



# **Rijndael – the Advanced Encryption Standard (AES)**

**Technical Whitepaper**

**Version 1.0  
Author: Dr. Volker Scheidemann**

## **Legal Notice**

Technical Whitepaper Rijndael – the Advanced Encryption Standard.

All rights reserved. Reproduction, translation, microfilming, storage and processing on electronic media without prior permission by Applied Security GmbH is prohibited.

Applied Security GmbH disclaims all rights of ownership for brands and trademarks that are not in its possession.

© 2007  
Applied Security GmbH  
Industriestraße 16  
63811 Stockstadt  
Germany

Fon: + 49 (0) 60 27 / 40 67 - 0  
Fax: + 49 (0) 60 27 / 40 67 - 99  
E-Mail: [info@apsec.de](mailto:info@apsec.de)  
<http://www.apsec.de>

**Table of Contents:**

<b><u>1. Abstract.....</u></b>	<b><u>4</u></b>
<b><u>2. Introduction.....</u></b>	<b><u>4</u></b>
<b><u>3. Rijndael: An overview.....</u></b>	<b><u>4</u></b>
3.1 SubBytes.....	4
3.2 ShiftRows.....	5
3.3 MixColumns.....	5
3.4 AddRoundKey.....	5
3.5 Decryption.....	5
3.6 Security and performance issues.....	6
<b><u>4. Overview of the fideAS® file product line.....</u></b>	<b><u>6</u></b>
<b><u>5. References.....</u></b>	<b><u>6</u></b>

## 1. Abstract

This document gives an overview of the algorithm Rijndael, which was selected as the Advanced Encryption Standard (AES) in 2001 and which is used in the fideAS<sup>®</sup> file product line by the Applied Security GmbH.

## 2. Introduction

On September 12, 1997, the U.S. National Institute of Standards and Technology (NIST) initiated a competition to develop a successor for the Data Encryption Standard (DES) for the encryption of sensitive, but not classified data for commercial institutions, government and public administration. NIST demanded a symmetrical block cipher that could handle blocks of 128 bit length and would be able to deal with key lengths of 128, 192 and 256 bit. The competition was open to the international public and was won by the algorithm Rijndael. It was designed by the two Belgian cryptographers Joan Daemen and Vincent Rijmen. Rijndael was announced AES in summer 2001.

## 3. Rijndael: An overview

Rijndael is an iterated block cipher operating in 10, 12 or 14 rounds (depending on the key length) on cleartext blocks of 128 bit which are organized in quadratic arrays of 16 bytes. Each array is called a *state*.

$a_0$	$a_4$	$a_8$	$a_{12}$
$a_1$	$a_5$	$a_9$	$a_{13}$
$a_2$	$a_6$	$a_{10}$	$a_{14}$
$a_3$	$a_7$	$a_{11}$	$a_{15}$

**Pic.1: The state**

A single round consists of the composition of four transformations of the state which are called *SubBytes*, *ShiftRows*, *MixColumn* and *AddRoundKey*. This scheme is consistent in all rounds except for the last round, in which no *MixColumn* operation is performed.

### 3.1 SubBytes

The *SubBytes* transformation is the most important one for the security of Rijndael, since it is the only non-linear operation within the algorithm. *SubBytes* acts separately on every byte of the state. A byte is interpreted as an element of the finite Galois field  $GF(2^8)$  as well as an element of the vector space  $GF(2)^8$  over  $GF(2)$ . Then the *SubBytes* transformation is the composition of the following two functions:

Inversion

$$\text{inv}: GF(2^8) \rightarrow GF(2^8): x \mapsto \begin{cases} 0, & \text{if } x = 0 \\ x^{-1}, & \text{otherwise} \end{cases}$$

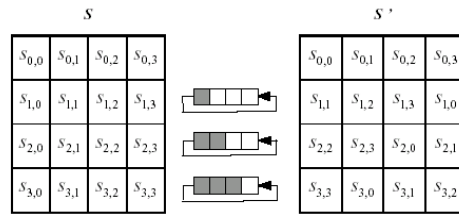
The inversion is followed by an affine-linear transformation

$$x \mapsto Mx + b$$

where  $M$  is an element of  $GL(8, GF(2))$  and  $b$  is a byte, represented as 8 bit vector. The specific values of  $M$  and  $b$  can be found in the Rijndael specification [1].

### 3.2 ShiftRows

The *ShiftRows* operation is very easy. It shifts every row of the current state cyclically by 0, 1, 2 and 3 positions to the left.



**Pic.2: ShiftRows**

Combined with the following *MixColumn* operation this provides for the good diffusion properties of Rijndael.

### 3.3 MixColumns

The *MixColumns* operation acts on every column of the state. Every column transformation can be expressed as a matrix-vector multiplication:

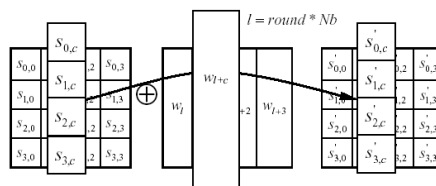
$$\begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

**Pic.3: MixColumn**

Note that a single byte-by-byte multiplication is performed by the rules of finite field multiplication in  $GF(2^8)$ , where the field  $GF(2^8)$  is represented as the quotient of the polynomial ring  $GF(2)[x]$  modulo the (ideal generated by the) irreducible polynomial  $m(x) = x^8+x^4+x^3+x+1$ . The matrix used in this transformation is nonsingular. Hence, the associated linear mapping  $GF(2^3)^4 \rightarrow GF(2^3)^4$  is invertible.

### 3.4 AddRoundKey

*AddRoundKey* adds a round key column to a state column by bitwise XOR. The generation of round keys is described in the AES specification.



**Pic.4: AddRoundKey**

### 3.5 Decryption

Unlike many other ciphers, e.g. DES, Rijndael is not a Feistel cipher. A characteristic of Feistel ciphers is that encryption and decryption are almost identical processes. In order to decrypt a Rijndael-enciphered text, one has to reverse all functions in each round, which can be easily done because the operations are all simple.

### **3.6 Security and performance issues**

Due to the clear structure of the algorithm which needs only a limited amount of mathematical background, Rijndael is well understood. This implies that it would have been impossible to hide a backdoor within the algorithm. It would have been discovered in the selection process. Of course, the easy structure also attracts cryptanalysts. In 2002, N. Cortois and J. Pieprzyk [2] claimed to have found a method (the XLS attack) which would be more effective than a brute force attack, i.e. searching the entire key space. They also claimed to have found out that the complexity of breaking Rijndael does not grow exponentially with the number of rounds. Note that these results are merely of a theoretical nature. Besides that, major crypto experts such as Don Coppersmith or Bruce Schneier are not convinced the XLS method really works, since no experiments have yet asserted the theoretical result. And even if it does, it will not compromise the security of Rijndael from a practical point of view [3], [4]. Even if breaking a Rijndael-enciphered text using the XLS method was, say, one billion times faster than a brute force attack, it would still take millions of years to break the cipher. From a practical point of view, there really is no difference between breaking a cipher in a million of years or in a billion of years. Besides being extremely secure, Rijndael is also a very fast encryption method. Though performance is always dependent on platforms and specific implementations, one can say that on identical platforms, Rijndael is on average about three times faster compared to its predecessor, Triple-DES.

#### 4. Overview of the fideAS® file product line

The AES algorithm Rijndael is used in the file and folder encryption solution fideAS® file enterprise by the Applied Security GmbH.

The encryption software fideAS® file is available in three different versions:

- **fideAS® file personal**
  - File and folder encryption for private use
  - Integrated into the Windows Explorer
  - Free download from [www.apsec.de](http://www.apsec.de) in the download section
- **fideAS® file professional**
  - Encryption and digital signatures
  - Support of smartcards and USB tokens
  - Multi-user capability
  - Integrated into the Windows Explorer
  - Also as mobile installation on a USB storage device
- **fideAS® file enterprise**
  - Transparent file and folder encryption for company-wide use
  - Can be used in the network and for the encryption of notebooks
  - Easy central administration
  - Highly performant and scalable
  - Supports smartcards and USB tokens
  - Group concept for the representation of the organizational structure
  - Innovative key handling (patent pending)
  - Thwarts physical data theft by blocking removable devices

## 5. References

- [1] <http://csrc.nist.gov/encryption/aes/rijndael/>
- [2] <http://eprint.iacr.org/2002/044.pdf>
- [3] <http://www.counterpane.com/crypto-gram-0209.html#1>
- [4] <http://www.usdsi.com/aes.html>