

1. Record Nr.	UNINA9910461902303321
Autore	Sinkov Abraham <1907->
Titolo	Elementary cryptanalysis [[electronic resource]] : a mathematical approach // Abraham Sinkov
Pubbl/distr/stampa	[Washington, D.C.], : Mathematical Association of America Cambridge, : Cambridge University Press [distributore], c2009
ISBN	0-88385-937-8
Edizione	[2nd ed. /]
Descrizione fisica	1 online resource (227 p.)
Collana	Anneli Lax new mathematical library ; ; v. 22
Altri autori (Persone)	FeilTodd <1951->
Disciplina	652.80151
Soggetti	Cryptography - Mathematics Ciphers - Mathematics Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references (p. 205-206) and index.
Nota di contenuto	<p>""cover ""; ""copyright page ""; ""title page ""; ""Contents""; ""Preface to the First Edition""; ""Preface to the Second Edition""; ""1 Monoalphabetic Ciphers Using Additive Alphabets""; ""1.1 The Caesar Cipher""; ""Exercises""; ""1.2 Modular arithmetic""; ""Exercises""; ""1.3 Additive alphabets""; ""Exercises""; ""1.4 Solution of additive alphabets by completing the plain component""; ""Exercises""; ""1.5 Solving additive alphabets by frequency considerations""; ""Exercises""; ""1.6 Alphabets based on multiplications of the normal sequence""; ""Exercises""</p> <p>""1.7 Solution of multiplicative alphabets""""Exercises""; ""1.8 Affine ciphers""; ""Exercises""; ""2 General Monoalphabetic Substitution""; ""2.1 Mixed alphabets""; ""Exercises""; ""2.2 Solution of mixed alphabet ciphers""; ""Exercises""; ""2.3 Solution of monoalphabets in five letter groupings""; ""Exercises""; ""2.4 Monoalphabets with symbols as cipher equivalents""; ""Exercises""; ""3 Polyalphabetic Substitution""; ""3.1 Polyalphabetic ciphers""; ""Exercises""; ""3.2 Recognition of polyalphabetic ciphers""; ""Exercises""; ""3.3 Determination of number of alphabets""; ""Exercises""</p> <p>""3.4 Solution of individual alphabets, if additive""""Exercises""; ""3.5 Polyalphabetic ciphers with a mixed plain sequence""; ""3.6 Matching alphabets""; ""Exercises""; ""3.7 Reduction of a polyalphabetic cipher to</p>

a monoalphabet"; "3.8 Polyalphabetic ciphers with mixed cipher sequences"; "3.9 General comments about polyalphabetic ciphers"; "Exercises"; "4 Polygraphic Systems"; "4.1 Digraphic ciphers based on linear transformationsa€?matrices"; "Exercises"; "4.2 Multiplication of matricesa€?inverses"; "Exercises"; "4.3 Involutory transformations"; "Exercises"; "4.4 Recognition of digraphic ciphers"; "4.5 Solution of a linear transformation"; "Exercises"; "4.6 How to make the Hill System more secure"; "5 Transposition"; "5.1 Columnar transposition"; "Exercises"; "5.2 Solution of transpositions with completely filled rectangles"; "Exercises"; "5.3 Incompletely filled rectangles"; "Exercises"; "5.4 Solution of incompletely filled rectanglesa€?probable word method"; "Exercises"; "5.5 Incompletely filled rectanglesa€?general case"; "Exercises"; "5.6 Repetitions between messages; identical length messages"; "Exercises"; "6 RSA Encryption"; "6.1 Public-key encryption"; "6.2 The RSA method"; "6.3 Creating the RSA keys"; "Exercises"; "6.4 Why RSA worksa€?Fermata€?s Little Theorem"; "Exercises"; "6.5 Computational considerations"; "Exercises"; "6.6 Maple and Mathematica for RSA"; "Exercises"; "6.7 Breaking RSA and signatures"; "Exercises"; "7 Perfect Securitya€?One-time Pads"; "7.1 One-time pads"; "Exercises"; "7.2 Pseudo-random number generators"; "Exercises"; "Appendix A: Tables"; "Table of digraphic frequencies"; "Log Weights"; "Frequencies of the letters of the alphabet in a sample of 1000 letters, arranged alphabetically and by frequency."

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.)