Information Security Technical Report, Vol 4, No. 4 (1999) 12-17

The Advanced Encryption Standard (AES)

Sean Murphy, Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK

Introduction

In 1997, the US government's National Institute of Standards and Technology (NIST) initiated a process to select a symmetric key algorithm to protect sensitive (unclassified) federal information. The symmetric key algorithm is to be a block cipher, and the algorithm selected would be known as the *Advanced Encryption Standard* (AES).

A block cipher is a highly flexible cryptographic tool. In its basic form, the so-called electronic codebook (ECB) mode, the data is divided into blocks of a given length and the block cipher encrypts the data block by block under the control of single key. However, a block cipher can be used in many other standard modes, such as cipher block chaining (CBC), cipher feedback (CFB) and output feedback (OFB). These different modes are used to provide encryption with different functionality and properties. For example, some of these modes can be used to define a stream cipher. Furthermore, block ciphers are used as building blocks in other common cryptographic primitives such as hash functions (essential for public key cryptography), message authentication codes (MAC) and various key management functions (e.g. key derivation).

Given their versatility, it is clear that it would be of enormous benefit, in terms of interoperability and lowering of costs, if there were a standard block cipher that was generally accepted as being secure and efficient. Although the remit of the NIST is to produce a block cipher standard, AES, for the protection of (unclassified) federal data, AES has the potential to quickly become a *de facto* global standard block cipher algorithm.

Cryptology is a key technology to the future of the Internet and electronic commerce. For the reasons given above, block ciphers are central to such cryptology. Thus, the AES process is one of the most interesting developments in cryptology of recent years. AES could potentially have as much impact in cryptology, both scientifically and commercially, as its predecessor, the Data Encryption Standard (DES).

The Data Encryption Standard (DES)

In 1973, the National Bureau of Standards (forerunner of NIST) issued a call for the public submission of cryptographic algorithms for standardization, for much the same reasons as NIST initiated the AES process. There were no responses. A second call was issued in the following year, and IBM submitted an algorithm. The algorithm was published in March 1975 with a request for comments. The algorithm was a block cipher that used 64-bit blocks using a key of effective size of 56 bits. There were comments submitted primarily about the small key size and the design criteria of the 'S-Boxes', one of the internal components. Nevertheless, the algorithm was published in Federal Information Processing Standard (FIPS) PUB 46 as a federal standard known as the *Data Encryption Standard* (DES) in January 1977. Thereafter many standards with DES as an integral part were developed, either guidelines on how to use DES (e.g. FIPS PUB 81 on modes of operation of DES) or standardizing the use of DES within an industry (e.g. ANSI X9.* with standards for

banking). Indeed DES was almost adopted as an ISO standard, its adoption only being vetoed at the final adoption meeting. The conditions of the standard for DES stated that it should be reviewed every five years. DES was eventually endorsed for five further years in both 1987 and 1993. However, it was clear by then that DES was coming to the end of its useful life and would have to be replaced.

It is probably not possible to understate the importance of DES to the field of cryptography, both commercially and scientifically. Commercially, DES has been universally adopted in many sectors of industry. Scientifically, DES has probably been the catalyst for much open cryptographic research. Certainly, barely any existed before the publication of DES. In its own terms as a cryptographic algorithm, DES has been incredibly successful. Despite being designed in the early 1970s, there were no analytical attacks until the early 1990s. Even so these analytical attacks require vastly more data than could ever be collected and so are impractical by a large margin. The only practical way to attack DES is exhaustive key search, in which every key is tried until the correct key is identified. However, the number of DES keys (DES has a 56-bit key) is small by modern standards. Even when DES was first published there were concerns about the key size of DES. In 1977, Diffie and Hellman envisaged a machine that could be built for $20 million that would recover DES in 12 hours. More recently, in 1993, Wiener described a machine that could be built with standard components for $1 million that would recover DES keys in three hours. Finally, in July 1998, the Electronic Freedom Foundation (EEF) built a machine for $250 000 and actually recovered a DES key in 50 hours. Having built the machine, the cost per DES key recovered is minimal. Clearly, in the future the design of such machines will improve and the costs will plummet. Furthermore, as a DES key search can be carried out in parallel, it is feasible to carry out a networked attack. This technique has also been demonstrated in the last couple of years.

Early concerns about the key size of DES led to the development of Triple-DES (3-DES), in which a DES encryption is used repeatedly. In its most usual form, 3-DES uses two DES keys and three DES encryptions. This clearly increases the encryption time, particularly in software (about 20 Mbits/S on 333MHz Pentium), but though there are time-memory trade-offs, a vastly increased strength against exhaustive key search.

From the above discussion, it can be argued that the shelf life of DES is nearing its end, though it is against DES and particularly 3-DES that any successor to DES will be judged. However, a current design of block cipher would have many advantages over DES. In particular, a modern block cipher design would allow a larger block length and key length, and a possible improved design (better speed for security) by using additional cryptanalytic skills in the public domain and design techniques for modern processors and hardware.

The AES Selection Process

The AES process was initiated by NIST with an announcement of an effort to develop the AES. A formal call for algorithms followed in September 1997. The call stipulated that the AES must specify an unclassified, publicly disclosed encryption algorithm, available royalty-free world wide, and that the AES algorithm would implement a block cipher and would have a block size of 128-bits and would support three key sizes: 128, 192 and 256 bits. In the call for algorithms, and following public comment, NIST gave criteria that would be used to evaluate submitted algorithms. These evaluation characteristics are divided into three categories:

- **Security**: Features such as resistance of the algorithm to cryptanalysis, soundness of its mathematical basis, randomness of the algorithm output, and relative security as compared to other candidates.

- **Cost**: Considerations such as licensing requirements, computational efficiency (speed) on various platforms, and memory requirements. Since one of NIST's goals is that the AES algorithm be available world wide on a royalty-free basis, intellectual property claims and potential conflicts must be considered in the selection process. The speed of the algorithms on a variety of platforms must also be considered. Memory requirements and constraints for software implementations of the candidates are also important factors.

- **Algorithm and implementation characteristics**: Characteristics such as hardware and software suitability, algorithm simplicity and flexibility. It must be feasible to efficiently implement an algorithm in both hardware and software. Flexibility includes the ability of an algorithm to:

    - handle key and block sizes beyond the minimum that must be supported;

    - be implemented securely and efficiently in many different types of environments;

    - be implemented as a stream cipher, hashing algorithm, and to provide additional cryptographic services.

The deadline for submissions of algorithms to NIST was 15 June 1998, and 21 algorithms were submitted. In the selection process for the AES following the submission deadline, the selection process is to be conducted in two rounds with three public AES conferences. Of the algorithms submitted, 15 were accepted into the first round. The first round began in August 1998, with the first AES conference (AES1) in California and finished in April 1999. The purpose of the first round was to select the five or so most promising algorithms to go forward for further scrutiny into the second round. To facilitate this discussion, a second AES conference (AES2) was held in Rome in March 1999. Twenty-one papers on the AES candidates were presented at AES2 often yielding lively discussions. NIST also received 56 other public comments on the AES candidates. Following AES2, submitters were allowed to perform minor 'tweaks' to their algorithms. As part of the AES first round, NIST itself carried out extensive testing of the candidate algorithms, both of an algorithm's implementation characteristics in various scenarios and also of an algorithm's statistical properties.

Two main issues that are not algorithm specific came to prominence during the first round and particularly during AES2. The first of these is whether the AES should consist of a single algorithm or more than one algorithm. The second of these concerned the exact nature of the waiver to intellectual property rights. The main arguments in favour of a single algorithm concern costs and interoperability, whereas the main arguments for multiple AES algorithms include resiliency against a single algorithm being compromised, intellectual property concerns and greater flexibility over the range of AES algorithms. Both of these issues, the number of algorithms and the intellectual property issues have yet to be fully resolved.

At the conclusion of the first round public review, NIST conducted a technical review of AES candidate algorithms in order to recommend algorithms for the second round. The review process considered comments and papers, verbal at conferences, NIST studies,

reports, and proposed modifications, and considered candidates relative to the announced evaluation criteria and other pertinent criteria suggested during the public analysis. In particular, for each algorithm, a methodical evaluation of the following factors was conducted:

- security (including any known attacks or weaknesses);
- efficiency (both speed and memory usage);
- flexibility (implementation on low- and high-end smart cards; support of additional key and block sizes, including whether the reference code actually supported the additional key sizes; suitability for use as a pseudo-random number generator, hashing algorithm, etc.; and whether or not encryption and decryption were the same procedure);
- algorithm simplicity, and
- other issues that were discussed in the received public comments.

Following the review, NIST selected five algorithms to go forward to the second round. The second round began on 10 August 1999 (with the announcement of the five algorithms). The second round ends on 15 May 2000, the deadline for submitting public comments to NIST, with the third AES conference (AES3) taking place in New York in April 2000.

After the end of the second round, NIST will conduct a review of the algorithms, and propose the AES, which will incorporate one or more of the algorithms from the second round. (It is not clear at this stage whether the final standard will consist of a single algorithm.) After a period for public comment and further review, the AES will be announced as a proposed Federal Information Processing Standard (FIPS). After further review, approval and dissemination, it is hoped that the AES standardization process will be completed by summer 2001.

The AES First Round Candidates

The fifteen accepted submissions announced at AES1 were:

CAST-256	(Canada)
Crypton	(Korea)
DEAL	(Canada)
DFC	(France)
E2	(Japan)
Frog	(Costa Rica)
HPC	(USA)
LOKI97	(Australia)
Magenta	(Germany)
MARS	(USA)
RC6	(USA)
Rijndael	(Belgium)
Safer+	(USA)
Serpent	(UK/Il/Dk)
Twofish	(USA)

Of the submissions, the following algorithms were soon discovered to have key scheduling weaknesses:

- Magenta, HPC, DEAL, Crypton, SAFER+ (for long keys);

and a cryptanalysis was discovered for the following algorithms:

- LOKI97 and Frog (weak keys).

For some of the remaining algorithms, there have been cryptanalyses of reduced (shorter) versions. The impact of these analyses of reduced version on the full version is unclear. The algorithms concerned are:

- DFC (six of eight rounds),

- E2 (eight of 12 rounds),
- Crypton (six of 12 rounds).

Speed of operation is a factor as well as security. Estimates of speed vary according to which platform they are measured on. To give an indication of speeds, the following ordering of the fastest candidates is based on clock cycles per byte encrypted on a Pentium II:

- RC6, Rijndael, MARS, Twofish, Crypton, CAST-256, E2, Serpent...

The speeds for these algorithms range from 20 to 60 clock cycles per byte encrypted. For comparison, DES and 3-DES have speeds of about 60 and 140 clock cycles per byte encrypted.

The AES Second Round Candidates

For the second round NIST selected the following five algorithms:

- **MARS** (with tweak), **RC6, Rijndael, Serpent, Twofish.**

Below are the brief summary comments of NIST on the five selected algorithms.

No significant security vulnerabilities were found for these candidates during the Round 1 analysis, and each of these algorithms constitutes potentially superior technology.

MARS incorporates its 'cryptographic core' into an innovative, heterogeneous overall structure. It also features a variety of operations, including the technique of rotating digits by a varying number of places that is determined by both the data and the secret key. Consequently, while MARS performs well in general, it performs particularly well on computer platforms that support its rotation and multiplication operations efficiently. NIST accepted a modification to MARS for Round 2 (proposed by the submitter) that should improve its ability and flexibility to function in some memory-constrained environments, such as low-end smart cards. MARS was submitted to the AES development effort by the International Business Machines Corporation.

RC6 is an algorithm that is simple enough to memorize and should be easy to implement compactly in both software and hardware. Its simplicity also should facilitate its further security analysis in Round 2, which is assisted by the analysis of its predecessor, RC5. RC6 does not use substitution tables; instead, the principal engine for its security is the technique of rotating digits by a varying number of places that is determined by the data. In general, RC6 is fast and it is particularly fast on platforms that support its rotation and multiplication operations efficiently; its key setup is also fast. RC6 was submitted to the AES development effort by RSA laboratories.

Rijndael performs excellently across all considered platforms. Its key setup is fast and its memory requirements are low, so it also should perform well in hardware and in memory-constrained environments. The straightforward design and the conservative choice of operations should facilitate its further analysis, and the operations should be relatively easy to defend against certain attacks on physical implementations. Even though parallel processing was not considered during the Round 1 selection process by the AES review team, Rijndael has the potential of benefiting from advances in computer processors that allow many instructions to be executed in parallel. Rijndael was submitted to the AES development effort by Joan Daemen and Vincent Rijmen.

Serpent is ultra-conservative in its security margin; the designers chose to use twice as many iterations as they believed secure against currently known attacks. Consequently, Serpent's performance is relatively slow compared to the other four finalists. In some settings, however, this should be mitigated by the efficiency of optimized implementations using what the submitters call the 'bitslice' mode, for which the algorithm was specially designed. Serpent should fit well in hardware (with potential tradeoffs of speed versus space) and in memory-constrained environments. The straightforward design and the conservative choice of operations should facilitate further analysis of this candidate, and the operations should be easy to defend against certain attacks on physical implementations. Serpent was submitted to the AES development effort by Ross Anderson, Eli Biham and Lars Knudsen.

Twofish exhibits fast and versatile performance across most platforms; it also should perform well both in hardware and in memory-constrained environments. It features variable substitution 'tables' that depend on the secret key. The submitters believe that such tables generally offer greater security than tables with fixed values. The possibility of pre-computing these tables to varying degrees helps Twofish offer a wide variety of performance trade-offs. Depending on the setting, Twofish can be optimized for speed, key setup, memory, code size in software, or space in hardware. Twofish was submitted to the AES development effort by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson.

Conclusions

NIST will reach a decision regarding AES in the next year or so. To assist NIST in reaching their conclusion will be a wide range of public comments as well as input from other US government agencies. It is also possible that submitted algorithms may be modified before adoption as the AES. There has also been speculation as to whether the US government through NIST would actually select an algorithm of non-US origin.

The main issue about the AES is whether eventually it will be a success. Though AES is receiving extensive and high-profile backing, there are some drawbacks to the AES process. Firstly, it is not clear exactly how much public security analysis the second round AES algorithms have actually received. Secondly, in many situations, certain cryptographic primitives, such as stream ciphers, are very much faster. Finally and most importantly, it is not clear whether the financial community will feel the immediate need to migrate from 3-DES.

Further Information

More extensive information and discussion of the AES process and candidate algorithms can be found on NIST's Web page and at Lars Knudsen's 'Block Cipher Lounge', with respective addresses:

http://csrc.nist.gov/encryption/aes/aes_home.htm, and http://www.ii.uib.no/~larsr/aes.html.