Welcome to AES3

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

Conference Logistics

- Lunches, Tonight's Reception:
  - **Regent Parlor**
- Tomorrow's Sessions:
  - Located in **Sutton Center/Sutton South**
- Questions?
  - Please ask NIST staff at the Registration Desk.
- Audiotaping
- Press

2

Where are we now?

- Round 2 analysis period.
- Round 2 public comments must be submitted to NIST by **May 15, 2000**.
- After Round 2 ends, NIST will analyze comments and select the algorithm(s) for the AES standard.

3

Round 2 Comments

- Posted bi-weekly at **www.nist.gov/aes**
- Mail to: **AESround2@nist.gov**
- Comments are welcome regarding the papers and discussions at AES3 and FSE2000. NIST needs this feedback.

4

Fast Software Encryption 2000

- Abstracts for AES-related papers are located at the front of the AES3 Proceedings.

5

AES3 Conference

- Last of three conferences for the AES development effort.
- Final opportunity for global crypto community to gather and discuss Round 2 analysis before NIST's selection.

6

AES3 Program Committee

• Tom Berson	*Anagram Laboratories*
• Dennis Branstad	*Consultant with TIS Labs*
• Craig Clapp	*PictureTel Corp.*
• Morris Dworkin	*NIST* (and NIST Staff)
• Susan Langford	*Certicom*
• Stefan Lucks	*Universität Mannheim*
• Tim Moses	*Entrust Technologies*
• Miles Smid	*CygnaCom Solutions*
• David Solo	*Citigroup*

7

Conference Goals

- Presentation of Round 2 Analysis;
- Discussion of Relevant Issues; and

- Provide NIST with a clearer understanding of which candidate algorithm(s) that NIST SHOULD or SHOULD NOT select for the AES standard.
  - "FIPS" - Federal Information Processing Standard

8

Main Issues to be Addressed

- Security
  - Cryptanalysis
- Efficiency
  - Hardware performance (FPGA, ASIC, DSP)
  - Software performance (various platforms)
- Flexibility
  - Implementations in various environments.
- Number of algorithms / Modes of operation

9

Conference Sessions

- Day 1
  - FPGA Evaluations
  - Platform-Specific Evaluations
  - Surveys
  - Cryptographic Analysis and Properties
  - Rump Session
    - Title and Presenter - in writing to Jim by 2:00 this afternoon

10

Sessions, continued

- Day 2
  - Cryptographic Analysis and Properties
  - "AES Issues" Panel
  - ASIC Evals. / Individual Alg. Testing
  - Algorithm Submitter Presentations *(handout)*
  - Discussion, Q&A

  - Future Schedule for the AES

11

Post-Conference Evaluations

- Optional questions to answer on the evaluation forms.
- Questions to keep in mind:
  - Which algorithm(s) SHOULD and SHOULD NOT be included in the standard?
  - How many algs. should be selected?
  - If multiple algs. are selected, then which algs. should be matched together?
- Will be distributed after last coffee break.
- Results posted on AES home page next week

12