NIST's Cryptographic Toolkit (of Standards and Recommendations)

Elaine Barker

November 8, 2011

ebarker@nist.gov

Block Ciphers

- FIPS 197: AES
  - The result of a multi-year, world-wide competition
- SP 800-67: TDEA
  - A “mode” of the original FIPS 46 (DES)

Block Cipher Modes

- SP 800-38A: AES & TDEA encryption (ECB, CBC, OFB, CFB, CTR)
- SP 800-38B: AES & TDEA authentication (CMAC)
- SP 800-38C: AES authenticated encryption (CCM)
- SP 800-38D: AES authentication and encryption (GCM & GMAC)
- SP 800-38E: AES encryption for storage devices (XTS-AES)
- SP 800-38F: (Draft) AES and TDEA key wrapping

- Under development: Format Preserving Encryption

Digital Signatures

- FIPS 186-3: DSA, ECDSA, RSA
- SP 800-89: Assurances for digital signature generation
- SP 800-102: Digital signature timeliness

Key Management

- Key Management
  - SP 800-57, Part 1: General key mgmt. guidance
  - SP 800-57, Part 2: Best practices for key mgmt. organizations
  - SP 800-57, Part 3: Application-specific key mgmt. guidance (currently revising to include SSH and TPMs)
  - SP 800-131A: Transitioning the Use of Cryptographic Algorithms and Key Lengths
  - SP 800-130: A Framework for Designing Cryptographic Key Management Systems
  - SP 800-152: Profile of SP 800-130 for the Federal govt.

Key Management (Contd.)

- Key Establishment
  - SP 800-56A: Finite field and elliptic curve Diffie-Hellman & MQV key agreement schemes
  - SP 800-56B: RSA key agreement and key transport schemes
  - SP 800-56C: Key derivation using extraction-then-expansion
  - SP 800-108: Key derivation from a shared key
  - SP 800-132: Password-based key derivation for storage applications
  - SP 800-133: Cryptographic key generation
  - SP 800-135: Application-specific key derivation functions

Message Authentication

- SP 800-38B: CMAC (AES and TDEA)
- SP 800-38 D: CCM (AES)
- SP 800-38:; GMAC
- FIPS 198-1: Keyed-hash message authentication
- Digital signatures: DSA, ECDSA and RSA

Hash Functions

- FIPS 180-3/4: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
- SHA3: Hash competition nearing completion
  - BLAKE, Grøstl, JH, Keccak, and Skein
  - SHA3 final conference: March 22-23, 2012
  - Decision about June, 2012?
- SP 800-107: Applications using approved hash algorithms (digital signatures, KDFs, HMAC, random bit generation)
- SP 800-106: Randomized hashing for digital signatures

Random Number Generation

- SP 800-90A: Deterministic random bit generation mechanisms (aka pseudorandom number generators)
- SP 800-90B: Entropy sources
- SP 800-90C: Random bit generator constructions
- FIPS 186-2: DSS specifies/adopts SHA-1 and TDEA RNGs

For More Information

- Web sites:
  - FIPS and SPs: http://csrc.nist.gov/publications/
  - SHA3: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

- Contacts:
  - Elaine Barker: ebarker@nist.gov
  - Lily Chen: llchen@nist.gov
  - Shujen Chang: sjchang@nist.gov
  - Quynh Dang: qdang@nist.gov
  - Morris Dworkin: morri@nist.gov
  - Tim Polk: william.polk@nist.gov