Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

AES: The Making of a New Encryption Standard

This paper describes the issues, programs, and processes related to the development of standards. First, the NIST standard and module certification programs are described. Security specialists and equipment manufactures reference these documents to understand conformance requirements. Second, a historical perspective of the DES project is presented, along with past export control practices. This section highlights the important issues associated with privacy rights. Lastly, a description of the AES selection process is...

Copyright SANS Institute
Author Retains Full Rights

AD

AES: The Making of a New Encryption Standard

By

Mitchell C. Richards

© SANS Institute 2001, Author retains full rights

Course: SANS Security Essentials Certification (GSEC)
Practical Version: 1.2e
Date: 9/5/2001

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

AES: The Making of a New Encryption Standard

Introduction

Most people agree that reading through a stack of governmental standards – full of proclamations, legal jargon, acronyms, and technical specifications – is quite laborious. Few information security professionals, however, survive without them. Standards form the backbone of communication systems, describing (if not requiring) the detailed requirements for interoperability. One needs only to consider the Internet to perceive the importance. The Internet Protocol (IP), considered the fundamental network standard, allows millions of computers to communicate. Many other Internet protocols (e.g., TCP, X.509, and IPSec) serve critical roles in specifying how IP packets are controlled, authenticated, and encrypted.

Recognizing the key role standards play, the Federal government often develops, issues, and revises the controlling documents. The process is long in duration (years) and sometimes bogs down due to the lack of consensus. Not withstanding, a number of standards exist in the area of commerce. Financial transactions need to remain private. Sensitive unclassified information (commonly produced by the government) also requires protection. Thus, a number of Federal Information Processing Standards are available that specify encryption methods and approval processes.

Of course, creating a strong encryption standard is not an easy task. The job requires a large conglomerate (e.g., mathematicians, analysts, computers, etc.) of cryptographic resources. In the past, very few of those resources exist outside of government. Thus, when a standard is needed, large corporations and government agencys ally together to create secure solutions. In the case of the Data Encryption Standard (DES), the development process draws much public criticism. Controversy arises, when work is kept highly secretive.

Today, though, an international cryptography community abounds in private industry and academia. Thus, when a new Advanced Encryption Standard (AES) is proposed, the National Institute of Standards and Technology (NIST) chooses to enlist the help of the global cryptographic community. This gesture marks a significant shift from the past and recognizes the importance of public privacy. Interestingly, the AES development process is designed as a competition, where encryption experts submit algorithms, perform analyses, and present arguments.

The discussion below, presented in three sections, describes the issues, programs, and processes related to the development of standards. First, the NIST standard and module certification programs are described. Security specialists and equipment manufactures reference these documents to understand conformance requirements. Second, a historical perspective of the DES project is presented, along with past export control practices. This section highlights the important issues associated with privacy rights. Lastly, a description of the AES selection process is provided. The success of the project heralds in a new era of cooperation between the U.S. Government, private industry, and academia.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Standards Program and Module Certification

The Data Encryption Standard, issued in 1977, provided a data encryption standard for use by the Federal government to protect sensitive but unclassified information (SUI). The standard required Federal agencies (absent high-level waivers) to use approved encryption modules for SUI transmission. Commercial industries were not under that mandate but were encouraged to voluntarily follow the standard for privacy protection.

Later, to add a mechanism for module certification, the National Institute of Standards and Technology (NIST), formerly the National Bureau of Standards (NBS), established the Cryptographic Module Validation Program (CVMP). The program, developed by NIST and the Communication Security Establishment (CSE) of Canada, validated products against Federal Information Processing Standard (FIPS) specifications.

To help with the task of module testing, NIST accredited independent laboratories through the National Voluntary Laboratory Accreditation Program (NVLAP). Thus, the laboratories tested or verified products for FIPS compliance and reported the results to NIST. NIST, in turn, evaluated a module's conformance level, issuing product certifications as appropriate. Once certified, the product's name was added to a Validated Product List (VPL). Federal and commercial organizations reviewed the VPL, when searching for cryptographic appliances that meet FIPS requirements (NIST, n.d.). Moreover, FIPS specifications, widely implemented in technology, were often adopted and translated to American National Standards Institute (ANSI) standards.

There were a number of FIPS standards that specified requirements for encryption (e.g., FIPS 140-1, FIPS 46-2, and FIPS 81). FIPS 140-1 was the standard that defined the security requirements for cryptographic modules used by the Federal government to protect sensitive unclassified information. Four security levels were described, levels 1-4, with level 1 being the least protective. Determination of the level required for protection depended on the sensitivity of the data and application environment (NIST, 1994).

In addition to the different levels, eleven areas were associated with module design and implementation. Those areas were crypto module, module interfaces, roles & responsibilities, finite state machine, physical security, software security, operating system security, key management, cryptic algorithms, EMI/EMC, and self tests (NIST, 1994).

The FIPS 46-2 or DES standard provided the technical specifications for the Data Encryption Algorithm (DEA). Use of the DEA was mandated by the FIPS 140-1 requirements. From a functional viewpoint, DEA utilized a 64-bit data block and 56-bit key to perform sixteen rounds of mathematical operations on plain text (UIC, n.d.). The resultant text, called cipher or ciphertext, was a series of characters that gave no indication of the original message content or structure.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The mathematical operations generally consisted of substitution, permutation, and addition modulo 2. Substitution occurred, when one character was swapped with another, the letter "A" replaced with the letter "x," for example. Permutation occurred, when characters swapped places in a string. Both operations were considered simple functions and, used alone for encrypting a message, were insecure. Modulo 2 addition occurred, when two bits were added together using exclusive-or digital logic (Landau, 2000a). Interestingly, all three functions used together with a large key in a well thought out algorithm proved to be very resilient to decoding efforts. In fact, DES was used successfully for two decades by the Federal government and private industry.

The FIPS 81 standard specified the modes of operation for DEA. Four modes were described in the document, Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB). The ECB mode was a direct operation of the DEA algorithm on plain text, independent of subsequent data blocks. CBC, an enhanced version of ECB, utilized components from successive blocks for improved encryption. The CFB mode mixed previously encrypted text with plain text, thus creating a function that linked a series of ciphertext together. Lastly, the OFB mode was similar in operation to the CFB mode. OFB, however, used the DEA output to feedback instead of the encrypted text and did not link the cipher blocks (NIST, 1999).

Over time, the FIPS standards were reviewed (usually 5 year intervals) and revised as necessary. Recently, FIPS 140-1 was superseded by FIPS 140-2 and FIPS 46-2 was replaced with FIPS 46-3. The new FIPS 140-2 revision incorporated changes in technical standards and comments by vendors. (A more significant rewrite, taking into consideration Common Criteria, Application Notes, and Lessons Learned, is being evaluated [NIST, 2001d].) Both FIPS 140-2 and FIPS 140-1 were active, with FIPS 140-1 phasing out one year after the FIPS 140-2 effective date.

The new FIPS 46-3 standard specifies the DES algorithm and the Triple Data Encryption Standard (TDES). The use of DES, though approved for legacy systems, was discouraged, since successful, exhaustive or brute force, attacks proved the algorithm insecure. TDES was the approved algorithm described and mandated by the updated FIPS 46-3 document. Other changes, due to the coming Advanced Encryption Standard (AES), were expected. Plans were for TDEA and AES to run concurrently, with AES replacing DES (and possibly TDES) for future cryptographic applications.

The DES Development Controversy and Export Control

On January 2, 1997, NIST announced the development effort to create a new FIPS encryption standard called the Advanced Encryption Standard (AES). Critics claimed that the government's decision to develop a new algorithm was far overdue. For, the Data Encryption Standard (DES) was proven insecure and criticized by cryptography experts. The process for creating DES, closed and secretive, was also a source of much public skepticism.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

From a historical perspective, the development of DES (standardized in 1977) aroused suspicion from the beginning. The National Security Agency (NSA), although considered the largest accumulation of cryptographic resources on the continent (if not the world), declined the encryption project. IBM eventual took the job and submitted a modified design based on an earlier algorithm, called Lucifer. In addition, the work was done in secret, with a number of design documents controlled as classified information.

Causing more suspicion, the NSA, though refusing to create the standard, continued in a powerful over-site role. Ultimately, the secret agency convinced IBM to use a 56-bit key instead of a 64-bit key, influenced the design of the S-box structures, and certified the final algorithm as secure (The Crypt Cabal, 1994). Skepticism bred mistrust in the standard, leaving people to wonder if a trapdoor (a quick means of decryption) was placed in DES (Landau, 2000b). (As of date, no evidence proving that a trapdoor exists has been publicly disclosed).

The control over cryptography, however, did not end with the adoption of DES. Over the next twenty years, academia and private industry battled with government agencies concerning freedom of speech and export controls. For example, MIT professors and cryptography inventors found themselves gagged with secrecy orders and threatened with arrest, when preparing to present innovative research associated with public-key cryptography (Landau, 2000b).

In the end, the encryption designers, supported by legal advice, chose to present their work. The secrecy orders, as a result, were lifted and the research published (Landau, 2000b). The story was quite a history lesson for privacy advocates. For, the coding method – invented by authors Rivest, Shamir, and Adleman – became the most popular public-key algorithm used, known as RSA.

The AES Development Process

In addition to being the next generation encryption method (replacing DES), AES, or the process of developing the standard, heralds in a new era of openness and cooperation between the Federal government, private industry, and global cryptographic community. In fact, the greatest irony occurs, when the algorithm, developed by Belgium scientists, is selected by the U.S. government for adoption as a FIPS standard. The process takes four years to complete (standard is awaiting signature) and, though some speculation is evident at the start, stays on schedule – announcing a winner of the international competition in October of 2000. A description of the development process follows.

In January of 1997, NIST makes the AES project announcement, calling the effort (opposite the covert operations of the past) an “open standards-setting activity” (NIST, 2001b, p. 2). NIST follows through with the promise, soliciting, from the beginning, public comments concerning acceptance requirements, evaluation criteria, and submission components. Eight months after, calls for algorithms occur. Later, as the process continues, three international conferences are held, openly discussing AES encryption methods. In between the three scientific gatherings, Fast Software Encryption

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

(FSE) workshops are held and analysis reports are published, with NIST requesting further reviews and comments.

The minimum acceptability requirements and evaluation criteria appear as a draft document. The general design for the standard, openly discussed at a public work shop, mandates that the algorithm be publicly defined, a symmetric block cipher, adaptable to multiple key lengths, executable in hardware and software, and freely available (NIST, 1997). Each submission is judged according to security, efficiency, memory, ease of hardware and software implementation, simplicity, flexibility, and licensing requirements (NIST, 1997). Early deliberation produces the block and key specification. Accepted algorithms must use a 128-bit block and accommodate 128-bit, 192-bit, and 256-bit keys.

Twenty-one AES submissions are sent in response to the call. NIST, in August of 1998 at the First AES Candidate Conference (AES1), announces a group of fifteen as meeting the minimal requirements. The entry list is made up individuals and groups from around the globe, with members of commercial and academic organizations represented. There is a lot of work to do. NIST petitions the cryptographic community to evaluate all 15 candidates against the evaluation criteria. The field of submissions must be narrowed to 5 or less in this technical analysis, called Round 1. The evaluators are also asked to provide crosscutting analysis reports, comparing algorithm implementation in software and resistance to cryptologic attacks (NIST, 1998).

In March of 1999, NIST holds the Second AES Candidate Conference. The papers submitted include performance comparisons, cryptographic logic evaluations, attack analyses, and intellectual property issues. Round 1 comes to an end and, after a review of the test results and comments, NIST selects five of the fifteen candidates for the Round 2 technical evaluations. The finalists are **MARS**, by IBM; **RC6**, by RSA Laboratories; **Rijndael**, by J. Daemon and V. Rijmen; **Serpent**, by R. Anderson, E. Biham, and L. Knudsen; and **Twofish**, by B. Schneier et al, of Counterpane systems (Srinivas, 2000).

Round 2 is on the way, subjecting the five remaining AES candidates to a much more in-depth study. NIST solicits public comments, giving a deadline of May 15, 2000. Some researchers question the feasibility of performing comprehensive tests on five encryption algorithms in such a small allotment of time.

The third and last conference occurs in April of 2000. Armed with technical reports, the five AES finalists prepare for the final bout. Completed Round 2 tests are presented, comparing the performance of each algorithm on hardware devices, multiple platforms, and reduced round attacks. Competition is intense, with candidates publishing poor performance results on competing submissions. The evaluators claim that MARS and Twofish are to complex, RC6 has a low security margin, Rijndael has insufficient rounds, Serpent demonstrates poor software performance (Srinivas, 2000). There are informal (rump) meetings, too, where researchers argue their findings and opinions. During the debates, the selection of two winning AES candidates is suggested.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

All five finalists, at the end of the conference, present documents supporting why their algorithm should be selected. NIST agrees to consider the idea of two winners and requests further comments. The Round 2 comment period closes in 30 days. This summer or fall, a summary report is scheduled for release, announcing the winner or winners (Dworkin, n.d.). The competition is praised as monumental – involving public, commercial, and academic members of the global cryptographic community.

On October 2, 2000, NIST announces the selection of Rijndael (pronounced Rhine Doll) as the algorithm of choice for the new AES standard (NIST, 2001a). NIST chooses not to name a backup algorithm, citing vendor concerns relative to manufacturing. That is, a backup selection causes the computer industry to add (by default) the second method to AES solutions. Implementing two different encryption methods hurts the industry, since increasing production costs and decreasing interoperability (NIST, 2001c).

NIST, though considering the other four candidates as secure solutions, credits the Rijndael algorithm as the best choice. When evaluated against design criteria, Rijndael performs well in hardware and software implementations and across multiple platforms. The low memory requirement makes the algorithm a great choice for limited resource devices, such as Smart Cards. In addition, Rijndael's key setup time is impressive and logic is easily defendable against known attacks. Lastly, there is a good computational efficiency benefit (when using parallel processing) associated with the internal round structure (NIST, 2001c).

The success of the AES algorithm and selection process draws considerable praise from the industry. For example, Whitfield Diffie, an inventor and leader in cryptography, commented that '"Rijndael offers a good combination of simplicity, performance, and efficient implementation"'(SUN, n.d., p.2). David Aucsmith, Chief Security Architect for Intel, acclaims the selection as a '"model of industry, academic, and government cooperation"' (NIST, 2000, p.1). He also states, in his experience of standard generation, '"there has never been a more equitable, judicious, and timely process."' (NIST, 2000, p1).

Summary

NIST standards establish the rules in which communication systems are built. To encourage interoperability between encryption devices, a number of FIPS documents (e.g., FIPS 140-2, FIPS, 46-3, and FIPS 81) are published. FIPS 46-3, for example, specifies the DES algorithm. A Federal government agency, when transmitting sensitive unclassified data, must use devices specified on the Validated Product List. NIST accredits independent laboratories to perform the actual product testing.

The development of the DES standard, approved in 1977, draws a lot of skepticism. IBM and the Federal Government, working in collaboration, keep the work highly secretive. Export controls are also implemented, raising the concerns of privacy advocates. One academic group, though faced with secrecy orders and arrest threats, present their work on public-key cryptography.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Today, over 20 years after DES, discussions between the government and cryptography community grow more cordial. In fact, a monumental event occurs, when NIST decides to develop AES and solicits help from private industry and academia. In turn, an international competition is held, drawing submissions from around the globe. Candidate algorithms are put through rigorous testing and analysis – evaluated against security, performance, and flexibility. Ironically, the invention of two Belgium scientists, called Rijndael, is selected for the new U.S. standard. In the aftermath, cryptography experts praise the selection process, marking the AES project as a grand example of cooperation between diverse participants, representing government, commercial, and academic interests.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

Dworkin, M. (n.d.). Third advanced encryption standard candidate conference. Retrieved August 25, 2001 from http://csrc.nist.gov/encryption/aes/round2/conf3/aes3report.pdf

Landau, S. (2000a, March). Standing the test of time: The data encryption standard. *Notices, 47*(3), 341-349. Retrieved August 27, 2001 from http://www.ams.org/notices/200003/fea-landau.pdf

Landau, S. (2000b, April). Communications security for the twenty-first century: The advanced encryption standard. *Notices, 47*(4), 450-459. Retrieved August 27, 2001 from http://www.ams.org/notices/200004/fea-landau.pdf

National Institute of Standards and Technology (1994, January 11). Federal Information Processing Standards Publication 140-1, *Security requirements for cryptographic modules.* Retrieved August 27, 2001 from http://www.itl.nist.gov/fipspubs/fip140-1.htm

National Institute of Standards and Technology (1997, January 2). Announcing development of a federal information processing standard for the advanced encryption standard. *Federal Register*. Retrieved August 25, 2001 from http://csrc.nist.gov/encryption/aes/pre-round1/aes_9701.txt

National Institute of Standards and Technology (1998, September 14). Request for comments on candidate algorithms for the advanced encryption standard (AES). *Federal Register, 63*(177). Retrieved August 25, 2001 from http://csrc.nist.gov/encryption/aes/round1/aes_9809.htm

National Institute of Standards and Technology (1999, October 25). Federal Information Processing Standards Publication 46-3, *Data encryption standard.* Retrieved August 27, 2001 from http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

National Institute of Standards and Technology (2000, October 2). *Comments about the advanced encryption standard from industry and government executives*. Retrieved August 25, 2001 from http://www.nist.gov/public_affairs/releases/aescomments.htm

National Institute of Standards and Technology (2001a, February 28). *Advanced encryption standard (AES) development effort*. Retrieved August 25, 2001 from http://csrc.nist.gov/encryption/aes/encryption/aes/index2.html

National Institute of Standards and Technology (2001b, February 28). Announcing the federal information processing standard (FIPS) for the advanced encryption standard (AES) and request for comments. *Federal Register, 66*(40). Retrieved August 25, 2001 from http://csrc.nist.gov/encryption/aes/draftfips/fr-AES-200102.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References (continued)

National Institute of Standards and Technology (2001c, March 5). *Advanced encryption standard (AES) questions and answers.* Retrieved August 27, 2001 from http://csrc.nist.gov/encryption/aes/round2/aesfact.html

National Institute of Standards and Technology (2001d, April 2). *Cryptographic module protection profile development*. Retrieved August 27, 2001 from http://niap.nist.gov/niap/projects/crypto-proj.html

National Institute of Standards and Technology (n.d.). *CSL bulletin for FIPS 140-1*. Retrieved August 27, 2001 from http://www.itl.nist.gov/fipspubs/bul-1401.htm

Srinivas, R. (2000, October). Java World. *AES: Who won?*. Retrieved August 27, 2001 from http://www.javaworld.com/javaworld/jw-10-2000/jw-1027-aes_p.html

Sun Microsystems Laboratories, Feature Stories. (n.d.). *Crypto-politics: Decoding the new encryption standard*. Retrieved August 27, 2001 from http://research.sun.com/research/features/encryption/index.html

The Crypt Cabal. (1994, June 7). Cryptography-faq/part05. Retrieved August 27, 2001 from http://raphael.math.uic.edu/~jeremy/crypt_faq.5.10.txt

University of Illinois at Chicago (n.d.) *The data encryption standard: An update*. Retrieved August 27, 2001 from http://raphael.math.uic.edu/~jeremy/crypt/text/des.txt

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced