SPRINGER BRIEFS IN COMPUTER SCIENCE

John F. Dooley

A Brief History of Cryptology and Cryptographic Algorithms

KNOX COLLEGE

Springer

SpringerBriefs in Computer Science

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

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

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

J. F. Dooley, *A Brief History of Cryptology and Cryptographic Algorithms*,
SpringerBriefs in Computer Science, DOI: 10.1007/978-3-319-01628-3_1,