

SPRINGER BRIEFS IN COMPUTER SCIENCE

John F. Dooley

A Brief History of Cryptology and Cryptographic Algorithms



Springer

SpringerBriefs in Computer Science

Series Editors

Stan Zdonik

Peng Ning

Shashi Shekhar

Jonathan Katz

Xindong Wu

Lakhmi C. Jain

David Padua

Xuemin Shen

Borko Furht

V. S. Subrahmanian

Martial Hebert

Katsushi Ikeuchi

Bruno Siciliano

For further volumes:

<http://www.springer.com/series/10028>

John F. Dooley

A Brief History of Cryptology and Cryptographic Algorithms

 Springer

John F. Dooley
Department of Computer Science
Knox College
Galesburg, IL
USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-3-319-01627-6 ISBN 978-3-319-01628-3 (eBook)
DOI 10.1007/978-3-319-01628-3
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013945798

© The Author(s) 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

For diane

Preface

Cryptology is the science of secret communications. You are likely to use some form of cryptology every day. If you login to a computer you are using cryptology in the form of a one-way hash function that protects your password. If you buy something over the Internet, you are using two different forms of cryptology—public-key cryptography to set up the encrypted network connection between you and the vendor and a symmetric key algorithm to finish your transaction. These days much of the cryptology that is in use is invisible, just like the examples given. It wasn't always so. The story of cryptology goes back at least 2,500 years and for most of that time it was considered an arcane science, known only to a few and jealously guarded by governments, exiled kings and queens, and religious orders. For a time in the European Middle Ages it was even considered to be a form of magic. It is only recently, really beginning in the twentieth century, that cryptology has become known and studied outside the realms of secret government agencies. Even more recently, the study of cryptology has moved from a branch of linguistics to having a firm foundation in mathematics.

This book is a brief history of cryptology from the time of Julius Caesar up through around the year 2001. It also covers the different types of cryptographic algorithms used to create secret messages, and it discusses methods for breaking secret messages. There are several examples in the text that illustrate the algorithms in use. Being 'brief', it is not meant to be a comprehensive history of either cryptology or the algorithms themselves. Rather I have tried to touch on a subset of the important stories in cryptologic history and the algorithms and people involved. Most of the chapters begin with a story that tries to illustrate the importance of cryptology in that particular time period.

I teach an upper-level undergraduate survey course in *Cryptography and Computer Security* and the contents of this book are about the first quarter of that course where I do a review of the different cryptographic algorithms from a historical perspective. My goal in that part of the course is to give students a better understanding of *how* we got from the early days of pencil and paper secret messages to a place where cryptology is pervasive and invisible. This book could easily serve as the text for that part of a course on computer or network security or as a supplemental text for a stand-alone course on computer security. No mathematics is required beyond what a computer science or mathematics student would see

in a course on discrete mathematics. If you want to pursue a more comprehensive treatment of the history of cryptology, I recommend David Kahn's excellent book *The Codebreakers: The Story of Secret Writing*, and for a more mathematical treatment, Craig Bauer's equally good *Secret History: The Story of Cryptology*.

Acknowledgments

I would like to thank the library staff at Knox College for their patience and professional help in finding copies of many of the articles and letters referenced here. I would also like to thank the staff of the National Archives and Records Administration (NARA) in College Park, MD, Librarian René Stein at the Research Library at the National Cryptologic Museum in Ft. Meade, MD, and Paul Barron and Jeffrey Kozak of the George C. Marshall Foundation Research Library in Lexington, VA for their excellent help. And of course, thanks to Diane, who inspires me, encourages me, and—above the call of duty—reads and edits everything I write.

This research was funded in part by a grant from the Andrew W. Mellon Foundation and by the Office of the Dean of the College at Knox College.

Contents

1 Introduction: A Revolutionary Cipher	1
1.1 A Traitorous Doctor	1
1.2 A Few (Vocabulary) Words About Cryptology	4
1.3 Codes	5
1.4 Ciphers	6
1.5 Substitution Ciphers	7
1.6 Transposition Ciphers	8
References	9
2 Cryptology Before 1500: A Bit of Magic	11
2.1 Veni, Vidi, Cipher	11
2.2 Cryptology in the Middle Ages	12
2.3 Frequency Analysis, the First Cryptanalytic Tool	12
References	17
3 The Black Chambers: 1500–1776	19
3.1 Mary, Queen of Scots and the Spymaster	19
3.2 Nomenclators	23
3.3 The Black Chambers	23
3.4 The Next Complexity: Polyalphabetic Substitution	24
References	29
4 Crypto Goes to War: 1861–1865	31
4.1 Technology Goes to War	31
4.2 The Union Tries a Route	32
4.3 Crypto for the Confederates	35
4.4 Solving a Vigenère Cipher	36
References	42
5 Crypto and the War to End All Wars: 1914–1918	43
5.1 The Americans Start from Behind	43
5.2 America Catches Up	44
5.3 The A.E.F in France	45
5.4 Ciphers in the Great War: The Playfair	46

5.5 Ciphers in the Great War: The ADFGVX Cipher. 48

5.6 A New Beginning. 50

References. 51

6 The Interwar Period 1919–1939 53

6.1 Herbert O. Yardley and the Cipher Bureau. 53

6.2 William Friedman and the Signal Intelligence Service 58

References. 60

7 The Coming of the Machines: 1918–1945. 63

7.1 Early Cipher Machines. 63

7.2 The Rotor Makes its Appearance 64

7.3 How does the Enigma Work?. 66

7.4 Solving the Enigma: Turing, Marian, and the Bombe 70

7.5 SIGABA: Friedman and Rowlett’s Triumph 71

7.6 How Does the SIGABA Work? 72

References. 74

8 The Machines Take Over: Computer Cryptography. 75

8.1 The Shoulders of Giants. 75

8.2 Modern Computer Cipher Algorithms: The DES. 77

8.2.1 How Does the DES Work?. 77

8.2.2 The $f()$ Function 79

8.2.3 The Key Scheduler 79

8.2.4 Discussion of DES 80

8.3 The Advanced Encryption Standard. 82

References. 85

9 Alice and Bob and Whit and Martin: Public Key Crypto. 87

9.1 The Problem with Symmetric Ciphers. 87

9.2 Enter Whit and Martin 88

9.3 The Key Exchange Problem. 88

9.4 Public-Key Cryptography Appears. 90

9.5 Authentication is a Problem Too 91

9.6 Implementing Public-Key Cryptography: The RSA Algorithm. 92

9.6.1 RSA Key Generation 93

9.6.2 Encrypting and Decrypting 94

9.7 Analysis of RSA. 94

9.8 Applications of Public-Key Cryptography. 94

References. 96

Index. 97

Chapter 1

Introduction: A Revolutionary Cipher

Abstract Cryptology is the science of secret writing. It is made up of two halves; cryptography consists of the techniques for creating systems of secret writing and cryptanalysis encompasses the techniques of breaking them. Over the past 2,500 years, cryptology has developed numerous types of systems to hide messages and subsequently a rich vocabulary in which to describe them. In this chapter we introduce the reader to the vocabulary of cryptology, explain the differences between codes and ciphers and begin the discussion of how to decipher an unknown message.

1.1 A Traitorous Doctor

In the summer of 1775, the American revolutionary forces were near a state of chaos. The main body of the American force was laying siege to Boston. The Continental Congress had just appointed George Washington of Virginia as commander of all continental forces. Money was scarce, enlistments were short, and most of the Continental Army was comprised of colonial militias with little training, no common equipment, and no idea of the enemy they faced. The officer corps was not in much better shape, with most of the colonial officers having had little or no command experience. Logistics were haphazard, artillery was practically non-existent, and the British held all the major urban areas in the thirteen colonies. The last thing that Lieutenant General Washington needed in September 1775 was a Tory spy in his midst sending secret messages to the British. But that is exactly what he got.

In mid-August 1775 a young patriot from Newport, Rhode Island named Godfrey Wenwood received a request from a former lover. It was to deliver a letter to a “Major Cane in Boston on his magisty’s service”. Wenwood was rather reluctant to deliver the letter, assuming, quite correctly, that Major Cane was a British