NIST Cryptographic Standards Program

Bill Burr
william.burr@nist.gov

Dec 4, 2002

NIST Cryptographic Standards

- First Federal Information Processing Standard (FIPS) in Cryptography in 1977
  - FIPS 46, The Data Encryption Standard (DES)
- Mandatory for Federal use of cryptography to protect unclassified, sensitive data
  - FIPS 140-2
- Standardize a set of strong cryptographic tools
  - Can't test and approve every good algorithm/method
    - Too expensive to study each one
  - Too many would confound interoperability

Crypto Standards Toolkit

- Standardized, best of breed solutions for
  - Encryption
    - algorithms
    - modes
  - Message authentication
  - Digital signature
  - Hashing
  - Key generation
    - deterministic (pseudorandom) generators
    - nondeterministic (hardware) generators
    - key derivation
  - Key management
    - wrapping
    - agreement
    - transport

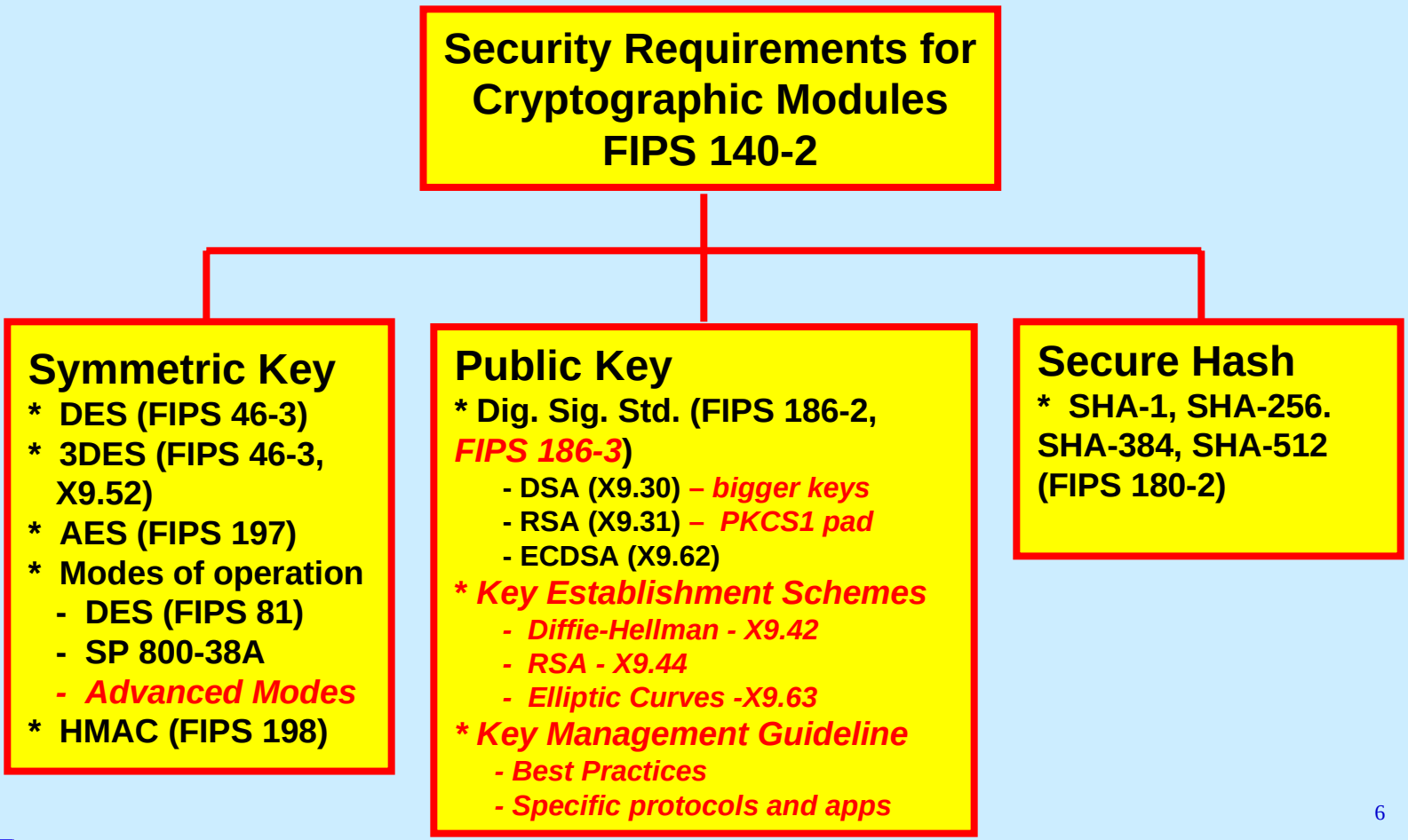
Toolkit Advantages

- FIPS 140-2 product testing
  - CMVP Laboratory validation testing
  - Known answer testing for many of the tools
- Confidence in the security of the tools
  - Carefully evaluated and monitored
- Interoperability and acceptance
  - Tools very widely implemented and used
  - Seen as the safe choice
- Use by Federal agencies often required

Sources of Standards & Recommendations

- Public submissions with NIST selection
  - DES, AES, new crypto modes
- Standards Bodies
  - ANSI-X9
    - TDES, Diffie-Hellman, ECDSA and ECDH, DSA (sorta), RSA variants
  - IETF
    - HMAC
    - perhaps eventually PKIX, TLS, S/MIME, IKE….
- NSA
  - DSA, SHAxxx, proposed AES Key Wrap

Cryptographic Standards



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: under development
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: 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 Recommendation

- SP 800-38A 2001 ED, Recommendation for Block Cipher Modes of Operation, 2001
  - update of FIPS 81
  - 5 modes
    - ECB
    - CBC
    - CFB
    - OFB
    - *Counter*
- Generalized for any block cipher

Submitted Modes

- Total of 17 Modes submitted
- Message authentication seemed most urgent
  - Problems with CBC MAC
    - Extension and collision attacks
  - Originally proposed to limit CBC MAC to fixed size or known size messages
    - Didn’t make anybody happy

RMAC

- Proposed NIST Special Publication 800-38B, The RMAC Authentication Mode
  - submitted by E. Jaulmes, A. Joux, & F. Valette
    - DCSSI Crypto Lab
  - comments to EncryptionModes@nist.gov by 12/02/02
  - resists “general forgery” & “extension forgery” attacks
  - parameters:
    - *k*, the keysize of the encryption algorithm
    - *b*, the blocksize of the encryption algorithm
    - *m*, the length of the MAC
    - *r*, the size of R, a per message random salt
  - define five parameter sets for b=128 and 2 for b=64
    - Most are roughly “balanced” wrt “general forgery” and “extension forgery” attacks

Next Modes?

- Counter with CBC-MAC mode
  - appears destined to be mandatory to implement in 802.11
- AES Key Wrap
  - encryption mode or or key management scheme?

Key Management

- Key Management
  - Workshop in November 2001
  - Schemes document
    - missing part is RSA
      - Bert Kaliski & Russ Housley
        - » Proof of security of TLS with RSA
        - » Simple RSA per per Shoup for endgame
  - Guidance document: hard to scope, many issues
  - Proposed 80-bit crypto end of use date: 2015
  - http://csrc.nist.gov/encryption/tkkeymgmt.html

e-Authentication

- 24 Projects
  - President's Management Agenda
  - E-Sign and Paperwork Elimination acts
  - Intense OMB interest
  - Concept of authentication gateway
    - Password authentication
- NIST doing technical guidance on e-Authentication
  - Success of 802.11 complicates this
    - Access point authentication
      - Man-in-the-middle used to be harder
    - Eavesdropping is more probable

802.11 Issues

- Authentication
  - Theft of service
  - Active attacks inside Government LANs
  - Broader implications for business and citizen e-Authentication
    - more passwords through tunnels
      - rogue APs
      - man-in-the middle
- Confidentiality
  - Need “FIPS quality” encryption

Questions

Crypto FIPS

- FIPS 46-3, Data Encryption Standard -1999
  - refers to ANSI X9.52-1998 for triple DES
  - expect to kill 56-bit DES with 46-4 due in 94
    - http://csrc.nist.gov/encryption/TDESGuidance.pdf
- FIPS 81, DES Modes of Operation – 1980
- FIPS 113, Computer Data Authentication - 1985
  - DES MAC for financial apps.
- FIPS 117, Key Management using ANSI X9.17
  - being withdrawn
- FIPS 180-2, Secure Hash Standard – 2002
  - SHA1, SHA-256, SHA-384, SHA-512

Crypto FIPS

- FIPS 185, Escrowed Encryption Alg. – 1994
  - Skipjack
- FIPS 186-2, Digital Signature Standard
  - DSS, RSA: X9.31 & PKCS#1, ECDSA: X9.62
- FIPS 197, Advanced Encryption Standard (AES) 2001
- FIPS 198, HMAC - Keyed-Hash Message Authentication Code, 2002

Links

- NIST Cryptographic Toolkit
  - http://csrc.nist.gov/encryption/
- AES
  - http://csrc.nist.gov/encryption/aes/
- Modes of Operation
  - http://csrc.nist.gov/encryption/modes/
- Key Management
  - http://csrc.nist.gov/encryption/tkkeymgmt.html
- Cryptographic Module Validation
  - http://csrc.nist.gov/cryptval/