The Design of Rijndael : AES - The Advanced Encryption Standard /

Daemen, Joan

Springer Berlin Heidelberg,
2002

Electronic books

Monografía

In October 2000, the US National Institute of Standards and Technology selected the block cipher Rijndael as the Advanced Encryption Standard (AES). AES is expected to gradually replace the present Data Encryption Standard (DES) as the most widely applied data encryption technology. This book by the designers of the block cipher presents Rijndael from scratch. The underlying mathematics and the wide trail strategy as the basic design idea are explained in detail and the basics of differential and linear cryptanalysis are reworked. Subsequent chapters review all known attacks against the Rijndael structure and deal with implementation and optimization issues. Finally, other ciphers related to Rijndael are presented. This volume is THE authoritative guide to the Rijndael algorithm and AES. Professionals, researchers, and students active or interested in data encryption will find it a valuable source of information and reference

Título: The Design of Rijndael AES - The Advanced Encryption Standard by Joan Daemen, Vincent Rijmen

Editorial: Berlin, Heidelberg Springer Berlin Heidelberg 2002

Descripción física: 1 online resource (xvii, 238 pages)

Mención de serie: Information Security and Cryptography, Texts and Monographs 1619-7100

Copyright/Depósito Legal: 934995384 936317639 968656448

ISBN: 9783662047224 electronic bk.) 3662047225 electronic bk.) 9783642076466 3642076467 3662047225

Materia: Computer science Computer Communication Networks Data protection Data encryption (Computer science) Computer software Computer science Computer software Data encryption (Computer science) Data protection

Autores: Rijmen, V.

Enlace a formato físico adicional: Print version 9783642076466

Punto acceso adicional serie-Título: Information Security and Cryptography, Texts and Monographs

---