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.

Codes and ciphers

Julius Caesar, the Enigma and the internet

R. F. CHURCHHOUSE

CAMBRIDGE
UNIVERSITY PRESS

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

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

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.