

Cambridge University Press

052181054X - Codes and Ciphers: Julius Caesar, the Enigma and the Internet

R. F. Churchhouse

Frontmatter

[More information](#)

Codes and ciphers

The design of code and cipher systems has undergone major changes in modern times. Powerful personal computers have resulted in an explosion of e-banking, e-commerce and e-mail, and as a consequence the encryption of communications to ensure security has become a matter of public interest and importance. This book describes and analyses many cipher systems ranging from the earliest and elementary to the most recent and sophisticated, such as RSA and DES, as well as wartime machines such as the Enigma and Hagelin, and ciphers used by spies. Security issues and possible methods of attack are discussed and illustrated by examples. The design of many systems involves advanced mathematical concepts and these are explained in detail in a major appendix. This book will appeal to anyone interested in codes and ciphers as used by private individuals, spies, governments and industry throughout history and right up to the present day.

ROBERT CHURCHHOUSE is Emeritus Professor of Computing Mathematics at Cardiff University and has lectured widely on mathematics and cryptanalysis at more than 50 universities and institutes throughout the world. He is also the co-author of books on computers in mathematics, computers in literary and linguistic research, and numerical analysis.

Cambridge University Press

052181054X - Codes and Ciphers: Julius Caesar, the Enigma and the Internet

R. F. Churchhouse

Frontmatter

[More information](#)

Codes and ciphers

Julius Caesar, the Enigma and the internet

R. F. CHURCHHOUSE



CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press
052181054X - Codes and Ciphers: Julius Caesar, the Enigma and the Internet
R. F. Churchhouse
Frontmatter
[More information](#)

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa
<http://www.cambridge.org>

© R. F. Churchhouse 2002

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2002

Printed in the United Kingdom at the University Press, Cambridge

Typeface Lexicon (*The Enschedé Font Foundry*) 9/13 pt System QuarkXPress™ [SE]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

Churchhouse, R. F.
Codes and ciphers: Julius Caesar, the Enigma, and the Internet / R. F. Churchhouse.
p. cm.

Includes bibliographical references and index.
ISBN 0 521 81054 X – ISBN 0 521 00890 5 (pbk.)
1. Cryptography. 2. Ciphers. I. Title.

Z103 .C48 2002
652'.8–dc21 2001037409

ISBN 0 521 81054 X hardback
ISBN 0 521 00890 5 paperback

Contents

Preface ix

- 1 Introduction 1
 - Some aspects of secure communication 1
 - Julius Caesar's cipher 2
 - Some basic definitions 3
 - Three stages to decryption: identification, breaking and setting 4
 - Codes and ciphers 5
 - Assessing the strength of a cipher system 7
 - Error detecting and correcting codes 8
 - Other methods of concealing messages 9
 - Modular arithmetic 10
 - Modular addition and subtraction of letters 11
 - Gender 11
 - End matter 12
- 2 From Julius Caesar to simple substitution 13
 - Julius Caesar ciphers and their solution 13
 - Simple substitution ciphers 15
 - How to solve a simple substitution cipher 17
 - Letter frequencies in languages other than English 24
 - How many letters are needed to solve a simple substitution cipher? 26
- 3 Polyalphabetic systems 28
 - Strengthening Julius Caesar: Vigenère ciphers 28
 - How to solve a Vigenère cipher 30
 - Indicators 33
 - Depths 34
 - Recognising 'depths' 34
 - How much text do we need to solve a Vigenère cipher? 37
 - Jefferson's cylinder 37

vi CONTENTS

- 4 Jigsaw ciphers 40
 - Transpositions 40
 - Simple transposition 40
 - Double transposition 44
 - Other forms of transposition 48
 - Assessment of the security of transposition ciphers 51
 - Double encipherment in general 52
- 5 Two-letter ciphers 54
 - Monograph to digraph 54
 - MDTM ciphers 56
 - Digraph to digraph 58
 - Playfair encipherment 59
 - Playfair decipherment 60
 - Cryptanalytic aspects of Playfair 61
 - Double Playfair 61
- 6 Codes 64
 - Characteristics of codes 64
 - One-part and two-part codes 65
 - Code plus additive 67
- 7 Ciphers for spies 72
 - Stencil ciphers 73
 - Book ciphers 75
 - Letter frequencies in book ciphers 79
 - Solving a book cipher 79
 - Indicators 86
 - Disastrous errors in using a book cipher 86
 - 'GARBO's ciphers 88
 - One-time pad 92
- 8 Producing random numbers and letters 94
 - Random sequences 94
 - Producing random sequences 95
 - Coin spinning 95
 - Throwing dice 96
 - Lottery type draws 97
 - Cosmic rays 97
 - Amplifier noise 97
 - Pseudo-random sequences 98
 - Linear recurrences 99
 - Using a binary stream of key for encipherment 100
 - Binary linear sequences as key generators 101

Cambridge University Press

052181054X - Codes and Ciphers: Julius Caesar, the Enigma and the Internet

R. F. Churchhouse

Frontmatter

[More information](#)

- Cryptanalysis of a linear recurrence 104
- Improving the security of binary keys 104
- Pseudo-random number generators 106
- The mid-square method 106
- Linear congruential generators 107
- 9 The Enigma cipher machine 110
 - Historical background 110
 - The original Enigma 112
 - Encipherment using wired wheels 116
 - Encipherment by the Enigma 118
 - The Enigma plugboard 121
 - The Achilles heel of the Enigma 121
 - The indicator ‘chains’ in the Enigma 125
 - Aligning the chains 128
 - Identifying R1 and its setting 128
 - Doubly enciphered Enigma messages 132
 - The Abwehr Enigma 132
- 10 The Hagelin cipher machine 133
 - Historical background 133
 - Structure of the Hagelin machine 134
 - Encipherment on the Hagelin 135
 - Choosing the cage for the Hagelin 138
 - The theoretical ‘work factor’ for the Hagelin 142
 - Solving the Hagelin from a stretch of key 143
 - Additional features of the Hagelin machine 147
 - The slide 147
 - Identifying the slide in a cipher message 148
 - Overlapping 148
 - Solving the Hagelin from cipher texts only 150
- 11 Beyond the Enigma 153
 - The SZ42: a pre-electronic machine 153
 - Description of the SZ42 machine 155
 - Encipherment on the SZ42 155
 - Breaking and setting the SZ42 158
 - Modifications to the SZ42 159
- 12 Public key cryptography 161
 - Historical background 161
 - Security issues 163
 - Protection of programs and data 163
 - Encipherment of programs, data and messages 164

viii CONTENTS

	The key distribution problem	166
	The Diffie–Hellman key exchange system	166
	Strength of the Diffie–Hellman system	168
13	Encipherment and the internet	170
	Generalisation of simple substitution	170
	Factorisation of large integers	171
	The standard method of factorisation	172
	Fermat’s ‘Little Theorem’	174
	The Fermat–Euler Theorem (as needed in the RSA system)	175
	Encipherment and decipherment keys in the RSA system	175
	The encipherment and decipherment processes in the RSA system	178
	How does the key-owner reply to correspondents?	182
	The Data Encryption Standard (DES)	183
	Security of the DES	184
	Chaining	186
	Implementation of the DES	186
	Using both RSA and DES	186
	A salutary note	187
	Beyond the DES	187
	Authentication and signature verification	188
	Elliptic curve cryptography	189
	Appendix	190
	Solutions to problems	218
	<i>References</i>	230
	<i>Name index</i>	235
	<i>Subject index</i>	237

Preface

Virtually anyone who can read will have come across codes or ciphers in some form. Even an occasional attempt at solving crosswords, for example, will ensure that the reader is acquainted with anagrams, which are a form of cipher known as *transpositions*. Enciphered messages also appear in children's comics, the personal columns of newspapers and in stories by numerous authors from at least as far back as Conan Doyle and Edgar Allan Poe.

Nowadays large numbers of people have personal computers and use the internet and know that they have to provide a password that is enciphered and checked whenever they send or receive e-mail. In business and commerce, particularly where funds are being transferred electronically, authentication of the contents of messages and validation of the identities of those involved are crucial and encipherment provides the best way of ensuring this and preventing fraud.

It is not surprising then that the subject of codes and ciphers is now much more relevant to everyday life than hitherto. In addition, public interest has been aroused in 'codebreaking', as it is popularly known, by such books and TV programmes as those that have been produced following the declassification of some of the wartime work at Bletchley, particularly on the Enigma machine.

Cipher systems range in sophistication from very elementary to very advanced. The former require no knowledge of mathematics whereas the latter are often based upon ideas and techniques which only graduates in mathematics, computer science or some closely related discipline are likely to have met. Perhaps as a consequence of this, most books on the subject of codes and ciphers have tended either to avoid mathematics entirely or to assume familiarity with the full panoply of mathematical ideas, techniques, symbols and jargon.

It is the author's belief, based upon experience, that there is a middle way and that, without going into all the details, it is possible to convey to non-specialists the essentials of some of the mathematics involved even in the more modern cipher systems. My aim therefore has been to introduce the general reader to a number of codes and ciphers, starting with the ancient and elementary and progressing, via some of the wartime cipher machines, to systems currently in commercial use. Examples of the use, and methods of solution, of various cipher systems are given but in those cases where the solution of a realistically sized message would take many pages the method of solution is shown by scaled-down examples.

In the main body of the text the mathematics, including mathematical notation and phraseology, is kept to a minimum. For those who would like to know more, however, further details and explanations are provided in the mathematical appendix where, in some cases, rather more information than is absolutely necessary is given in the hope of encouraging them to widen their acquaintance with some fascinating and useful areas of mathematics, which have applications in 'codebreaking' and elsewhere.

I am grateful to Cardiff University for permission to reproduce Plates 9.1 to 9.4 inclusive, 10.1 and 10.2, and to my son John for permission to reproduce Plate 11.1. I am also grateful to Dr Chris Higley of Information Services, Cardiff University, for material relating to Chapter 13 and to the staff at CUP, particularly Roger Astley and Peter Jackson, for their helpfulness throughout the preparation of this book.