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.

The Advanced Encryption System (AES) Development Effort: Overview and Update

Cryptography is a technology that allows us to build security into computer systems and therefore, cyberspace. Without it, there would be no privacy, no e-commerce, and no security of information. The purpose and objective of this paper is to provide a brief overview of where we've been and an update of where we are headed in the United States Department of Commerce's quest for a suitable standard algorithm that can be used to protect sensitive data in the future. This effort arose from the common belief that systems c...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

The Advanced Encryption System (AES) Development Effort: Overview and Update

William M. Tatun
August 26, 2001

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e (amended 5/22/01)

© SANS Institute 2001, Author retains full rights

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

The Advanced Encryption System (AES) Development Effort: Overview and Update

William M. Tatun

August 26, 2001

Selecting a single research topic relevant to the information security arena is not as easy as it may seem at first blush. Even though there are many topics and an immense amount of research material to wade through on each, I experienced the same feeling inside when I selected a topic as I do every time I enter my kids' room, which usually looks like a tornado had just passed through, and not knowing where to begin. After some thought, I decided to research and report on a topic that is fundamental to all of information security, cryptosystems, specifically, the Advanced Encryption System (AES) Development Effort headed up by the United States government. Wherever you find a process that protects data, especially data that may travel through public networks, you are bound to find a cryptosystem. As Bruce Schneier points out in his book, Secrets and Lies, "…cryptography is a core technology of cyberspace."[1] Cryptography is a technology that allows us to build security into computer systems and therefore, cyberspace. Without it, there would be no privacy, no e-commerce, and no security of information. The purpose and objective of this paper is to provide a brief overview of where we've been and an update of where we are headed in the United States Department of Commerce's quest for a suitable standard algorithm that can be used to protect sensitive data in the future. This effort arose from the common belief that systems currently used to protect sensitive data will become obsolete as technology and computer system capabilities increase.

The National Institute of Standards and Technology (NIST), a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration, has been working toward developing a Federal Information Processing Standard (FIPS) aimed at being able to protect sensitive government information. Working with industry and the cryptography community, NIST's goal is to specify an encryption algorithm or set of algorithms that will be capable of protecting sensitive government information into the next century. It is generally accepted that the process of developing new cryptographic algorithms works best when the entire cryptographic community is invited to participate and be allowed to intensely scrutinize the product at every stage of development. It is believed that this process will yield the most effective and efficient way to develop a cryptosystem algorithm that can be trusted to serve as the foundation for protecting sensitive data. The goal of NIST's AES development effort is to apply these beliefs in a way, such that, the end product provides a secure, thoroughly scrutinized and tested algorithm that can be used in future cryptosystems to secure sensitive data.

What is cryptography?

A message or data that can be read and understood without any special process is considered plaintext or otherwise referred to as cleartext. There are times when we wish to protect sensitive messages or computer data, especially if it needs to travel across public networks. For example, an email message sent in plaintext through the Internet to a friend is like sending a postcard through the postal service. The message sent could be read by virtually anyone who cared to take a look. The email scenario might be worse than the postal service due to the speed of worldwide exposure that is possible with email. The postcard-like method may

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

be fine for the casual message but what about sensitive or confidential messages? It is at times like these users may opt to protect their data through the use of a process that invokes encryption and decryption. Encryption is a method of converting plaintext into an unreadable an unintelligible format called ciphertext. The process of converting ciphertext back to a recognizable and readable format is call decryption. Using the process of encryption, a user can store or send sensitive information over public networks in a more secure manner than just sending or storing the data in plaintext. When intended viewers of the data wish to access the encrypted data, they use the process of decryption to convert the ciphertext back to a readable format.

Cryptography can be generally defined as the science of using mathematics to encrypt and decrypt data enabling the storage and transmission of sensitive data in a secure manner. A cryptosystem consists of a cryptographic algorithm, or cipher, which is a mathematical function to encrypt and decrypt data and all of the possible keys and protocols that make it work. Using a key, the cryptographic cipher can be used to convert plaintext to and from ciphertext.

An early example of a cryptosystem is the Ceasar cipher. The Ceasar's cipher, considered developed by Julius Ceasar when he sent messages to his generals through untrusted messengers, can be classified as a substitution cipher, which replaces one piece of information with another. By substituting each letter in the message with the letter that corresponds to the letter 3 places forward in the alphabet from the original, Ceasar was able to encrypt his messages. Basically, Ceasar used a key of 3 and shifted the alphabet plus 3 when encrypting and minus three when decrypting. Thus, the message "SECRET" would become "VHFUHW" when encrypting by using a key of three and shifting the alphabet forward three letters. Decrypting "VHFUHW" would revert back to "SECRET" by shifting the alphabet back three letters. Another substitution cipher, ROT13, is based on this exact process utilizing a key of 13. The ROT13 cipher is a popular mechanism for obfuscating plaintext on USENET.[2]

Obviously, these types of ciphers are considered weak using today's standards and the computing power that is available. The advancement of computing power is precisely the reason we must continuously evaluate our cryptosystems to ensure our sensitive data can be adequately protected while stored and/or sent over public networks.

Background of the Advanced Encryption Standard (AES)

On March 17, 1975, the United States government proposed that the Data Encryption Standard, as originally specified in FIPS-42, be adopted as the national standard cryptosystem to be used with sensitive unclassified computer data. From its inception, DES was criticized and concerns were raised about its main vulnerability, a small key length (56-bits). With a key length of 56-bits, there exists a possibility of only 2^{56} unique keys. Because of the limited key size of DES, it is vulnerable to brute force attacks. The first public crack of the DES cryptosystem occurred in 1997 by Rocke Verser as a part of a challenge. Initially, DES was still considered secure because the first crack took over four months to complete. This changed, however, when in 1998 the Electronic Frontier Foundation proved that they could crack a 56-bit key length in 56 hours.[3] Subsequent attempts to crack DES keys have taken less and less time as the capability of computing systems dramatically increased. Because of these developments, the

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

eventual consensus of the cryptography community was that DES is not secure. DES is no longer supported by the United States Department of Commerce, the agency originally establishing the standard, as a method to secure sensitive data.

When the inherent weakness of DES was discovered, proven, and subsequently causing DES to be considered insecure, it was proposed that multiple encipherments using the DES algorithm could be an effective way to increase key length, increasing the strength of the security. It was proven that DES was not a group therefore proving that performing multiple encipherments would, in fact, increase the key length. That being said, double-DES, enciphering twice, is not used because it, effectively only increases the key length from 2^{56} to 2^{57} leaving it vulnerable to a man-in-the-middle attack. By using a process of applying the algorithm three times and utilizing two different crypto-variables an encipherment that is considered secure by today's standards is produced, known as triple-DES. Triple-DES is considered secure because there have been no public reports claiming to have cracked the algorithm. To crack triple-DES, all of the possible pairs of crypto-variables would need to be examined, which is considered to be outside of the capabilities of the computing resources that currently exist. Triple-DES was not chosen as permanent replacement for DES because of certain limitations that included, but are not limited to, slow implementations on many hardware configurations and the implied vulnerability of its 64-bit block size when compared with anticipated future data rates and computing power. Triple-DES however, was accepted as a temporary replacement to DES until a replacement is established through the AES development process. Both the DES and Triple-DES algorithms are specified together in FIPS-43.[4]

The Cryptographic Algorithm Selection Process

As a part of it's AES development effort, NIST made a formal call for cryptographic algorithms of September 12, 1997. This call for cryptographic algorithms included information on candidate submission specifications, documentation requirements, and evaluation criteria. Specifically, the call stipulated that the AES would specify an unclassified, publicly disclosed encryption algorithm, available royalty-free worldwide. A core requirement of the algorithm is that it must implement symmetric key cryptography as a block cipher and support block sizes of 128-bits, as a minimum, with key sizes of 128-, 192, and 256-bits.[5]

The call for submissions resulted in numerous algorithms being submitted by the worldwide cryptography community. In August of 1998, at the First AES Candidate Conference held in Ventura, California, NIST announced a group of fifteen algorithms that were going be considered in round one of the selection process. A list of the initial fifteen candidate algorithms selected by NIST can be found in Appendix A of this paper. Once the candidate algorithms were identified, NIST solicited comments at the conference and through a Federal Register noticed titled, "Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES)," published in September of 1998.[6] This was part of NIST's process of allowing and soliciting participation from the worldwide cryptographic community.

In March of 1999, a second AES Candidate Conference (AES2) was held in Rome, Italy to discuss the cryptographic community's results and experiences with their analysis of the initial fifteen AES candidate algorithms. Using the input and analyses received, a complete list of

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

which can be found at http://csrc.nist.gov/encryption/aes/round1/pubcmnts.htm, NIST published a list of five finalist algorithms to be considered for the AES development project. The five finalist candidate algorithms selected by NIST were *MARS, RC6, Rijndael, Serpent,* and *Twofish.*

The third AES Candidate Conference (AES3) was held in New York, New York in April of 2000. The purpose of this gathering was to further discuss comments and analyses of the five finalist algorithms. The public analysis and comment period ended in May 2000, allowing NIST to analyze all of the information gathered on AES and make an algorithm selection. In October 2000, NIST announced that it had selected Rijndael as the algorithm for the AES development project.

The Chosen One: Rijndael

Rijndael, how do you pronounce that? Oddly enough, this is one of the first questions that pop into people's minds when they first read about Rijndael. According to the authors' Rijndael web site located at, http://www.esat.kuleuven.ac.be/~rijmen/rijndael/, they claim if you are Dutch, Flemish, Indonesian, Surinamer or South-African, "it's pronounced like you think it should be." Otherwise, they recommend pronouncing it, "Reign Dahl", "Rain Doll" or "Rhine Dahl." In Nick Baran's Dr. Dobbs Journal article, "NIST Selects AES Algorithm," Bruce Schneier, who was co-sponsor of the final five algorithm *Twofish,* was quoted as stating, "...the chief drawback to this cipher is the difficulty Americans have pronouncing it.... The designers, Vincent Rijmen and Joan Daemen, know what they are doing," when asked to comment about the Rijndael algorithm.[7]

The block cipher Rijndael was developed by Joan Daemen and Vincent Rijmen and was based on their previously developed block cipher, Square. The algorithm can be efficiently implemented on a wide range of computer system processors and hardware. The AES development process has determined that the Rijndael algorithm is very secure and has no known weaknesses. In accord with AES requirements, Rijndael's key length can be defined at 128-, 192- or 256-bits. Rijndael has a variable block length that can defined as 128-, 192-, or 256-bits. What does this mean? Basically, Rijndael, which will use the AES specified key sizes of 128-, 192- and 256-bits will provide approximately:

- 3.4×10^{38} possible 128-bit keys;
- 6.2×10^{57} possible 192-bit keys; and
- 1.1×10^{77} possible 256-bit keys.

If we compare these key possibilities with that of DES, which has a 56-bit key size and approximately 7.2×10^{16} possible keys, it is evident that it would require much more computing power to crack the key. In their AES Fact Sheet, NIST uses the following hypothetical example to illustrate the theoretical security provided by AES. If one were to assume that a computing system existed that could recover a DES key in a second, it would take that same machine approximately 149 trillion years to crack a 128-bit AES key. They further illustrate the point by reminding us that the universe is believed to be less than 20 billion years old.[8]

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

What's Next?

NIST released a draft of the Federal Information Processing Standard (FIPS) for AES in February 2001. The draft FIPS for AES can be found at the NIST web site at the link, http://csrc.nist.gov/publications/drafts/dfips-AES.pdf. The ninety-day comment period on the draft FIPS ended on May 29, 2001. At that time, NIST began the process of revising the FIPS taking in account the public comments they have received. After revision, the FIPS will undergo a process of review, approval and promulgation. NIST reports that if all goes as planned, a final published FIPS for AES should be published by the end of this summer (Summer 2001). At the time the finalized FIPS for AES is published it is expected that validation testing for AES implementations will be available through NIST's Cryptographic Module Validation Program (http://csrc.nist.gov/cryptval/).[9]

Does this mean that information technology groups around the world will need to implement Rijndael-based solutions in their systems at the very earliest moment? No. Rijndael will be transitioned into existence, which is the normal process that any standard must go through before becoming one of wide-use. The transition process will allow Triple-DES and Rijndael to co-exist for some time. Eventually, Rijndael will be transitioned into use so that security processes and products that currently use DES and Triple-DES and newly developed systems will be able to benefit from the enhanced security of the AES.

Once the AES is established, NIST will continue to evaluate the standard at regular intervals applying developments in cryptanalysis into a maintenance cycle. Because of developments in cryptanalysis and advances in computing power, no one can be sure how long AES, or any other cryptographic algorithm, will remain secure. But NIST and the worldwide cryptographic community are taking the steps necessary to produce a product that will last an extremely long time. Of course time is relative, but if one considers that DES was the Unites States Government standard for over twenty years before it was publicly cracked, the AES, with significantly larger key sizes, even with the advances in computing technology, has the potential to last.

One important fact we need to be cognizant of is the requirement that the security of a cryptosystems must constantly be scrutinized and evaluated. This is important because as we recall from our training and experience, one can never prove that a particular cryptosystem is secure, only that it is not. With the existence of the impossibility of proving a cryptosystem secure, it is extremely important that proper monitoring of cryptanalysis developments take place and that modifications or adjustments to existing cryptosystems are made as necessary.

The National Institute of Standards and Technology's Advanced Encryption Standard development effort is a bold attempt to develop an encryption standard suitable to protect sensitive data for the next century. The means to this end, NIST believes, is by combining the talent, analysis and input from the worldwide cryptographic community. Through the open exchange of information, intense testing and extreme scrutiny, the AES standard should provide cryptosystems a method of securing data for a long time to come. It is believed that this method of developing such a standard, as opposed to developing a closed proprietary system is the best way to guarantee any reasonable longevity.

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

At the time of the writing of this paper, the AES development effort has NIST preparing the final Federal Information Processing Standard (FIPS) for the AES. Once the FIPS is completed, the transition and implementation of the AES can begin. This process will mark the new beginning of the AES effort. Once established, the AES will need to be cared for and fed like a child so that it may provide cryptosystems the necessary tool to protect sensitive data well into the future.

© SANS Institute 2001, Author retains full rights

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

Appendix A

AES Round 1 Candidate Algorithms

Algorithm Name	Submitter Name(s)
CAST-256	Entrust Technologies, Inc. (represented by Carlisle Adams)
CRYPTON	Future Systems, Inc. (represented by Chae Hoon Lim)
DEAL	Richard Outerbridge, Lars Knudsen
DFC	CNRS - Centre National pour la Recherche Scientifique - Ecole Normale Superieure (represented by Serge Vaudenay)
E2	NTT - Nippon Telegraph and Telephone Corporation (represented by Masayuki Kanda)
FROG	TecApro Internacional S.A. (represented by Dianelos Georgoudis)
HPC	Rich Schroeppel
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
MAGENTA	Deutsche Telekom AG (represented by Dr. Klaus Huber)
MARS	IBM (represented by Nevenko Zunic)
RC6™	RSA Laboratories (represented by Burt Kaliski)
RIJNDAEL	Joan Daemen, Vincent Rijmen
SAFER+	Cylink Corporation (represented by Charles Williams)
SERPENT	Ross Anderson, Eli Biham, Lars Knudsen
TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Source: **National Institute of Standards and Technology**

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

References

1. Schneier, Bruce. Secrets and Lies. New York: John Wiley & Sons Incorporated, 2000.

2. Wilms, Flip. "The Encryption Tutorial."
URL: http://www.sin.khk.be/~wilms/ict/, (August 2001).

3. Electronic Frontier Foundation. "EFF DES Cracker."
URL: http://www.eff.org/descracker.html, (January 1989).

4. United States Department of Commerce/National Institute of Standards and Technology. "Federal Information Processing Standard Publication 43."
URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, (October 1999).

5. United States Department of Commerce/National Institute of Standards and Technology. "Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)."
URL: http://csrc.nist.gov/encryption/aes/pre-round1/aes_9709.htm, (September 1997).

6. United States Department of Commerce. "Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES)."
URL: http://csrc.nist.gov/encryption/aes/round1/aes_9809.htm, (September 1998).

7. Baran, Nick. "NIST Selects AES Algorithm." Dr. Dobbs Journal (Online Edition).
URL: http://www.ddj.com/articles/2000/0065/0065j/0065j.htm?topic=security, (2000).

8. United States Department of Commerce/National Institute of Standards and Technology. "Advanced Encryption Standard (AES) Fact Sheet."
URL: http://csrc.nist.gov/encryption/aes/round2/aesfact.html, (October 2000).

9. United States Department of Commerce/National Institute of Standards and Technology. "National Institute of Standards and Technology Cryptographic Module Validation Program."
URL: http://csrc.nist.gov/cryptval/, (August 2001).

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

Last Updated: June 19th, 2013

Upcoming SANS Training

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

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**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**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 Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**