1.	Record Nr.	UNINA9910790365003321
	Autore	Sinkov Abraham <1907->
	Titolo	Elementary cryptanalysis : a mathematical approach / / Abraham Sinkov [[electronic resource]]
	Pubbl/distr/stampa	Washington : , : Mathematical Association of America, , 2009
	ISBN	0-88385-937-8
	Edizione	[Second edition.]
	Descrizione fisica	1 online resource (xiv, 212 pages) : digital, PDF file(s)
	Collana	Anneli Lax New Mathematical Library, , 2643-5586 ; ; v. 22 Anneli Lax new mathematical library ; ; v. 22
	Disciplina	652.80151
	Soggetti	Cryptography - Mathematics Ciphers - Mathematics
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Title from publisher's bibliographic system (viewed on 02 Oct 2015).
	Nota di bibliografia	Includes bibliographical references (p. 205-206) and index.
	Nota di contenuto	1. Monoalphabetic ciphers using additive alphabets -- 2. General monoalphabetic substitution -- 3. Polyalphabetic substitution -- 4. Polygraphic systems -- 5. Transposition -- 6. RSA encryption -- 7. Perfect security: one-time pads.
	Sommario/riassunto	Originally published in the New Mathematical Library almost half a century ago, this charming book explains how to solve cryptograms based on elementary mathematical principles, starting with the Caesar cipher and building up to progressively more sophisticated substitution methods. Todd Feil has updated the book for the technological age by adding two new chapters covering RSA public-key cryptography, one-time pads, and pseudo-random-number generators. Exercises are given throughout the text that will help the reader understand the concepts and practice the techniques presented. Software to ease the drudgery of making the necessary calculations is made available. The book assumes minimal mathematical prerequisites and therefore explains from scratch such concepts as summation notation, matrix multiplication, and modular arithmetic. Even the mathematically sophisticated reader, however, will find some of the exercises challenging. (Answers to the exercises appear in an appendix.)