Future Plans for the AES

Miles Smid

End of Round 1

- Comment period for Round 1 closes April 15.
- ALL OFFICIAL COMMENTS MUST BE SENT TO <AESFirstRound@nist.gov>.
- On April 19, all official public comments on the AES will be posted on the AES Home Page.

2

Formal "Tweaks"

- Original request for algorithms addressed the issue of "tweaks":
  - Minor adjustments to an algorithm, to correct small deficiencies identified in Round 1.
  - Should not invalidate majority of Round 1 analysis for that algorithm.
  - Allowed, but not required.
  - No substantial redesigns .

3

Submitting Tweaks

- Minor adjustments to algorithm (OPTIONAL)
- "Tweak" proposals:
  - May 15, 1999 deadline
  - Algorithm submitters who propose tweaks to NIST must include:
    - ❶ Summary of proposed modifications;
    - ❷ Justification for changes;
    - ❸ Identification of any papers or comments that discussed the specific weakness(es) being addressed;
    - ❹ Updated algorithm specification that incorporates the tweak.

4

Transition to Round 2

- NIST will select the finalists, based on the following information:
  - Official Round 1 versions of the algorithms;
  - Official Comments received;
  - Results of AES2 presentations & discussions;
  - NIST analysis of algorithms;
  - Allowed tweaks;
  - Other pertinent information.

5

Announcement of Finalists

- Mid-summer 1999.
- Notification of Finalists several days prior to official announcement.
- NIST press release, and announcement on AES Home Page.
- Justification of Selection, and Specifications of Finalists will be available immediately on AES Home Page.

6

Round 2

- Begins when NIST announces finalists.
- Any updated / additional optimized code for finalists must be submitted to NIST within ONE MONTH of start of Round 2.
- CD-ROMs with code and specs shall be distributed 2-3 months after start of Round 2.
  - Automatically send to everyone who received CD-2 (with code) in Round 1;
  - On-line request form.

7

Round 2

- Proposed analysis:
  - Continued Cryptanalysis,
  - Efficiency testing of 192- and 256-bit key sizes,
  - Performance of submitted code on 64-bit processors,
  - Hardware performance estimations, and
  - Continued Intellectual Property research,
  - Additional analysis.

8

Timeline Summary

- **April 15, 1999**: Round 1 Comment period closes.
- **May 15, 1999**: Explanation/justification of proposed "tweaks", and updated spec. are due.
- **Summer 1999**: Announcement of Finalists.
- **Announcement of Finalists + 1 month**: Updated code for Round 2 is due.
- **January 15, 2000**: Papers due for AES3.
- **Week of April 10, 2000**:AES3 (New York City)
- **May 15, 2000**: Round 2 Comment period closes.
- ~**August 2000**:

  Announcement of AES Winner(s)

9

Remaining Questions ?

10

Last Reminder!

- OFFICIAL COMMENTS are due April 15
- Submit to:
  <AESFirstRound@nist.gov>
- Please comment on information that was discussed here in Rome!

11

A Special "Thank You"

12

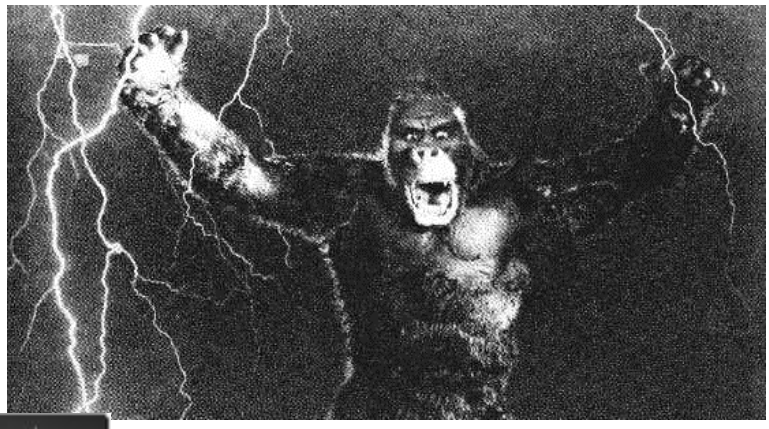
GRAZIE!

- Speakers
- Program Committee
- Algorithm Submitters
- FSE (Tomorrow)
- Lars Knudsen
- NIST Staff & Hotel Staff
- Attendees

13

Attendee Feedback Form

14



“Start spreadin’ the news…”

We’ll see you at AES3 in New York City!

15