Information Security and Cryptography
Texts and Monographs

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

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

http://www.springer.de

Originally published by Springer-Verlag Berlin Heidelberg New York in 2002.
Softcover reprint of the hardcover 1st edition 2002

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.

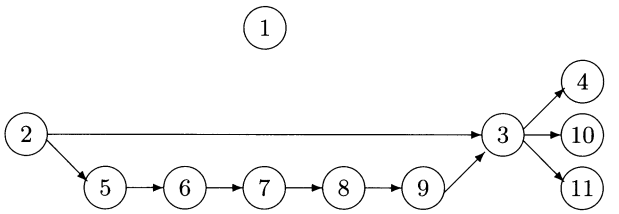

Fig. 1. Logical dependence of the chapters.

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