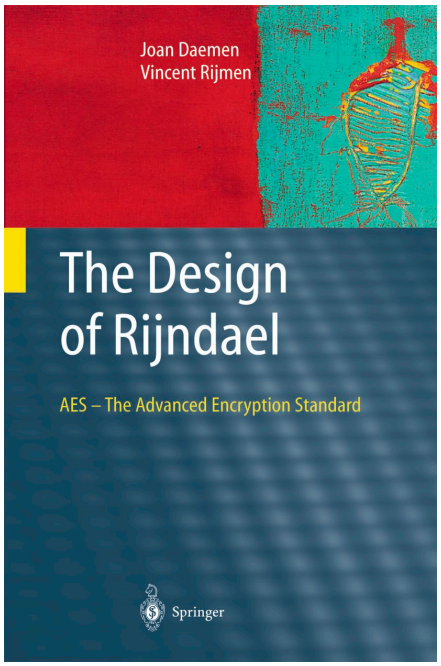

2002, XVII, 238 p.

Printed book

Hardcover

89,99 € | £79.99 | $109.99

[1]96,29 € (D) | 98,99 € (A) | CHF 106,50

eBook

74,89 € | £63.99 | $84.99

[2]74,89 € (D) | 74,89 € (A) | CHF 85,00

Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just

€ | $ 24.99

springer.com/mycopy

Joan Daemen, Vincent Rijmen

The Design of Rijndael

AES - The Advanced Encryption Standard

Series: Information Security and Cryptography

- This book is THE guide to the new Advanced Encryption Standard
- Written by its designers
- First book in the new Springer series Information Security and Cryptography, further information at http://www.springer.de/comp/series/is&c.html

Rijndael was the surprise winner of the contest for the new Advanced En- cryption Standard (AES) for the United States. This contest was organized and run by the National Institute for Standards and Technology (NIST) be- ginning 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 D.S. government would adopt as an encryption standard any algorithm that was not designed by D.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 EnglishjIsraelijDanish 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 and the operation of Rijndael, and it provides reference C code and underst test vectors for the cipher.