA
LOH97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFEPR
BUNDAEL
PCG
MAGS
MAGENTA
LOH97
HPC
PROG
E2
DFC
DEAL
CRYPTON
CAST-256