Advanced Encryption Standard (AES):

Selection and Plans

http://www.nist.gov/aes/

October 16, 2000

Jim Foti

NIST

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Jim’s Alternate Title:

Thank Goodness That Part of the Process is Over With!!!

Today's Briefing

- Third AES Conference
- Analysis
- Selection Steps
- AES Proposal
- Next Steps
- Related Efforts

“Royal Rumble”

MARS
RC6™
Rijndael
Serpent
Twofish

Springtime in New York…

- Third AES Conference (April 2000)
- Discussion of Round 2 Analysis
  - Security Analysis
  - Hardware performance
  - Multiple vs. Single Algorithms
- Submitters made the case for their algorithms.

Comments, Comments, Everywhere...

- Round 2 comment period closed (May 15)
- Public comments:
  - More than 160 comments/papers, consisting of 800+ pages of material
- Contradictions, different assumptions, different results…
- NIST AES team read and considered all comments.

Selection Preliminaries

- *Ad hoc* NIST AES selection team.
- Issues:
  - Selection approach
    - Qualitative, not Quantitative.
  - How many algorithms to choose?
  - Backup algorithm?
  - (Not) Modifying the algorithms
- Goal: evaluate algorithms & write report

Evaluation Criteria

- Security.
- Software & Hardware Performance.
- Suitability in Restricted-Space Environments.
- Resistance to Power Analysis & other implementation attacks.
- Intellectual Property.
- Others...

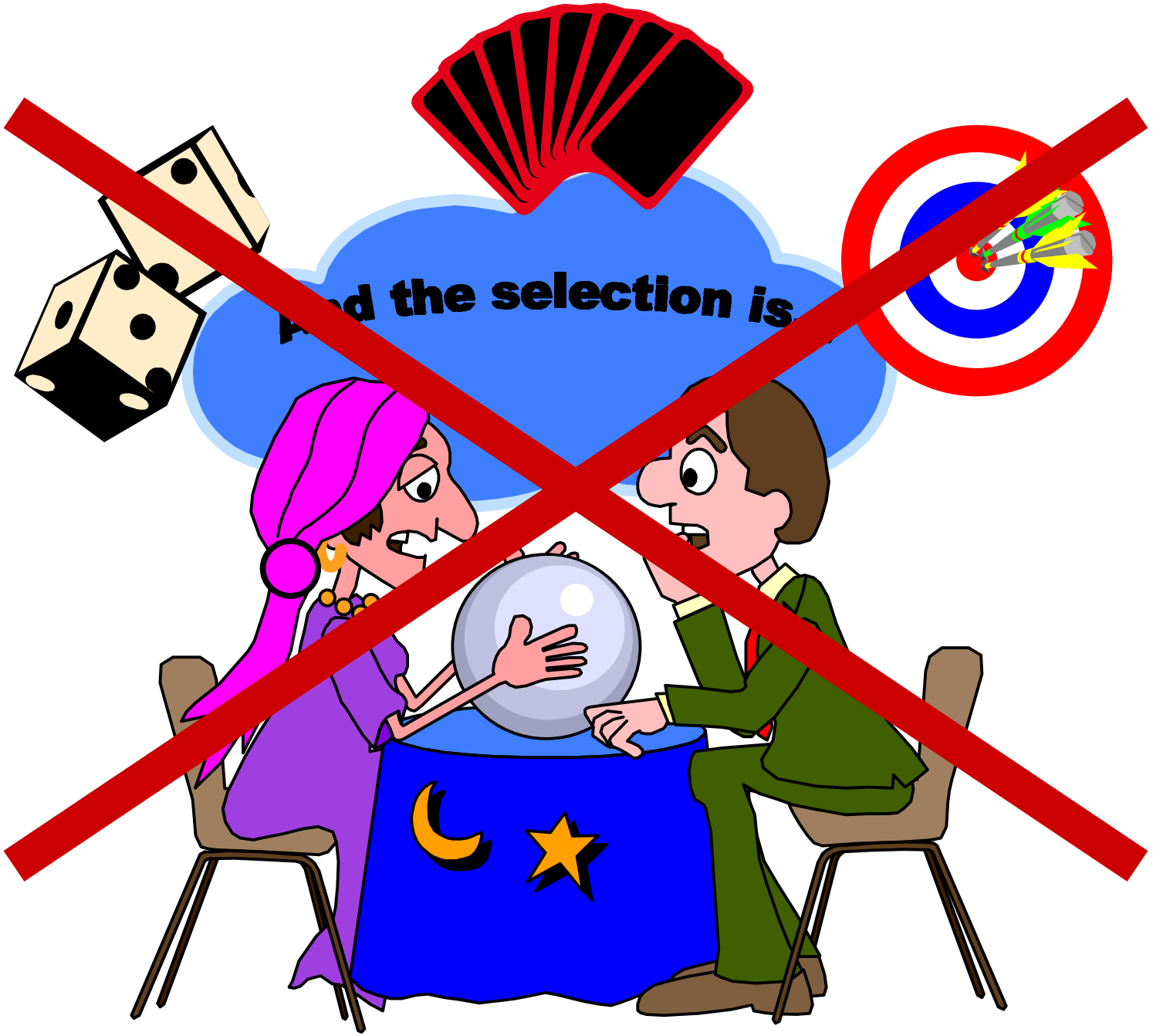
Meeting(s) of the minds...

- Criterion-by-criterion discussion of the algorithms.
- Simultaneous drafting of the report.

- Always in Mind: Fairness, Objectivity
- Consider the data, then select the algorithm AT THE END!

Assessing the Algorithms...

- Compared algorithms in each criterion “area”.
- All five appear to have adequate security for the AES. (No known attacks.)
- Intellectual Property - no role in the selection.
- Which algorithm appears to be the best selection, OVERALL?


d the selection is

Rijndael

submitted by Joan Daemen & Vincent Rijmen

"When considered together, Rijndael's combination of security, performance, efficiency, implementability, and flexibility make it an appropriate selection for the AES."

“A”-Day Arrives

- October 2, 2000
  - Press conference at NIST
  - Publish “Report on the Development of the Advanced Encryption Standard (AES)”
  - AES Questions & Answers

  - http://www.nist.gov/aes/

Is It Over Yet???!!!

- Draft AES standard
  - Nov. 2000
- 90-day public comment period
  - Nov. 2000 - Feb. 2001
- Approval by Secretary of Commerce
  - April-June 2001 ???
  - AES becomes “Official”
- Validation testing for AES
  - Cryptographic Module Validation Program (CMVP)

AES on the Move

- ANSI X9F Financial Standards
- ISO New Work Item for Encryption Algorithms
- IETF… (coming soon)