SHA-3 Strategies and Timeline

Bill Burr
Manager, Cryptographic Technology Group
Computer Security Division
National Institute of Standards and Technology
August 2010

NIST's Mission

- To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology …

©Robert Rathe

©Geoffrey Wheeler

… in ways that enhance economic security and improve our quality of life.

NIST
National Institute of Standards and Technology

SHA-3 Timeline

- ✓ 1Q07 draft submission criteria published
- ✓ 11/2/07 Federal Register announcement
- ✓ 8/31/08 Preliminary submissions due
- ✓ 10/31/08 Final submissions due
- ✓ 02/25/09 First Candidate Conference, Leuven Belgium
- ✓ 3Q09 Select 14 second round candidates
- ✓ 3Q10 Second Candidate Conference
- 4Q10 Announce finalist candidates
- 1Q11 Final tweaks of candidates
- 1Q12 Last Candidate Conference
- 2Q12 announce winner
- 4Q 12 FIPS package to Secretary of Commerce

For the next round

- If you’re going to tweak your submission, have the specification with the tweaks ready by the end of the year.
- A big change may hurt you – if you make it the finals there was a lot we liked.
  - Some tweaks may be a response to analysis, but if you made the final five in part because there has been a lot of analysis that didn’t get very far…
- Be specific about which variants you are proposing
  - Fewer variants is better