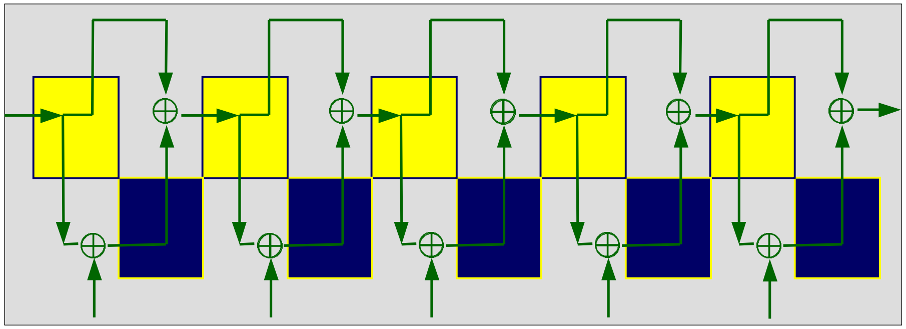
AES

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



Miles E. Smid

NIST

msmid@nist.gov

U.S.A.

Fast Software Encryption Workshop, March 24, 1998

NIST Philosophy

- Strong, publicly specified cryptographic standards and specifications are needed
- Government must work with commercial standards setting organizations and the cryptographic community for security, interoperability, and assurance
- Quality commercial security products is the goal

What are we looking for?

- Very strong symmetric block cipher for government and commercial use in the next century
- More efficient than Triple DES
- More secure than Triple DES
  - Key sizes: 128, 192, 256
  - Block sizes: 128 (64, 256, and others optional)
- Publicly Defined and Evaluated
- Worldwide royalty-free

What has been done so far?

- Announcement of intent to develop AES and request for comments, January 2, 1997
- Workshop on proposed requirements and procedures, summary of comments, April 15, 1997
- Informal draft requirements and procedures, June 16, 1997
- Formal call for candidate algorithms, Sep. 12

What are the next steps?

- Deadline for “pre-review” April 15, 1998
- Results of pre-review, May 15, 1998
- Close of call, June 15, 1998
- August 20-22, 1998, Presentation of candidates at First AES Conference
- Public review of candidates
- Second AES Conference, presentations of results of testing and analysis (6-9 months after first conference)
- Announcement of five (or less) candidates
- Public review of finalists
- Third AES Conference, presentation of results of testing and analysis (6-9 months after second conference)

How will the AES be Selected?

- The most open process yet
- Public input on selection criteria
- Public comments requested three separate times on algorithms:
    - all candidates
    - five (or less) semifinalists
    - finalist(s)
- Recommendation to Secretary of Commerce

Evaluation Criteria

- Security
  - Actual Security
  - Random permutation properties
  - Mathematical basis
  - Other security factors raised
- Cost
  - Computational efficiency
  - Memory requirements (hardware and software)

Criteria Continued

- Algorithm and Implementation Characteristics
  - Flexibility
  - Hardware and software suitability
  - Simplicity of design
- Other Aspects
  - Efficiency and Reference Implementations (available to the public for evaluation)
  - Sponsors to present and defend algorithms

Summary of AES Process

- Anyone can submit a candidate algorithm
- Anyone can test candidate algorithms
- Anyone can evaluate candidates
- This process requires PUBLIC participation
- To follow what is going on with AES, visit
  http://csrc.nist.gov/encryption/aes/aes_home.htm

Potential AES Contributors

- Both US and Foreign contributions welcomed
- Initial interest expressed as follows:

Country	**Academic**	**Company**
Australia	1	
Belgium		1
Canada		1
France	1	
Netherlands		1
Russia		1
US	2	7
Multi-nation	1	

TOTAL = 16

Responses to Latest Request

Country	**Academic**	**Company**
Australia	1	
Belgium		2
Canada		1
France	1	
Japan		1
Netherlands		1
US		5
Multi-nation	1	
Known Fence Sitter		1

TOTAL = 14

Playing the AES Game is Much Better than Playing the Lottery!

Current Odds of Winning = Approximately 1:14

(and We Still Need Evaluators)

See You In August!

- The First AES Candidate Conference
- Purpose: AES Candidates Announced & Contributors will brief their algorithms
- Dates: August 20-22, 1998 (Before Crypto)
- Location: Ventura, CA
- On-line Registration: http://www.nist.gov/public_affairs/confpage/980820.htm
- Conference contact: Lori Phillips, NIST, 301/975-4513, lori.phillips@nist.gov