From DES to AES:

Twenty years of U.S. Government Initiatives in Cryptography

From my Perspective

Miles E. Smid

NIST

DES Conception (1965-1972)

- Cryptography generally restricted to classified military applications (except Feistel Lucifer)
- Brooks act (PL89-306) required new standards for improving the utilization of computers by the Federal Government (1965)
- NBS assesses need for computer security within Federal Government (1968)
- NBS Institute for Computer Sciences and Technology saw the need for encryption standard for protection of computer data and requested NSA help in evaluation (1972)

Birth (1973-1977)

- First Federal Register solicitation for DES algorithm (1973) “Few responses”
- Privacy Act of 1974
- Second Federal Register solicitation (1974) IBM submission (Tuchman Group)
- Algorithm published, possible export control mentioned, and IBM grant of nonexclusive, royalty-free licenses (March 1975)

Birth Continued (1975-1977)

- Fourth notice and request for comments (August 1975)
- NBS Workshops (1976)
  - Adequate for 10-15 years
- DES published as first publicly available cryptographic algorithm endorsed by U.S. Government as a standard (January 1977)

Controversy in the 80's

- DES Key size (Diffie-Hellman)
- S-Box Design
- Trap Doors
- NSA Influence
- Government control of Research?
- Motivated Public Research

Acceptance Over Time

- Information Processing Systems (X3, DEA, 1981)
- Banking Applications (X9)
  - Retail: (ATM PIN generation and one-way mapping) (1982)
  - Wholesale: Financial Message Authentication
- ISO Standard? (1985)
- Shamir's Differential Cryptanalysis (1993)
- DES in 48% of U.S. Cryptoproducts (1997 TIS Survey)

DES Modes of Operation
(FIPS 81, 1980)

- Electronic Codebook (ECB)
- Cipher Feedback (CFB)
- Cipher Block Chaining (CBC)
- Output Feedback (OFB)

Message Authentication Code (ANSI X9.9 1982, FIPS 113,)

- DES in CBC Mode
- ANSI X9.9 (CHIPS 1.5 Trillion $/week)
- Treasury Electronic Certification of Forms (500 agencies 100 Billion $/month)
- Army Corps of Engineers Financial Management System
- Replacing Handwritten Signatures

ANSI X9.17 Key Management (1985)

- Symmetric Key Distribution/Translation Centers (H. Rosenbloom NSA)
- Use of counters to prevent playback
- “Key Notarization” gave digital signature like properties when cryptography is physically protected
- NBS provided Triple DES based Pseudo-random key and IV generator
- Triple DES for Key Transport

Second DES 5-year Review (1987)

- Reaffirmed DES for another 5 years
- Allowed DES to be implemented in “software, firmware, hardware, or any combination thereof”

DSA (1994)

- Discrete log based alternative to RSA
- Royalty Free
- Indicated Government acceptance of public key cryptography
- First implementation of DSA and RSA on smart card (Outstanding Security Application 1993, Card Tech/ Secur Tech)

SHA (1993)

- Based on MD4
- 160-bit Hash
- Modified to SHA-1 (1995)
- SHA-1 Probably most popular hash today

PKI Study (1994)

- Interviewed U.S. Federal Agencies
- Studied alternatives for U.S. Government PKI
- Recommended PKI Hierarchy
- Legal Issues
- Estimated cost
- Advisory Group ---> Federal PKI Steering Committee

Key Escrow/Recovery

- 1984 NSA Commercial COMSEC Endorsement Program (1984)
- Escrowed Encryption Standard (1994)
- Clipper (TSD 3600) Capstone (Tessera, Fortezza)
- Secret Algorithms, Government held keys, Distrust
- Technical Advisory Committee (1996)
- Key Recovery in many products

Cryptographic Toolbox with Multiple Technologies

- Symmetric Algorithms (DES, Skipjack, Triple DES, AES)
- Digital Signature Algorithms (DSA, rDSA, ECDSA)
- Key Exchange/Agreement (DH, RSA, ECDH)

Validation and Testing (1977- Present)

- Basic algorithms (DES, DSA, SHA-1, Triple DES, AES ....)
- Modes of Operation
- Cryptographic Module Validation Program
  - Joint US and Canada Program
  - Software and Hardware Modules
  - Twelve Security Areas
  - 65 FIPS 140-1 Validations
- Random Number Generator Tests

The Internet

- Internet research financed by DARPA
- Unprotected networks
- New business methods (E Commerce) require cryptographic based solution

AES Conception (Cryptography for the Next Century) (1997-

- Need for DES replacement
- Need for E Commerce Privacy
- DES Cracks
- Triple DES?
- Let's do it the right way
  - Public input and analysis
- International Process

The Birth Process

- Requirements
  - 128-bit block
  - 128, 192, 256 key sizes
- Process
  - Three Conferences
  - Three Evaluation periods
- Criteria
  - Security, Efficiency, and Flexibility

Conception

- CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT, TWOFISH
- Twelve Countries
- Large Companies, Small Companies, Academics

The Finalists

- MARS (with KS Tweak) (IBM)
  - No Significant Attacks
  - Large Security Margin
  - Good performance on 32-bit variable rotation and multiplication platforms
  - Flexible key size
- RC6 (RSA)
  - No Significant Attacks
  - Simplicity of design
  - Very fast on 32-bit platforms
  - Key, Block, and Rounds fully parameterized

Finalists Continued

- RIJNDAEL (Daemen and Rijmen)
  - No significant attacks
  - Fast on all platforms
  - Flexible on key and block size
  - No significant disadvantages
- SERPENT (Anderson, Biham, Knudsen)
  - No significant attacks
  - Very large secure margin
  - Suited to low end smart cards
  - Bitslice Implementation

Finalists Continued

- TWOFISH (Schneier, Kelsey, Whiting, Wagner, Hall, Ferguson)
  - No significant attacks
  - Large security margin
  - Fast on almost all platforms
  - Flexible on space/time tradeoffs

AES Significance

- Government, Industry, Academia working together to develop a new Advanced Encryption Standard

Third AES Conference - The plot thickens...

AES3 / FSE7

New York City

April 10-14, 2000

Stay Tuned

http://csrc.nist.gov/encryption/aes/aes_home.htm

Conclusions

- Whether intended or not, the U.S. Government initiatives have fostered the development of public research in cryptography
- Government initiatives have led to the development of significant standards which have been widely used to protect sensitive data
- NIST has played a valuable role in developing cryptographic based standards and tests

Special Acknowledgement

- Dr. Dennis K. Branstad
  - Believed in Standards
  - Taught Standards Development
  - Taught Dealing with People