NIST
Cryptographic Toolkit

Elaine Barker
ebarker@nist.gov

National InformationSystem Security Conference
October 16, 2000

1901-2001
NIST CENTENNIAL

Toolkit Purpose

- The NIST Cryptographic Toolkit will provide Federal agencies, and others who choose to use it, with a comprehensive toolkit of standardized cryptographic algorithms, protocols, and security applications that they can use with confidence to protect sensitive information.

Commercial Off-The-Shelf

✓ Agencies can’t afford special government cryptographic products

✓ Government needs are sometimes more severe than ordinary commercial needs

  – Many users look to government to set cryptographic standards

  – Adopt industry standards wherever possible

  – Work with industry to encourage strong, high assurance cryptographic products

Industry Participation

- ✓ NIST working with industry to develop a toolkit of high quality cryptographic algorithms
- ✓ Industry interaction & participation
  - – Participate in voluntary standards bodies
  - – Review draft FIPS
  - – AES workshop & participation
  - – Key Management workshop
  - – Modes of Operation Workshop
  - – Algorithm and Cryptographic Module Validation via CMVP

NIST Cryptographic Toolkit

- ✓ Encryption
- ✓ Encryption modes
- ✓ Authentication
- ✓ Hashing
- ✓ Digital Signatures
- ✓ Key Management
- ✓ Random Number Generation
- ✓ Prime Number Generation

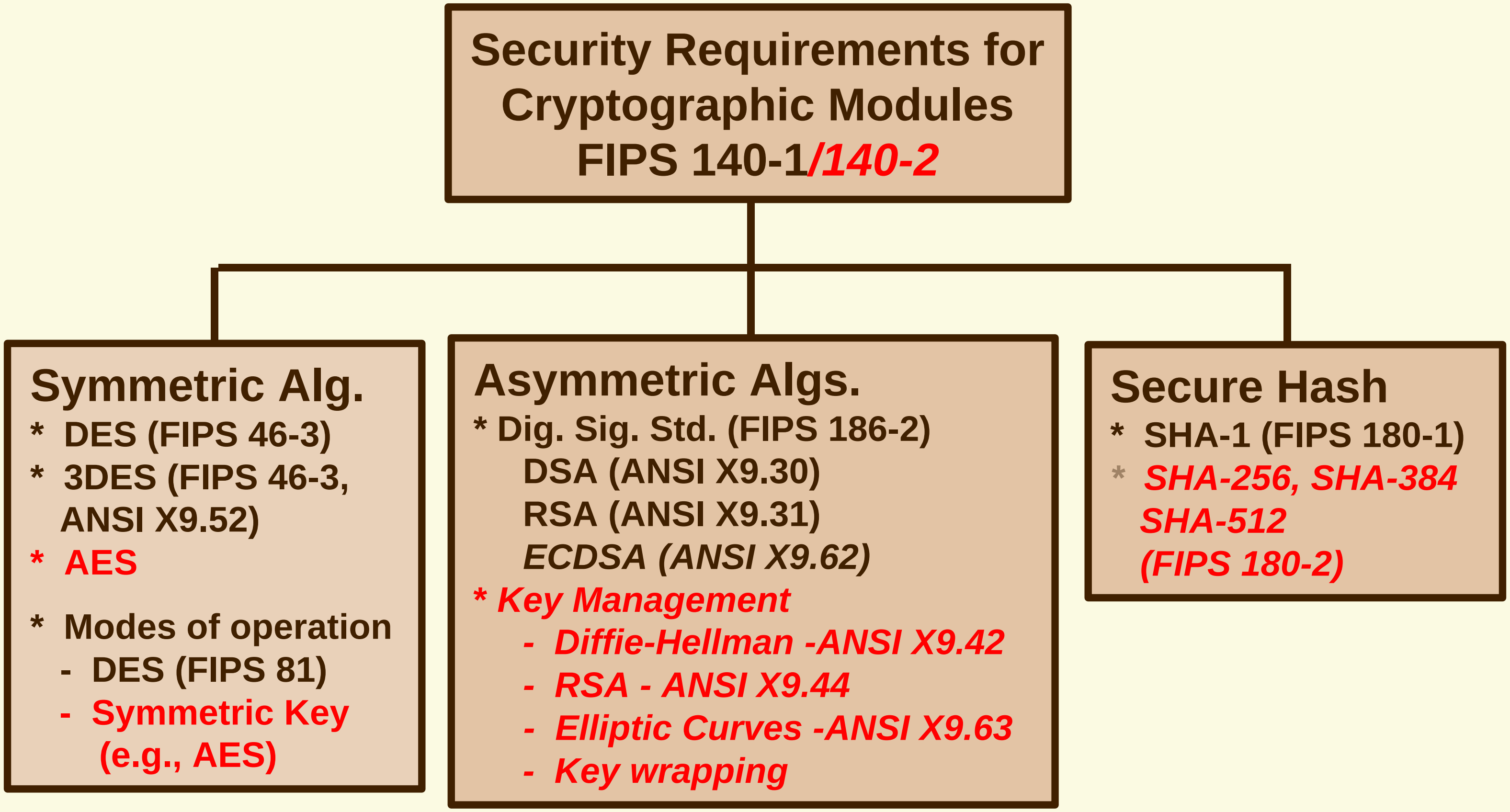
NIST Cryptographic Toolkit

✓ Standardized algorithms
  - Federal Information Processing Standards
  - Often based on ANSI or other voluntary standards
  - Confidence they are secure
    - now and for foreseeable future
  - Wide range of applications
  - Assurance testing
    - Cryptographic Module Validation Program (CMVP)

Algorithm Categories

- ✓ Symmetric (secret key cryptography)
  - Encrypt and decrypt using same key
- ✓ Asymmetric (public key cryptography)
  - Two related keys: one public, other private
  - Mainly used for signatures & key establishment
- ✓ Hashing
  - Compute a “cryptographic checksum” or “message digest” of messages or files
  - Used for integrity, authentication & signatures

Cryptographic Standards



Security Requirements for Cryptographic Modules FIPS 140-1/*140-2*

Symmetric Alg.

- * DES (FIPS 46-3)
- * 3DES (FIPS 46-3, ANSI X9.52)
- * AES
- * Modes of operation
  - - DES (FIPS 81)
  - - Symmetric Key (e.g., AES)

Asymmetric Algs.

- * Dig. Sig. Std. (FIPS 186-2)
  DSA (ANSI X9.30)
  RSA (ANSI X9.31)
  ECDSA (ANSI X9.62)
- ** Key Management*
  - *- Diffie-Hellman -ANSI X9.42*
  - *- RSA - ANSI X9.44*
  - *- Elliptic Curves -ANSI X9.63*
  - *- Key wrapping*

Secure Hash

- * SHA-1 (FIPS 180-1)
- * *SHA-256, SHA-384 SHA-512 (FIPS 180-2)*

FIPS Approved Crypto Algorithms

- ✓ Approved for US Government use
  - sensitive/unclassified
- ✓ Subject to 5 year NIST Reviews
- ✓ Analyzed for strength of security
- ✓ Have validation tests & program
- ✓ Coordination / cooperation with voluntary standards bodies
  - ANSI X9F (banking standards body)
  - IETF (major developer of standard apps that use crypto)

FIPS 140-1/2

- Joint program with Canadian Security Establishment
- Umbrella standard for Crypto FIPS
- Validation testing for algorithms & Crypto Modules
  - Four independent private testing laboratories
    - this number may grow
    - National Voluntary Laboratory Accreditation (NLVAP) accreditation
- Big increase in validations since 1999
  - About 120 validated modules to date
- Update (FIPS 140-2) waiting for SoC signature

Data Encryption Standard (DES)

- ✓ FIPS 46-3
- ✓ In wide use
  - First open standard for strong crypto
  - "Kickstarted" open, public discussion and development of cryptographic algorithms
  - Benchmark for everything that has come after
- ✓ 64 bit block
- ✓ 56 bit keys
  - More than 2 decades old
    - now vulnerable to attack by key exhaustion
      - should be moving to Triple DES
    - otherwise still a good algorithm

–

DES Modes of Operation

- ✓ FIPS 81
- ✓ Four modes defined
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
    - can be used for Message Authentication Code (MAC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
- ✓ Uses 64-bit blocks
- ✓ 56 bit keys

Triple DES

- ✓ FIPS 46-3 and ANSI X9.52
- ✓ 64 bit block size
- ✓ 112 and 168 bit keys
  - – DES repeated 3 times with 2 or 3 different keys
- ✓ Strong protection
- ✓ Easy substitution for DES
  - – Main difference is bigger key size & slower performance
- ✓ Expands 4 DES modes into 7 modes

Advanced Encryption Standard (AES)

- ✓ DES replacement
- ✓ Selected through open competition run by NIST
  - Public evaluation and analysis
  - 21 original submissions, 5 “finalists”
  - Final selection of Rijndael announced Oct. 2, 2000
  - http://www.nist.gov/aes
- ✓ Strong encryption with long expected life
  - 128 bit block size
  - 128, 192, & 256 bit key sizes
- ✓ Goal: royalty free worldwide

Modes of Operation for Symmetric Key Block Ciphers

- ✓ Plan to parameterize 4 DES Modes
  - Could be used with any block encryption algorithm
- ✓ Other modes???
  - Counter
  - MAC
  - Modes combining integrity, authentication & encryption
  - Interleaved CBC
  - Super-encryption (e.g., Triple AES?)
- ✓ Workshop on October 20 (this Friday)
  - http://www.nist.gov/modes)

SHA-1

- Secure Hash Algorithm
- FIPS 180-1; ANSI X9.30 Part 2
- 160 bit message digest
- Wide current use
  - Used with DSA, RSA or ECDSA

SHA-xxx

- ✓ "Birthday" attacks against a hash make make *n*-bit AES and a 2*n*-bit hash roughly equivalent
  - – 128-bit AES ≈ SHA-256
  - – 192-bit AES ≈ SHA-384
  - – 256-bit AES ≈ SHA-512
- ✓ Available at http://www.nist.gov/sha
- ✓ Draft standard available ~ February

Message. Authentication Code (MAC)

- ✓ Current DES-MAC
  - – FIPS 113 & FIPS 81
    - Cipher Block Chaining (CBC)
  - – 64-bit MAC
    - 2^{32} work factor for birthday attacks
      - – Not now strong enough for many applications

MAC (contd.)

- ✓ HMAC
  - – Generalization of RFC 2104 and ANSI X9.71
    - concatenate secret key and message
    - allow different FIPS-approved hash functions and sizes
  - – Soon available for public comment
- ✓ AES MAC Needed???
  - – Modes workshop issue

Digital Signature Std. (DSS)

- ✓ FIPS 186-2
  - Three algorithms
    - DSA (ANSI X9.30 Part 1)
    - RSA (ANSI X9.31)
      - transition period from PKCS#1
    - ECDSA (ANSI X9.62)
  - Use SHA-1 message digest

DSS Plans

- ✓ Planned modification of FIPS 186-2 → 186-3
- ✓ Need to expand key sizes
  - – DSA now limited to 1024 bits
  - – 128-bit AES roughly as strong as 3000 bit DSA
  - – 1024 bit DSA roughly as strong as 160-bit SHA-1
  - – SHA 256, SHA 384 & SHA 512
- ✓ Allow PKCS#1 (RSA)?
- ✓ Draft available ~ February 2001

Other Areas for New Crypto FIPS

- ✓ Prime Number Generation
  - ANSI X9.80
- ✓ Random Number Generation
  - ANSI X9.82
  - NIST RNG tests (http://csrc.nist.gov/rng)

Key Management

- ✓ Key Management = Key establishment + rules (including protocols)
- ✓ Key establishment = Key Agreement + Key Transport
- ✓ Key Agreement: no key sent; uses asymmetric/public key techniques
- ✓ Key Transport: encrypted key is sent; uses symmetric or public key techniques

Key Management (contd.)

- ✓ No current FIPS using public key techniques
- ✓ Workshop held Feb. 10 - 11, 2000
- ✓ Multi-level approach
  - – Framework document to lay out approach
  - – Key establishment schemes
  - – Rules/guidance/protocols

Key Management (contd.)

- ✓ Draft FIPS in early FY2002?
  - – ANSI X9.42, DH and MVQ Key Agreement
  - – ANSI X9.44, Factoring Based (e.g., RSA) Key Agreement & Transport
  - – ANSI X9.63, EC Key Agreement & TransportKey wrapping
  - – Key wrapping
- ✓ http://www.nist.gov/kms

Conclusion

✓ NIST is building a comprehensive cryptographic toolkit
  - strong security
  - assurance & validation testing
  - suitable for commercial use and COTS products
  - encourage industry participation

Further Information

- **NIST Computer Security Division Home Page**

  http://www.itl.nist.gov/div893/

- **Points of Contact**

Bill Burr	**wburr@nist.gov**
FIPS 140: Ray Snouffer	**rsnouffer@nist.gov**
Crypto stds.: Elaine Barker	**ebarker@nist.gov**