Advanced Encryption Standard

Eric Conrad

Advanced Encryption Standard (AES)

Introduction

AES is the Advanced Encryption Standard, a United States government standard algorithm for encrypting and decrypting data. The standard is described in Federal Information Processing Standard (FIPS) 197.[1]

On January 2, 1997, The National Institute of Standards and Technology (NIST) published a request for comments for the "Development of a Federal Information Processing Standard for Advanced Encryption Standard."[2] NIST sought to "consider alternatives that offer a higher level of security"[3] than that offered by the Data Encryption Standard (DES), which grew vulnerable to brute-force attacks due to its 56-bit effective key length.AES candidates were required to support a symmetric block cipher that supported multiple key lengths. The algorithm had to be publicly defined, free to use, and able to run efficiently in both hardware and software.[4]

Fifteen AES candidate algorithms were announced in August, 1998. Five finalists were chosen on August 9, 1999:

Name	Author	Type
Mars	IBM	Extended Feistel Network
RC6	RSA	Feistel Network
Rijndael	Joan Daemen and Vincent Rijmen	Substitution Permutation Network
Serpent	Ross Anderson, Eli Biham, and Lars Knudsen	Substitution Permutation Network
Twofish	Bruce Schneier, John Kelsey, Niels Ferguson, Doug Whiting, David Wagner, and Chris Hall	Feistel Network

Types of Networks

A Feistel Network (named after Horst Feistel, one of the authors of DES) conducts multiple rounds of transformation, substitution, and encryption. In each round, half a block of data is transformed. Many encryption algorithms use Feistel Networks, including DES and three of the five AES finalists.

An SPN uses a similar approach, using finite field mathematics. A SPN transforms an entire block of data in each round, and substitutions and permutations are applied as separate steps. Two of the five AES finalists use a SPN.

Rijndael was selected and announced as the Advanced Encryption Standard on November, 26, 2001. NIST chose Rijndael due to a "combination of security, performance, efficiency, ease of implementation, and flexibility."[5] Triple DES (three rounds of DES encryption) remain a FIPS-approved encryption algorithm until 2030 to allow transition to AES.[6]

---

[1] FIPS 197. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[2] Federal Register Vol. 62, number 1, January 2, 1997. URL: http://csrc.nist.gov/CryptoToolkit/aes/pre-round1/aes_9701.txt
[3] Federal Register V 62, number 1
[4] Federal Register V 62, number 1
[5] *AES Fact Sheet.* URL: http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html
[6] NIST SP 800-67, page viii. URL: http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

The name “Rijndael” is based on the algorithm’s authors’ names, Joan Daemen and Vincent Rijmen. In English, it is pronounced “Rhine Dahl.”[7] Rijndael is based on the Square Cipher (created by the same authors).

The AES Algorithm

AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits;[8] called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds.

The main loop of AES[9] performs the following functions:

- **`SubBytes()`**
- **`ShiftRows()`**
- **`MixColumns()`**
- **`AddRoundKey()`**

The first three functions of an AES round are designed to thwart cryptanalysis via the methods of “confusion” and “diffusion.” The fourth function actually encrypts the data. Claude Shannon described the concepts of confusion and diffusion in his seminal 1949 paper, “Communication Theory of Secrecy Systems:”

> “Two methods … suggest themselves for frustrating a statistical analysis. These we may call the methods of *diffusion* and *confusion*.”[10]

Diffusion means patterns in the plaintext are dispersed in the ciphertext. Confusion means the relationship between the plaintext and the ciphertext is obscured.

A simpler way to view the AES function order is:

1. Scramble each byte (SubBytes).
2. Scramble each row (ShiftRows).
3. Scramble each column (MixColumns).
4. Encrypt (AddRoundKey).

A term associated with AES is “the State,” an ‘intermediate cipher,’[11] or the ciphertext before the final round has been applied. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially `MixColumns()` and `Shiftrows()`.

SubBytes()

`SubBytes()`adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

Here is the AES Substitution Table:[12]

```
  | 0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
```

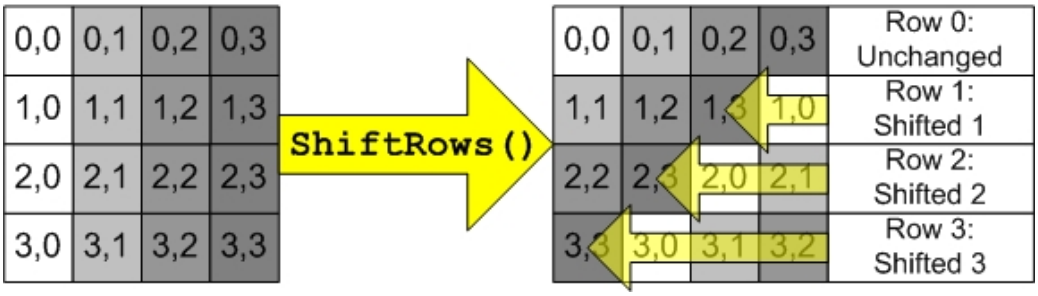
[7] URL of WAV file of proper pronunciation: http://rijndael.info/audio/rijndael_pronunciation.wav
[8] The Rijndael algorithm supported additional key lengths and block sizes which are not supported in AES.
[9] `SubBytes()` is called once before the first AES round. The final AES round omits the `MixColumns`() function
[10] Shannon, Claude. *Communication Theory of Secrecy Systems*. URL: http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf
[11] FIPS 197, page 6
[12] FIPs 197, page 16

```
--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
0 |63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab 76
1 |ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 c0
2 |b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 15
3 |04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 75
4 |09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84
5 |53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 cf
6 |d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8
7 |51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 d2
8 |cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 73
9 |60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b db
a |e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79
b |e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ae 08
c |ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a
d |70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d 9e
e |e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df
f |8c a1 89 0d bf e6 42 68 41 99 2d 0f b0 54 bb 16
```

To complete an S-Box operation on an example string of “ABC,” take the hexadecimal value of each byte. ASCII “A” == hex 0x42, “B” == 0x43 and “C” == 0x44. Look up the first (left) hex digit in the S-Box column and the second in the S-Box row. 0x42 becomes 0x2c; 0x43 becomes 0x1a, and 0x44 becomes 0x1b.

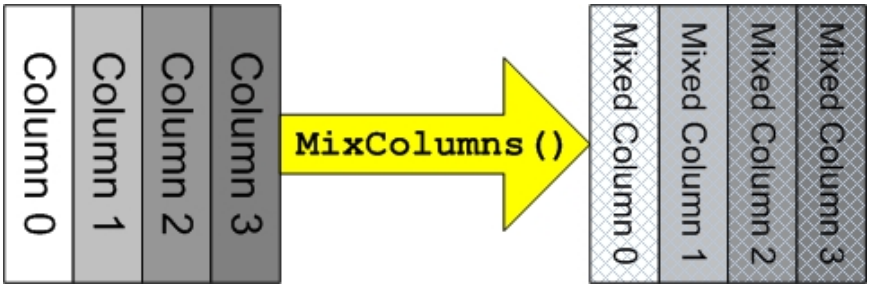
ShiftRows()

`ShiftRows()` provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes, as shown in the *FIPS* illustration that follows:



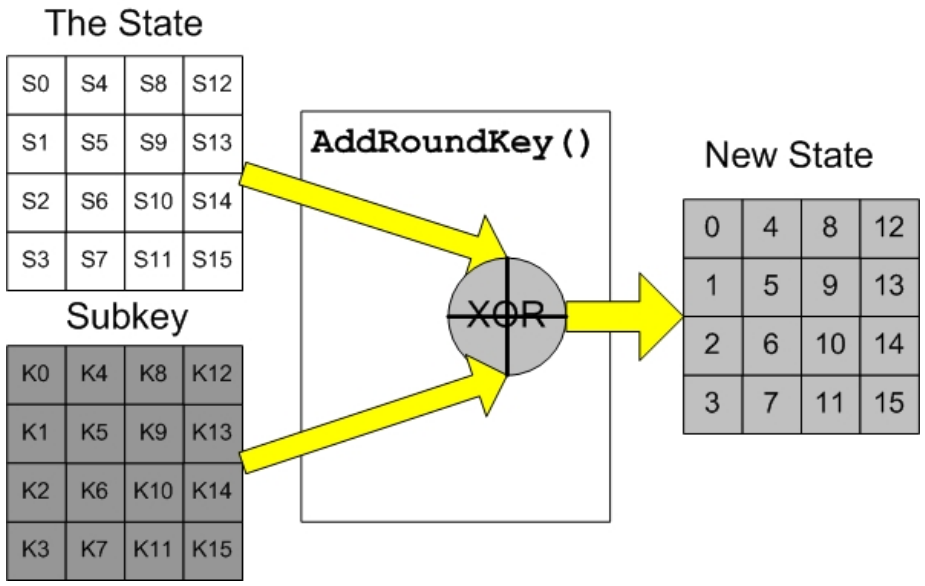
MixColumns()

`MixColumns()`also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics, as shown in the *FIPS* illustration that follows:



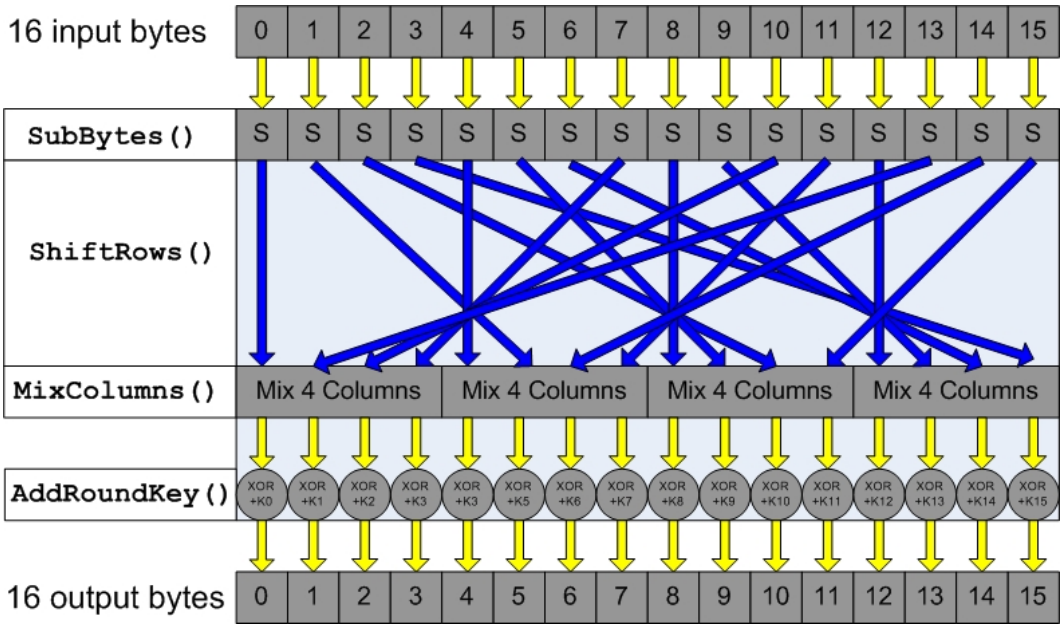
AddRoundKey()

The actual 'encryption' is performed in the `AddRoundKey()` function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a key expansion schedule, as shown in the *FIPS* illustration that follows:



One Round of AES

Here is one round of AES encryption, shown in the *FIPS* publication two dimensionally:



AES Decryption

Decryption occurs through the function `AddRoundKey()`, plus the inverse AES functions `InvShiftRows()`, `InvSubBytes()`, and `InvMixColumns()`.

`AddRoundKey()` does not require an inverse function, as it simply XORs the state with the subkey (XOR encrypts when applied once, and decrypts when applied again).

Attacks on AES

The most successful attack on AES to date is the 'Square Attack," based on the Square Cipher, which was also created by the authors of Rijndael. It "exploits the byte-oriented structure of Square cipher… This attack is also valid for Rijndael, as Rijndael inherits many properties from Square."[13]

The Square Attack is faster than a brute force attack for AES using six rounds or less. For seven rounds or more, brute force attacks are the fastest known attacks. AES uses 10–14 rounds, based on the key length.

Brute forcing AES-128 (smallest key length) is unlikely to be practical in the foreseeable future. According to NIST, "Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key."[14]

Summary

Based on the fact that it is a government standard AES is going to be used in the future as the symmetric algorithm of choice, unless a major flaw is found in the algorithm. It is important to remember that while all initial analysis looks like the algorithm is secure there is no way to prove an algorithm is secure, you can only prove it is not secure by breaking it. Therefore only time will tell but if all works out as planned, you will be seeing AES used in all products instead of DES/Triple DES.

---

[13] Daemen and Rijmen, *The Rijndael Block Cipher*. URL: http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

[14] *AES Fact Sheet*