





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

Status of the Advanced Encryption Standard (AES) Development Effort

Jim Foti
jfoti@nist.gov

October 6, 1998 Security Technology Group **NIST**



AES

- Future Government crypto standard - successor to DES
- NIST is relying on public participation:
 - algorithm proposals
 - cryptanalysis
 - efficiency testing

2



Goals of the AES effort

- Symmetric, block cipher with variable key size (128, 192, 256), and large (128-bit) block size.
- More secure and efficient than TripleDES.
- Royalty-free worldwide.
- Security for >30 years.
- Public confidence in AES algorithm, based on involvement in submission and analysis efforts.

3



Selecting the Candidates

- Twenty-one algorithms submitted to NIST
- NIST verified:
 - minimum criteria met
 - all required items included/addressed
 - required legal statements included
 - code operating correctly
- Six incomplete packages
- No cryptanalysis performed

4

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

(* placed in the public domain)

5

Candidate Algorithms, cont'd

- **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

(* placed in the public domain)

6



AES1 Conference Review

- August 20-22, 1998; Ventura, CA
- ~200 attendees (30 nations)
- Formal presentation of candidate algorithms and design philosophies
- Distributed Alg. Documentation on CD-ROM
- Discussion
- Kick-off of Round 1 Technical Analysis

7



Initial Observations

- Some variants of existing ciphers
- Traditional & modified Feistel networks
- “Conservative” vs. “Unorthodox” designs
- Provable security claimed against certain attacks

8

Next Steps

- Round 1: *Aug. 20 - April 15, 1999*
- Submit papers for 2nd AES conference: *Feb 1, 1999*
- Second AES conference: *March 22-23, 1999*
- Announcement of (about) five finalists
- Round 2 analysis of finalists: *6-9 months*
- Third AES Conference
- Selection of AES Algorithm
- Make the AES a FIPS

13





Challenges

- Defining requirements - striking a balance
- APIs for algorithm code
- Complying with export regulations
- Selecting candidates & preparing CDs
- Efficiency analysis - fair comparisons
- Picking Round 2 finalists and winner

15



For more information. . .

- AES Home Page:
<http://www.nist.gov/aes>
 - Request copies of CD-ROMs
 - Participate in AES Forum for informal discussions
 - Pointers to analysis & testing papers on WWW
 - Provide NIST with official e-mail comments
 - Info on future conferences/deadlines
 - Copy of this presentation

16