# *Developing the NIST Cryptographic Standards Toolkit*

Ed Roback

Chief, Computer Security Division

edward.roback@nist.gov

NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's primary mission is to promote economic growth by working with industry to develop and apply technology, measurements, and standards.

NIST carries out its mission through a portfolio of four programs:

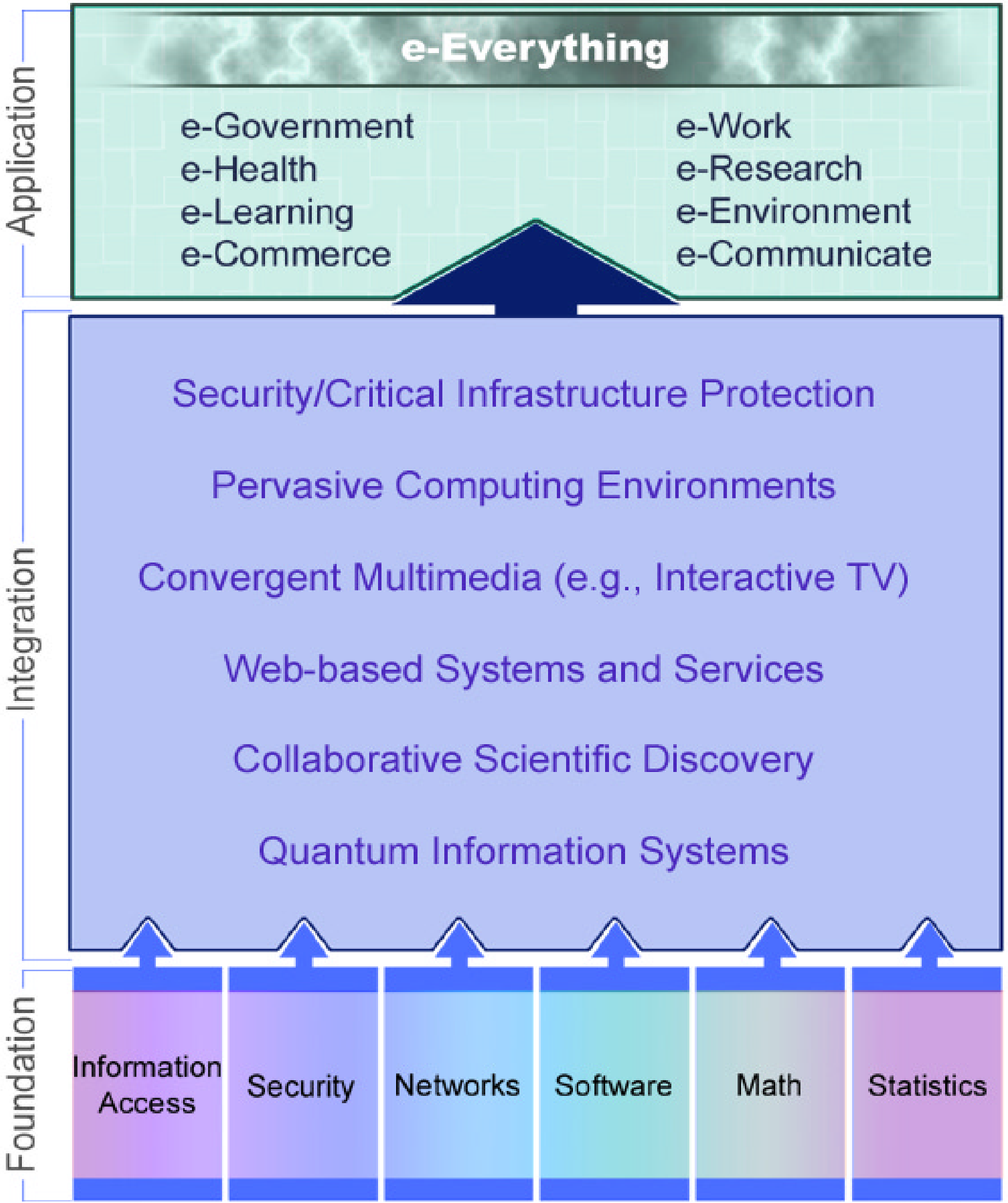
**Measurement and Standards Laboratories** provides technical leadership for the Nation's measurement and standards infrastructure, and assures the availability of essential reference data and measurement capabilities

**Advanced Technology Program** stimulates U.S. economic growth by developing high risk and enabling technologies through industry-driven cost-shared partnerships

**Manufacturing Extension Partnership** strengthens the global competitiveness of smaller U.S.-based manufacturing firms by assisting in the adoption of advanced technologies, techniques, and business practices

**National Quality Program** enhances U.S. competitiveness, quality, and productivity, manages the Malcolm Baldrige National Quality Award, and provides global leadership in promoting quality awareness

# NIST/ITL - ENABLING A BETTER FUTURE



Application

e-Everything

e-Government
e-Health
e-Learning
e-Commerce

e-Work
e-Research
e-Environment
e-Communicate

Integration

Security/Critical Infrastructure Protection

Pervasive Computing Environments

Convergent Multimedia (e.g., Interactive TV)

Web-based Systems and Services

Collaborative Scientific Discovery

Quantum Information Systems

Foundation

Information Access

Security

Networks

Software

Math

Statistics

# NIST Mandate for IT Security

- Develop standards and guidelines for the Federal government for sensitive (unclassified) systems

- Contribute to improving the security of commercial IT products and strengthening the security of users' systems and infrastructures

# Specific Focus Areas of NIST's Cybersecurity Program

1. Cryptography
2. Security Testing
3. Guidance
4. Research
5. Outreach

# Toolkit Purpose

- The NIST Cryptographic Standards 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.

# Motivation: 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

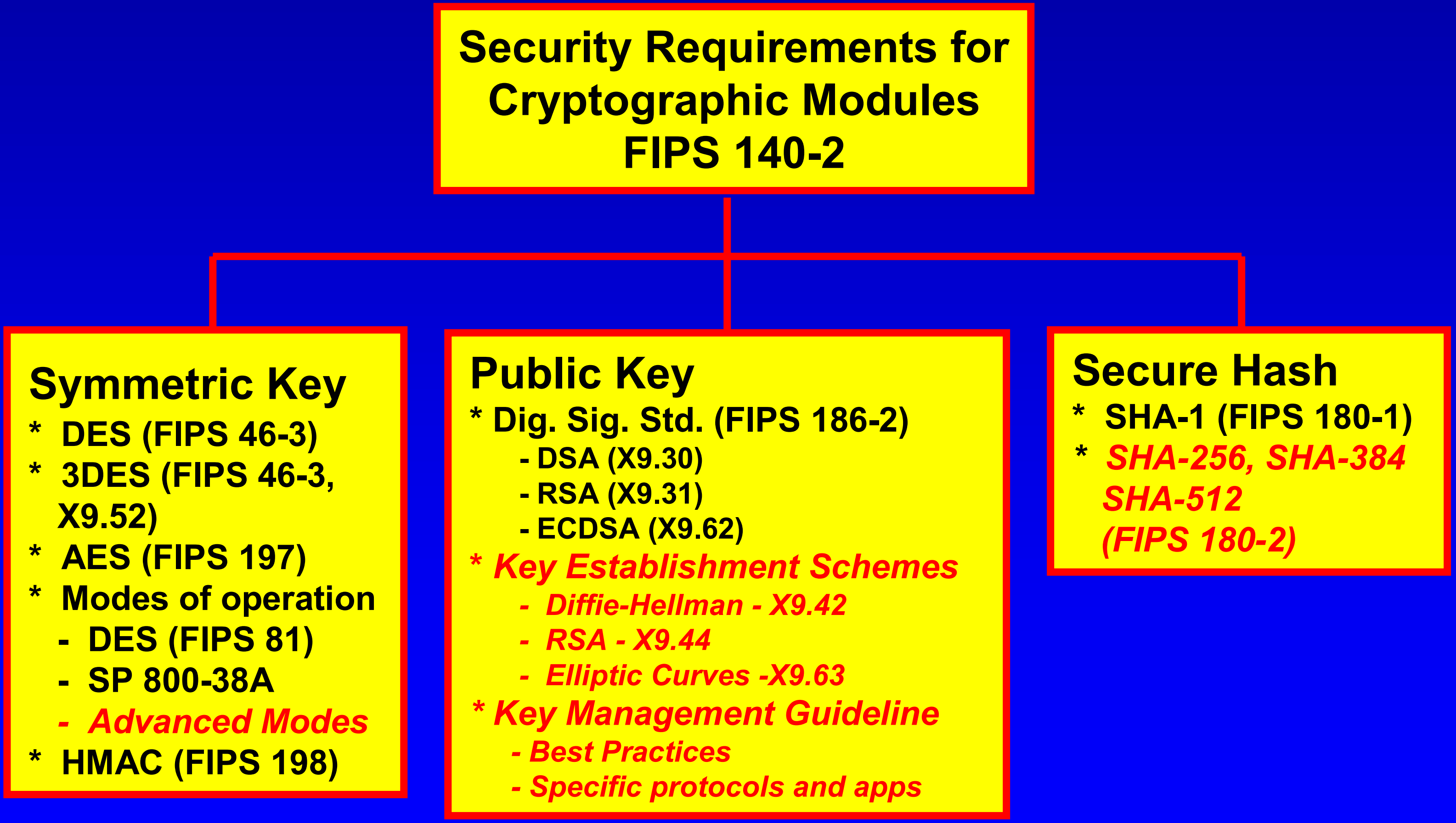
# NIST Cryptographic Toolkit

- 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
  - 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 140-2**

**Symmetric Key**

- * DES (FIPS 46-3)
- * 3DES (FIPS 46-3, X9.52)
- * AES (FIPS 197)
- * Modes of operation
  - - DES (FIPS 81)
  - - SP 800-38A
  - - *Advanced Modes*
- * HMAC (FIPS 198)

**Public Key**

- * Dig. Sig. Std. (FIPS 186-2)
  - - DSA (X9.30)
  - - RSA (X9.31)
  - - ECDSA (X9.62)
- ** Key Establishment Schemes*
  - *\- Diffie-Hellman - X9.42*
  - *\- RSA - X9.44*
  - *\- Elliptic Curves -X9.63*
- ** Key Management Guideline*
  - *\- Best Practices*
  - *\- Specific protocols and apps*

**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
  - IETF

# FIPS 140-2

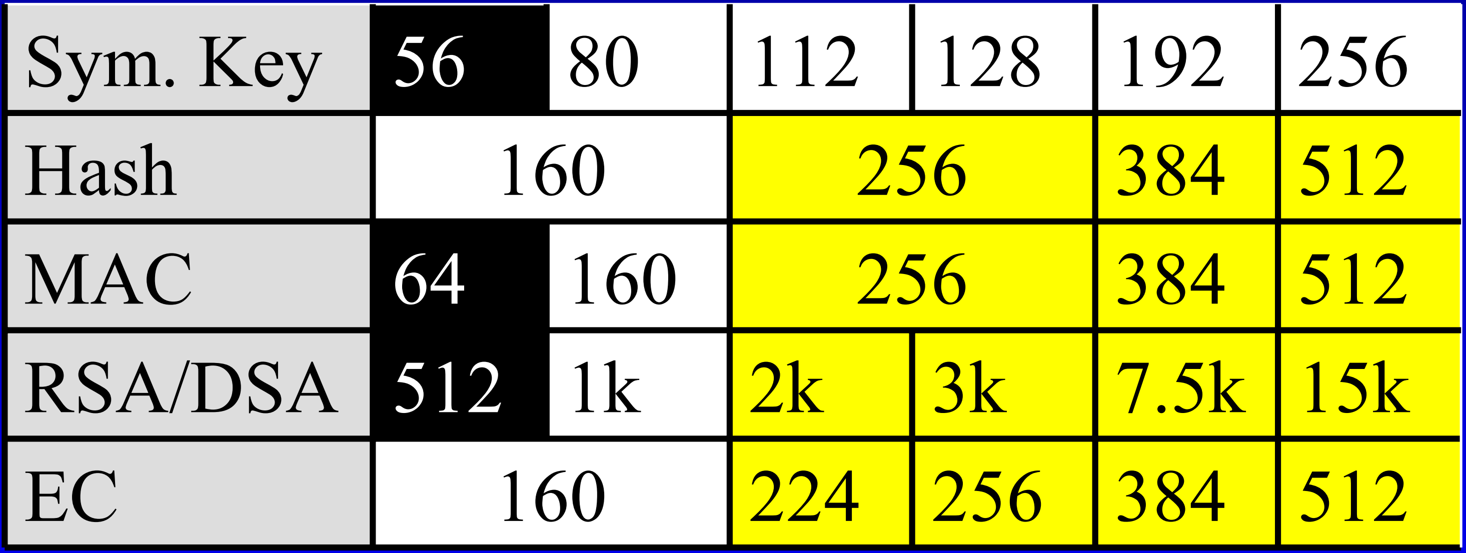
- Joint program with Government of Canada's Communications Security Establishment
- Umbrella standard for Cryptographic Security
- Validation testing for algorithms & Cryptographic Modules
  - Six independent private testing laboratories
    - National Voluntary Laboratory Accreditation (NLVAP) accredited
  - Big increase in validations since 1999
  - Over 200 validated modules to date

# Advanced Encryption Standard (AES)

- DES replacement
- Selected through open competition run by NIST
  - Public evaluation and analysis
  - 21 original submissions
  - 5 “finalists”
  - *Rijndael* selected announced Oct. 2, 2000
  - Standard (FIPS 197) Signed November 26, 2001
  - Testing through the CMVP initiated March 4, 2002
  - 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

# Comparable Strengths

Size in bits



| Sym. Key | 56 | 80 | 112 | 128 | 192 | 256 |
|---|---|---|---|---|---|---|
| Hash | 160 | | 256 | | 384 | 512 |
| MAC | 64 | 160 | 256 | | 384 | 512 |
| RSA/DSA | 512 | 1k | 2k | 3k | 7.5k | 15k |
| EC | 160 | | 224 | 256 | 384 | 512 |

**Sym. Key: Symmetric key encryption algorithms**
**MAC: Message Authentication code**
**Pub. Key: Factoring or discrete log based public key algorithms**
**EC: Elliptic Curve based public key algorithms**
**White background: currently approved FIPS**
**Yellow background: draft standard or recommendation**
**Black background: not secure now**

# NIST Crypto Standards Status

| | 56 | 80 | 112 | 128 | 192 | 256 |
|---|---|---|---|---|---|---|
| Sym. Key | 46-3 | 185 | 46-3 | FIPS 197 (AES) | | |
| Modes | 81 | | | SP 800-38-A | | |
| Hash | 180-1 | | 180-2 | | | |
| MAC | FIPS 198 (HMAC) | | | | | |
| RSA, DSA, EC-DSA | 186-2 | | 186-3 | | | |
| DH/RSA | Key Management FIPS:<br>Scheme and Guidance | | | | | |
| EC-DH | | | | | | |

**White: FIPS approved**
**Red: working draft phase**
**Black: no longer secure**

**Yellow: draft in progress**
**gray: initial recommendation published, more to come**

# Modes of Operation for Symmetric Key Block Ciphers

- Initial Workshop, October, 2000 (NIST)
- Workshop August, 2001 (Santa Barbara, CA)
- Special Publication 800-38-A: Recommendation for Block Cipher Modes of Operation, December 2001
  - Parameterized 4 DES Modes plus Counter Mode
    - Use with any block encryption algorithm
- Continue to consider other modes
  - MAC
  - Modes combining integrity, authentication & encryption
  - Interleaved CBC
  - Key Wrap
  - Super-encryption (e.g., Triple AES?)

# 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
  - These are too small today

# 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

# 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 *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-256
- Available at http://www.nist.gov/sha
- Draft standard (FIPS 180-2) announced May 30, 2001

# 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
  - FIPS 198: Keyed-Hash Message Authentication Code – HMAC, signed March 6, 2002
  - Generalization of RFC 2104 and ANSI X9.71
    - concatenate secret key and message
    - allow different FIPS-approved hash functions and sizes
- AES MAC planned as new mode
  - If you have an AES engine you may want to use it for everything
    - CBC MAC (with a few tweaks)
    - Parallelizable AES MAC also considered

# 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 ~ Spring 2002

# 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
- Workshops
  - Feb. 10 - 11, 2000
  - Nov. 1 - 2, 2001
- Multi-level approach
  - Schemes to define actual cryptographic primitives
    - ANSI X9.42, X9.44, X9.63
  - Key Management Guidance
    - Part 1 - Best Practices advice
    - Part 2 - Guidance on specific protocols or applications
      - PKI, Kerberos, DNS, S/MIME, TLS/SSL, Ipsec …
- 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** | **william.burr@nist.gov** |
| – **FIPS 140: Annabelle Lee** | **annabelle.lee@nist.gov** |
| – **Crypto stds.: Elaine Barker** | **ebarker@nist.gov** |