1. Record Nr. UNISA996465342203316

Autore	Daemen Joan
Titolo	The Design of Rijndael [[electronic resource]] : The Advanced Encryption Standard (AES) / / by Joan Daemen, Vincent Rijmen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2020
ISBN	3-662-60769-7
Edizione	[2nd ed. 2020.]
Descrizione fisica	1 online resource (xviii, 282 pages) : illustrations
Collana	Information Security and Cryptography, , 1619-7100
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security System safety Cryptology Principles and Models of Security Systems and Data Security Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	The Advanced Encryption Standard Process -- Preliminaries -- Specification of Rijndael -- Implementation Aspects -- Design Philosophy -- The Data Encryption Standard -- Correlation Matrices -- Difference Propagation -- The Wide Trail Strategy -- Cryptanalysis -- The Road to Rijndael -- Correlation Analysis in GF(2n) -- On the EDP of Two- and Four-Round Differentials and the ELP of Two- and Four-Round Hulls -- Two-Round Differential Trail Clustering -- Plateau Trails -- App. A, Substitution Tables -- App. B, Test Vectors -- App. C, Reference Code -- Bibliography -- Index.
Sommario/riassunto	This is the authoritative guide to Rijndael, the block cipher whose elegance, efficiency, security, and principled design made it the Advanced Encryption Standard (AES), now the most widely applied data encryption technology. The authors developed the Rijndael algorithm and in this book they explain the AES selection process and their motivation in the light of the earlier Data Encryption Standard. They explain their design philosophy and implementation and optimization

aspects, and the strength of their approach against cryptanalysis. They support the text with the relevant mathematics, reference code, and test vectors. In this new edition the authors updated content throughout, added new chapters, and adapted their text to the new terminology in use since the first edition. This is a valuable reference for all professionals, researchers, and graduate students engaged with data encryption.