1.	Record Nr.	UNISA996392006703316
	Autore	A. C (Arthur Crowther), <1588-1666.>
	Titolo	The dayly exercise of the devout Christian [[electronic resource]] : Containing several most pithy practices of piety, in order to live holily and dye happily. / / Published by T.V., monk, of the holy order of St. Benedict
	Pubbl/distr/stampa	[S.l., : s.n.], Printed Anno Dom. 1685
	Edizione	[The third edition, digested into better order, with many material additions, and alterations.]
	Descrizione fisica	[74], 408, 407-430, 433-503, [1] p
	Altri autori (Persone)	T. V <1604-1681.> (Thomas Vincent)
	Soggetti	Devotional exercises - 17th century Christian life - Catholic authors
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Earlier editions are "by A.C. [i.e. Arthur Crowther] and T.V. [i.e. Thomas Vincent]". Below imprint: Superiorum permissu. Place of publication from Wing. An edition of: "The daily exercise, of the devout Rosarists", published in 1657. With additional engraved title page. Text is continuous despite pagination. Reproduction of the original in the Bodleian Library.
	Sommario/riassunto	eebo-0179

2.	Record Nr.	UNINA9910484014203321
	Titolo	Selected Areas in Cryptography : 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006, Revised Selected Papers / / edited by Eli Biham, Amr M. Youssef
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
	ISBN	3-540-74462-2
	Edizione	[1st ed. 2007.]
	Descrizione fisica	1 online resource (XI, 395 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 4356
	Disciplina	001.5436
	Soggetti	Cryptography
		Data encryption (Computer science)
		Data protection
		Electronic data processing - Management
		Algorithms
		Computer networks
		Application software
		Cryptology
		Data and Information Security
		IT Operations
		Computer Communication Networks
		Computer and Information Systems Applications
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Block Cipher Cryptanalysis -- Improved DST Cryptanalysis of IDEA -- Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192 -- Related-Key Rectangle Attack on the Full SHACAL-1 -- Stream Cipher Cryptanalysis I -- Cryptanalysis of Achterbahn-Version 2 -- Cryptanalysis of the Stream Cipher ABC v2 -- The Design of a Stream Cipher LEX -- Dial C for Cipher -- Improved Security Analysis of XEX and LRW Modes -- Extended Hidden Number Problem and Its Cryptanalytic Applications -- Changing the Odds Against Masked Logic -- Advances on Access-Driven Cache Attacks on AES --

Blind Differential Cryptanalysis for Enhanced Power Attacks -- Efficient Implementations I -- Efficient Implementations of Multivariate Quadratic Systems -- Unbridle the Bit-Length of a Crypto-coprocessor with Montgomery Multiplication -- Delaying and Merging Operations in Scalar Multiplication: Applications to Curve-Based Cryptosystems -- Stream Cipher Cryptanalysis II -- On the Problem of Finding Linear Approximations and Cryptanalysis of Pomaranch Version 2 -- Multi-pass Fast Correlation Attack on Stream Ciphers -- Crossword Puzzle Attack on NLS -- Invited Talk -- When Stream Cipher Analysis Meets Public-Key Cryptography -- Efficient Implementations II -- On Redundant ?-Adic Expansions and Non-adjacent Digit Sets -- Pairing Calculation on Supersingular Genus 2 Curves -- Efficient Divisor Class Halving on Genus Two Curves -- Message Authentication on 64-Bit Architectures -- Some Notes on the Security of the Timed Efficient Stream Loss-Tolerant Authentication Scheme -- Constructing an Ideal Hash Function from Weak Ideal Compression Functions -- Provably Good Codes for Hash Function Design.

Sommario/riassunto	This book constitutes the thoroughly refereed post-proceedings of the 13th International Workshop on Selected Areas in Cryptography, SAC 2006, held in Montreal, Canada in August 2006. The 25 revised full papers presented together with 2 invited talks were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections on block cipher cryptanalysis, stream cipher cryptanalysis, block and stream ciphers, side-channel attacks, efficient implementations, message authentication codes, and hash functions.