

# Information Security and Cryptography

## Texts and Monographs

---

### *Series Editors*

Ueli Maurer

Ronald L. Rivest

### *Associate Editors*

Martin Abadi

Ross Anderson

Mihir Bellare

Oded Goldreich

Tatsuaki Okamoto

Paul van Oorschot

Birgit Pfitzmann

Aviel D. Rubin

Jacques Stern

**Springer-Verlag Berlin Heidelberg GmbH**

Joan Daemen • Vincent Rijmen

# The Design of Rijndael

AES – The Advanced Encryption Standard

With 48 Figures and 17 Tables



Springer

Joan Daemen  
Proton World International (PWI)  
Zweefvliegtuigstraat 10  
1130 Brussels, Belgium

Vincent Rijmen  
Cryptomathic NV  
Lei 8a  
3000 Leuven, Belgium

Library of Congress Cataloging-in-Publication Data

Daemen, Joan, 1965–  
The design of Rijndael: AES – The Advanced Encryption Standard/Joan Daemen, Vincent Rijmen.  
p. cm.  
Includes bibliographical references and index.

1. Computer security – Passwords. 2. Data encryption (Computer science) I. Rijmen, Vincent, 1970– II. Title

QA76.9.A25 D32 2001  
005.8–dc21

2001049851

ACM Subject Classification (1998): E.3, C.2, D.4.6, K.6.5

ISBN 978-3-642-07646-6 ISBN 978-3-662-04722-4 (eBook)  
DOI 10.1007/978-3-662-04722-4

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York,  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002

Originally published by Springer-Verlag Berlin Heidelberg New York in 2002.

Softcover reprint of the hardcover 1st edition 2002

The use of general descriptive names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by the authors

Cover Design: KünkelLopka, Heidelberg

Printed on acid-free paper SPIN 10851372 – 06/3142SR – 5 4 3 2 1 0

# Foreword

Rijndael was the surprise winner of the contest for the new Advanced Encryption Standard (AES) for the United States. This contest was organized and run by the National Institute for Standards and Technology (NIST) beginning in January 1997; Rijndael was announced as the winner in October 2000. It was the “surprise winner” because many observers (and even some participants) expressed scepticism that the U.S. government would adopt as an encryption standard any algorithm that was not designed by U.S. citizens.

Yet NIST ran an open, international, selection process that should serve as model for other standards organizations. For example, NIST held their 1999 AES meeting in Rome, Italy. The five finalist algorithms were designed by teams from all over the world.

In the end, the elegance, efficiency, security, and principled design of Rijndael won the day for its two Belgian designers, Joan Daemen and Vincent Rijmen, over the competing finalist designs from RSA, IBM, Counterpane Systems, and an English/Israeli/Danish team.

This book is the story of the design of Rijndael, as told by the designers themselves. It outlines the foundations of Rijndael in relation to the previous ciphers the authors have designed. It explains the mathematics needed to understand the operation of Rijndael, and it provides reference C code and test vectors for the cipher.

Most importantly, this book provides justification for the belief that Rijndael is secure against all known attacks. The world has changed greatly since the DES was adopted as the national standard in 1976. Then, arguments about security focussed primarily on the length of the key (56 bits). Differential and linear cryptanalysis (our most powerful tools for breaking ciphers) were then unknown to the public. Today, there is a large public literature on block ciphers, and a new algorithm is unlikely to be considered seriously unless it is accompanied by a detailed analysis of the strength of the cipher against at least differential and linear cryptanalysis.

This book introduces the “wide trail” strategy for cipher design, and explains how Rijndael derives strength by applying this strategy. Excellent resistance to differential and linear cryptanalysis follow as a result. High efficiency is also a result, as relatively few rounds are needed to achieve strong security.

The adoption of Rijndael as the AES is a major milestone in the history of cryptography. It is likely that Rijndael will soon become the most widely-used cryptosystem in the world. This wonderfully written book by the designers themselves is a “must read” for anyone interested in understanding this development in depth.

*Ronald L. Rivest*  
*Viterbi Professor of Computer Science*  
*MIT*

# Preface

This book is about the design of Rijndael, the block cipher that became the Advanced Encryption Standard (AES). According to the ‘Handbook of Applied Cryptography’ [68], a block cipher can be described as follows:

A block cipher is a function which maps  $n$ -bit plaintext blocks to  $n$ -bit ciphertext blocks;  $n$  is called the block length. [...] The function is parameterized by a key.

Although block ciphers are used in many interesting applications such as e-commerce and e-security, this book is *not* about applications. Instead, this book gives a detailed description of Rijndael and explains the design strategy that was used to develop it.

## Structure of this book

When we wrote this book, we had basically two kinds of readers in mind. Perhaps the largest group of readers will consist of people who want to read a full and unambiguous description of Rijndael. For those readers, the most important chapter of this book is Chap. 3, that gives its comprehensive description. In order to follow our description, it might be helpful to read the preliminaries given in Chap. 2. Advanced implementation aspects are discussed in Chap. 4. A short overview of the AES selection process is given in Chap. 1.

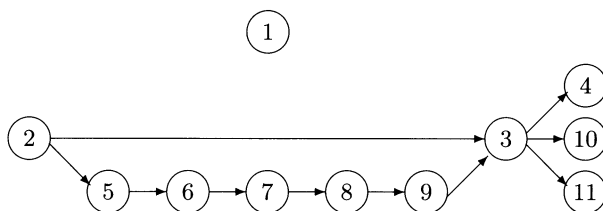
A large part of this book is aimed at the readers who want to know *why* we designed Rijndael in the way we did. For them, we explain the ideas and principles underlying the design of Rijndael, culminating in our wide trail design strategy. In Chap. 5 we explain our approach to block cipher design and the criteria that played an important role in the design of Rijndael. Our design strategy has grown out of our experiences with linear and differential cryptanalysis, two cryptanalytical attacks that have been applied with some success to the previous standard, the Data Encryption Standard (DES). In Chap. 6 we give a short overview of the DES and of the differential and the linear attacks that are applied to it. Our framework to describe linear cryptanalysis is explained in Chap. 7; differential cryptanalysis is described

in Chap. 8. Finally, in Chap. 9, we explain how the wide trail design strategy follows from these considerations

Chapter 10 gives an overview of the published attacks on reduced-round variants of Rijndael. Chapter 11 gives an overview of ciphers related to Rijndael. We describe its predecessors and discuss their similarities and differences. This is followed by a short description of a number of block ciphers that have been strongly influenced by Rijndael and its predecessors.

In Appendix A we show how linear and differential analysis can be applied to ciphers that are defined in terms of finite field operations rather than Boolean functions. In Appendix B we discuss extensions of differential and linear cryptanalysis. To assist programmers, Appendix C lists some tables that are used in various descriptions of Rijndael, Appendix D gives a set of test vectors, and Appendix E consists of an example implementation of Rijndael in the C programming language.

See Fig. 1 for a graphical representation of the different ways to read this book.



**Fig. 1.** Logical dependence of the chapters.

Large portions of this book have already been published before: Joan’s PhD thesis [18], Vincent’s PhD thesis [80], our submission to AES [26], and our paper on linear frameworks for block ciphers [22].

## Acknowledgements

This book would not have been written without the support and help of many people. It is impossible for us to list all people who contributed along the way. Although we probably will make oversights, we would like to name some of our supporters here.

First of all, we would like to thank the many cryptographers who contributed to developing the theory on the design of symmetric ciphers, and from who we learned much of what we know today. We would like to mention explicitly the people who gave us feedback in the early stages of the design



process: Johan Borst, Antoon Bosselaers, Paulo Barreto, Craig Clapp, Erik De Win, Lars R. Knudsen, and Bart Preneel.

Elaine Barker, James Foti and Miles Smid, and all the other people at NIST, who worked very hard to make the AES process possible and visible.

The moral support of our family and friends, without whom we would never have persevered.

Brian Gladman, who provided test vectors.

Othmar Staffelbach, Elisabeth Oswald, Lee McCulloch and other proof-readers who provided very valuable feedback and corrected numerous errors and oversights.

The financial support of K.U.Leuven, the Fund for Scientific Research – Flanders (Belgium), Banksys, Proton World and Cryptomathic is also greatly appreciated.

November 2001

*Joan Daemen and Vincent Rijmen*

# Contents

<b>1.</b>	<b>The Advanced Encryption Standard Process</b>	<b>1</b>
1.1	In the Beginning	1
1.2	AES: Scope and Significance	1
1.3	Start of the AES Process	2
1.4	The First Round	3
1.5	Evaluation Criteria	4
1.5.1	Security	4
1.5.2	Costs	4
1.5.3	Algorithm and Implementation Characteristics	4
1.6	Selection of Five Finalists	5
1.6.1	The Second AES Conference	5
1.6.2	The Five Finalists	6
1.7	The Second Round	7
1.8	The Selection	7
<b>2.</b>	<b>Preliminaries</b>	<b>9</b>
2.1	Finite Fields	10
2.1.1	Groups, Rings, and Fields	10
2.1.2	Vector Spaces	11
2.1.3	Fields with a Finite Number of Elements	13
2.1.4	Polynomials over a Field	13
2.1.5	Operations on Polynomials	14
2.1.6	Polynomials and Bytes	15
2.1.7	Polynomials and Columns	16
2.2	Linear Codes	17
2.2.1	Definitions	17
2.2.2	MDS codes	19
2.3	Boolean Functions	19
2.3.1	Bundle Partitions	20
2.3.2	Transpositions	21
2.3.3	Bricklayer Functions	22
2.3.4	Iterative Boolean Transformations	22
2.4	Block Ciphers	23
2.4.1	Iterative Block Ciphers	24

2.4.2	Key-Alternating Block Ciphers . . . . .	25
2.5	Block Cipher Modes of Operation . . . . .	27
2.5.1	Block Encryption Modes . . . . .	27
2.5.2	Key-Stream Generation Modes . . . . .	27
2.5.3	Message Authentication Modes . . . . .	28
2.5.4	Cryptographic Hashing . . . . .	29
2.6	Conclusions . . . . .	29
<b>3.</b>	<b>Specification of Rijndael . . . . .</b>	<b>31</b>
3.1	Differences between Rijndael and the AES . . . . .	31
3.2	Input and Output for Encryption and Decryption . . . . .	31
3.3	Structure of Rijndael . . . . .	33
3.4	The Round Transformation . . . . .	33
3.4.1	The SubBytes Step . . . . .	34
3.4.2	The ShiftRows Step . . . . .	37
3.4.3	The MixColumns Step . . . . .	38
3.4.4	The Key Addition . . . . .	40
3.5	The Number of Rounds . . . . .	41
3.6	Key Schedule . . . . .	43
3.6.1	Design Criteria . . . . .	43
3.6.2	Selection . . . . .	43
3.7	Decryption . . . . .	45
3.7.1	Decryption for a Two-Round Rijndael Variant . . . . .	45
3.7.2	Algebraic Properties . . . . .	46
3.7.3	The Equivalent Decryption Algorithm . . . . .	48
3.8	Conclusions . . . . .	50
<b>4.</b>	<b>Implementation Aspects . . . . .</b>	<b>53</b>
4.1	8-Bit Platforms . . . . .	53
4.1.1	Finite Field Multiplication . . . . .	53
4.1.2	Encryption . . . . .	54
4.1.3	Decryption . . . . .	55
4.2	32-Bit Platforms . . . . .	56
4.3	Dedicated Hardware . . . . .	59
4.3.1	Decomposition of $S_{RD}$ . . . . .	60
4.3.2	Efficient Inversion in $GF(2^8)$ . . . . .	61
4.4	Multiprocessor Platforms . . . . .	61
4.5	Performance Figures . . . . .	62
4.6	Conclusions . . . . .	62
<b>5.</b>	<b>Design Philosophy . . . . .</b>	<b>63</b>
5.1	Generic Criteria in Cipher Design . . . . .	63
5.1.1	Security . . . . .	63
5.1.2	Efficiency . . . . .	64
5.1.3	Key Agility . . . . .	64

5.1.4	Versatility .....	64
5.1.5	Discussion .....	64
5.2	Simplicity .....	65
5.3	Symmetry .....	65
5.3.1	Symmetry Across the Rounds .....	66
5.3.2	Symmetry Within the Round Transformation .....	66
5.3.3	Symmetry in the D-box .....	67
5.3.4	Symmetry and Simplicity in the S-box .....	68
5.3.5	Symmetry between Encryption and Decryption .....	68
5.3.6	Additional Benefits of Symmetry .....	68
5.4	Choice of Operations .....	69
5.4.1	Arithmetic Operations .....	70
5.4.2	Data-Dependent Shifts .....	70
5.5	Approach to Security .....	71
5.5.1	Security Goals .....	71
5.5.2	Unknown Attacks Versus Known Attacks .....	72
5.5.3	Provable Security Versus Provable Bounds .....	73
5.6	Approaches to Design .....	73
5.6.1	Non-Linearity and Diffusion Criteria .....	73
5.6.2	Resistance against Differential and Linear Cryptanalysis .....	73
5.6.3	Local Versus Global Optimization .....	74
5.7	Key-Alternating Cipher Structure .....	76
5.8	The Key Schedule .....	76
5.8.1	The Function of a Key Schedule .....	76
5.8.2	Key Expansion and Key Selection .....	77
5.8.3	The Cost of the Key Expansion .....	77
5.8.4	A Recursive Key Expansion .....	78
5.9	Conclusions .....	79
<b>6.</b>	<b>The Data Encryption Standard .....</b>	<b>81</b>
6.1	The DES .....	81
6.2	Differential Cryptanalysis .....	83
6.3	Linear Cryptanalysis .....	85
6.4	Conclusions .....	87
<b>7.</b>	<b>Correlation Matrices .....</b>	<b>89</b>
7.1	The Walsh-Hadamard Transform .....	89
7.1.1	Parities and Selection Patterns .....	89
7.1.2	Correlation .....	89
7.1.3	Real-valued Counterpart of a Binary Boolean Function .....	90
7.1.4	Orthogonality and Correlation .....	90
7.1.5	Spectrum of a Binary Boolean Function .....	91
7.2	Composing Binary Boolean Functions .....	93
7.2.1	XOR .....	93
7.2.2	AND .....	93

7.2.3	Disjunct Boolean Functions . . . . .	94
7.3	Correlation Matrices . . . . .	94
7.3.1	Equivalence of a Boolean Function and its Correlation Matrix . . . . .	95
7.3.2	Iterative Boolean Functions . . . . .	96
7.3.3	Boolean Permutations . . . . .	96
7.4	Special Boolean Functions . . . . .	98
7.4.1	XOR with a Constant . . . . .	98
7.4.2	Linear Functions . . . . .	98
7.4.3	Bricklayer Functions . . . . .	98
7.5	Derived Properties . . . . .	99
7.6	Truncating Functions . . . . .	100
7.7	Cross-correlation and Autocorrelation . . . . .	101
7.8	Linear Trails . . . . .	102
7.9	Ciphers . . . . .	103
7.9.1	General Case . . . . .	103
7.9.2	Key-Alternating Cipher . . . . .	104
7.9.3	Averaging over all Round Keys . . . . .	105
7.9.4	The Effect of the Key Schedule . . . . .	106
7.10	Correlation Matrices and Linear Cryptanalysis Literature . . . . .	108
7.10.1	Linear Cryptanalysis of the DES . . . . .	108
7.10.2	Linear Hulls . . . . .	109
7.11	Conclusions . . . . .	111
<b>8.</b>	<b>Difference Propagation . . . . .</b>	<b>113</b>
8.1	Difference Propagation . . . . .	113
8.2	Special Functions . . . . .	114
8.2.1	Affine Functions . . . . .	114
8.2.2	Bricklayer Functions . . . . .	114
8.2.3	Truncating Functions . . . . .	115
8.3	Difference Propagation Probabilities and Correlation . . . . .	115
8.4	Differential Trails . . . . .	117
8.4.1	General Case . . . . .	117
8.4.2	Independence of Restrictions . . . . .	117
8.5	Key-Alternating Cipher . . . . .	118
8.6	The Effect of the Key Schedule . . . . .	119
8.7	Differential Trails and Differential Cryptanalysis Literature . . . . .	119
8.7.1	Differential Cryptanalysis of the DES Revisited . . . . .	119
8.7.2	Markov Ciphers . . . . .	120
8.8	Conclusions . . . . .	122

<b>9. The Wide Trail Strategy</b> .....	123
9.1 Propagation in Key-alternating Block Ciphers .....	123
9.1.1 Linear Cryptanalysis .....	123
9.1.2 Differential Cryptanalysis .....	125
9.1.3 Differences between Linear Trails and Differential Trails	126
9.2 The Wide Trail Strategy .....	126
9.2.1 The $\gamma\lambda$ Round Structure in Block Ciphers .....	127
9.2.2 Weight of a Trail .....	129
9.2.3 Diffusion .....	130
9.3 Branch Numbers and Two-Round Trails .....	131
9.3.1 Derived Properties .....	133
9.3.2 A Two-Round Propagation Theorem .....	133
9.4 An Efficient Key-Alternating Structure .....	134
9.4.1 The Diffusion Step $\theta$ .....	134
9.4.2 The Linear Step $\Theta$ .....	136
9.4.3 A Lower Bound on the Bundle Weight of Four-Round Trails .....	136
9.4.4 An Efficient Construction for $\Theta$ .....	137
9.5 The Round Structure of Rijndael .....	138
9.5.1 A Key-Iterated Structure .....	138
9.5.2 Applying the Wide Trail Strategy to Rijndael .....	142
9.6 Constructions for $\theta$ .....	143
9.7 Choices for the Structure of $\mathcal{I}$ and $\pi$ .....	145
9.7.1 The Hypercube Structure .....	145
9.7.2 The Rectangular Structure .....	147
9.8 Conclusions .....	147
<b>10. Cryptanalysis</b> .....	149
10.1 Truncated Differentials .....	149
10.2 Saturation Attacks .....	149
10.2.1 Preliminaries .....	150
10.2.2 The Basic Attack .....	150
10.2.3 Influence of the Final Round .....	152
10.2.4 Extension at the End .....	153
10.2.5 Extension at the Beginning .....	153
10.2.6 Attacks on Six Rounds .....	153
10.2.7 The Herds Attack .....	154
10.3 Gilbert–Minier Attack .....	154
10.3.1 The Four-Round Distinguisher .....	154
10.3.2 The Attack on Seven Rounds .....	155
10.4 Interpolation Attacks .....	156
10.5 Symmetry Properties and Weak Keys as in the DES .....	156
10.6 Weak keys as in IDEA .....	157
10.7 Related-Key Attacks .....	157
10.8 Implementation Attacks .....	157

10.8.1	Timing Attacks .....	157
10.8.2	Power Analysis .....	158
10.9	Conclusion .....	160
<b>11.</b>	<b>Related Block Ciphers .....</b>	<b>161</b>
11.1	Overview .....	161
11.1.1	Evolution .....	161
11.1.2	The Round Transformation .....	162
11.2	SHARK .....	163
11.3	Square .....	165
11.4	BKSQ .....	168
11.5	Children of Rijndael .....	171
11.5.1	Crypton .....	171
11.5.2	Twofish .....	172
11.5.3	ANUBIS .....	172
11.5.4	GRAND CRU .....	173
11.5.5	Hierocrypt .....	173
11.6	Conclusion .....	173
 <b>Appendices</b>		
<b>A.</b>	<b>Propagation Analysis in Galois Fields .....</b>	<b>175</b>
A.1	Functions over $\text{GF}(2^n)$ .....	176
A.1.1	Difference Propagation .....	177
A.1.2	Correlation .....	177
A.1.3	Functions that are Linear over $\text{GF}(2^n)$ .....	179
A.1.4	Functions that are Linear over $\text{GF}(2)$ .....	180
A.2	Functions over $(\text{GF}(2^n))^\ell$ .....	181
A.2.1	Difference Propagation .....	182
A.2.2	Correlation .....	182
A.2.3	Functions that are Linear over $\text{GF}(2^n)$ .....	182
A.2.4	Functions that are Linear over $\text{GF}(2)$ .....	183
A.3	Representations of $\text{GF}(p^n)$ .....	184
A.3.1	Cyclic Representation of $\text{GF}(p^n)$ .....	184
A.3.2	Vector Space Representation of $\text{GF}(p^n)$ .....	184
A.3.3	Dual Bases .....	185
A.4	Boolean Functions and Functions in $\text{GF}(2^n)$ .....	186
A.4.1	Differences in $\text{GF}(2)^n$ and $\text{GF}(2^n)$ .....	186
A.4.2	Relationship Between Trace Patterns and Selection Patterns .....	187
A.4.3	Relationship Between Linear Functions in $\text{GF}(p)^n$ and $\text{GF}(p^n)$ .....	187
A.4.4	Illustration .....	190
A.5	Rijndael-GF .....	192

<b>B. Trail Clustering</b> .....	195
B.1 Transformations with Maximum Branch Number .....	196
B.2 Bounds for Two Rounds .....	199
B.2.1 Difference Propagation .....	200
B.2.2 Correlation .....	202
B.3 Bounds for Four Rounds .....	204
B.4 Two Case Studies .....	205
B.4.1 Differential Trails .....	205
B.4.2 Linear Trails .....	207
<b>C. Substitution Tables</b> .....	211
C.1 $S_{RD}$ .....	211
C.2 Other Tables .....	212
C.2.1 <code>xtime</code> .....	212
C.2.2 Round Constants .....	212
<b>D. Test Vectors</b> .....	215
D.1 KeyExpansion .....	215
D.2 Rijndael(128,128) .....	215
D.3 Other Block Lengths and Key Lengths .....	217
<b>E. Reference Code</b> .....	221
<b>Bibliography</b> .....	229
<b>Index</b> .....	235