The First SHA-3
Candidate Conference

System Priorities

Donna F Dodson

donna.dodson@nist.gov

February 26, 2009

SHA-3 needs to meet the requirements of….

- Cryptographers,
- Security Engineers,
- Protocol Mechanics and Developers,
- Product Implementers,
- Standards Developers.

Established Application Criteria for SHA-3

- SHA-3 will support:
  - Digital signatures,
  - Key derivation,
  - HMAC,
  - DRBGs.
- Are there other important applications?

What other attributes are required for acceptance and use of SHA-3?

- Security
- Application compatibility
- Platform suitability
  - Efficiency
  - Processing Environments
  - Power Consumption

Example Application Contexts

- Networking Infrastructure Components (e.g., routers)
- Embedded Systems
- Smart Cards
- Personal Networking Devices
- Sensors
- Others?

Example Performance and Implementations Tradeoffs

- Gate counts
- Dependence of Hash performance on hardware
- Storage requirements
- Parallelizability
  - SIMD
  - MIMD
- Others?

Q and A

- Are there other applications for SHA-3 that should be considered?
- What are the application contexts that SHA-3 needs to support, and why?
- What platforms are most important and why?
- What application contexts and platforms are less important and why?
- Are there particular systems that are challenging for a multi-purpose hash standard?
- List critical attributes needed for acceptance of SHA-3.