

Cambridge University Press

0521855225 - Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers

R. A. Ratcliff

Frontmatter

[More information](#)

DELUSIONS OF INTELLIGENCE

Enigma, Ultra, and the End of Secure Ciphers

In 1974, the British government admitted that its WWII secret intelligence organization had read Germany's ciphers on a massive scale. The intelligence from these decrypts influenced on the Atlantic, the Eastern Front and Normandy. Why did the Germans never realize the Allies had so thoroughly penetrated their communications? As German intelligence experts conducted numerous internal investigations that all certified their ciphers' security, the Allies continued to break more ciphers and to plug their own communication leaks. How were the Allies able to so thoroughly exploit Germany's secret messages? How did they keep their tremendous success a secret? What flaws in Germany's organization allowed this counterintelligence failure and how can today's organizations learn to avoid similar disasters?

This book, the first comparative study of WWII sigint (signals intelligence), analyzes the characteristics that allowed the Allies sigint success and that fostered the German blindness to Enigma's compromise.

R. A. Ratcliff currently lives and consults in Silicon Valley. She has lectured on cryptologic history at the National Security Agency's intelligence school and taught history at the University of San Francisco and University of California at Berkeley. She is the author of articles for *Intelligence* and *National Security and Cryptologia*

Cambridge University Press

0521855225 - Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers

R. A. Ratcliff

Frontmatter

[More information](#)

Delusions of Intelligence

ENIGMA, ULTRA, AND THE END OF
SECURE CIPHERS

R. A. Ratcliff



CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press

0521855225 - Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers

R. A. Ratcliff

Frontmatter

[More information](#)

CAMBRIDGE UNIVERSITY PRESS

Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press

40 West 20th Street, New York, NY 10011-4211, USA

www.cambridge.org

Information on this title: www.cambridge.org/9780521855228

© R. A. Ratcliff 2006

This publication 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 2006

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication Data

Ratcliff, R. A. (Rebecca Ann), 1963–

Delusions of intelligence : Enigma, Ultra, and the end of secure ciphers / R. A. Ratcliff.

p. cm.

Includes bibliographical references and index.

ISBN 0-521-85522-5 (hardcover)

1. Enigma cipher system. 2. ULTRA (Intelligence system) 3. World War, 1939–1945 – Cryptography. 4. World War, 1939–1945 – Electronic intelligence – Great Britain. I. Title.

D810.C88R37 2006

940-54'8743 – dc22 2005036466

ISBN-13 978-0-521-85522-8 hardback

ISBN-10 0-521-85522-5 hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party Internet Web sites referred to in this publication and does not guarantee that any content on such Web sites is, or will remain, accurate or appropriate.

Cambridge University Press

0521855225 - Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers

R. A. Ratcliff

Frontmatter

[More information](#)

*For Chris,
Nick, and Alec
who slowed progress on the book
and have made life marvelous*

CONTENTS

<i>List of Illustrations</i>	<i>page</i> ix
<i>Glossary of Terms Used</i>	xi
<i>Acknowledgments</i>	xv
Introduction: The Traitor in Our Midst	I
1 Enigma: The Development and Use of a New Technology	11
2 Early Triumph: German Intelligence Successes	33
3 Of No Mutual Assistance: Compartmentalization and Competition in German Signals Intelligence	56
4 The Work of Station X: Centralizing Allied Cryptology at Bletchley Park	72
5 Protecting Boniface: Allied Security, Disguise, and Dissemination of Ultra	106
6 The Illusion of Security: The German Explanations for Allied Successes	127
7 A Long-Standing Anxiety: Allied Communications Security	159
8 Determined Answers: Structural Problems in German Signal Intelligence	180

viii • Contents

9	Enter the Machines: The Role of Science and Machines in the Cryptologic War	198
	Conclusion: Recognizing the End of Security	214
	Notes	237
	Bibliography	287
	Index	305

LIST OF ILLUSTRATIONS

CHARTS

Basic Enigma Wiring Diagram	<i>page</i> 15
German Sigint Organization	38
British Sigint Organization	73

PHOTOGRAPHS

Enigma machine rotors (three-rotor machine)	14
The American M-209	49
SIS (the U.S. Army’s Signals Intelligence Service) in 1937	78
The Manor House at Bletchley Park	85
The U.S. Navy four-rotor Bombe	91
A month of three-rotor Enigma settings	96
The British Typex machine	121
Großadmiral Karl Dönitz’s surrender	157
M-209 in the field	165
Sigaba Machine (U.S.A.)	176
Lorenz SZ 40/42	206
Colossus	212

GLOSSARY OF TERMS USED

Admiralty	British Royal Navy (the Marine generally used this term)
Arlington Hall	A former girl's school that housed the main American naval decryption effort near Washington, D.C.
B-Dienst	The Marine observation (Beobachtung) service responsible for intercepting radio signals
Bombe	Electromechanical deciphering machine first designed by Polish cryptanalysts to discover the daily settings of the Enigma
BP	Bletchley Park, the primary location of GC&CS and the cracking of Enigma
Colossus	British-designed protocomputer used primarily to crack the Geheimschreiber
cribs	Known message texts or phrases used as possible solutions for unknown texts
cryptology	The development of codes and ciphers (cryptography) and the cracking of the same (cryptanalysis); the study of codes and ciphers
decrypt	A signal that has been decrypted by the enemy
depths	More than one message being encrypted at the same or nearly the same setting; a breach of standard security procedures and an excellent entry point for cryptanalysts
D/F	Direction Finding – the process of locating the source of a (usually radio) signal through triangulation
discriminant	A group of letters placed in front of the encrypted text to indicate the setup used (e.g., the alignment of the

xii • Glossary of Terms Used

	Enigma rotors) at the start of the message’s encipherment and hence the degree of secrecy of the message or to distinguish one type or section of traffic from another
Enigma	Commercial name, used by both Germans and Allies, for the (portable) electromechanical enciphering machine used by the branches of the German Wehrmacht, SS, and railroads
Enigma M	The Marine’s version of the Enigma machine
Fish	British cover name for German radioteletype non-Morse intercepts and ciphering machines, specifically the Siemens Geheimschreiber T-52 series (code-named Sturgeon) and the Lorenz SZ 40/42 machines (code-named Tunny)
Geheimschreiber	Electromechanical enciphering machine used by the Germans for messages sent by wire (i.e., nonradio)
Heer	German Army
Huff/Duff	High Frequency Direction Finding (D/F)
Inspk. 7	OKH/Inspektorat 7/VI, which included the Heer’s cryptanalytic unit
Index	A room-size index card catalog of crucial terms and people mentioned in decrypted Enigma signals
indicator	One or more letter or figure groups placed somewhere in the message to indicate the key or subtractor used
intercept	Radio signals “caught” by the enemy’s interceptors, usually for location through D/F or for decryption
key	The setting for a cipher (e.g., Enigma machine) in a particular network for a specific period, commonly one day (hence, daily key)
Luftwaffe	German Air Force
Magic	American code name for decrypts from Purple
Marine	German Navy
Metox	A German radar warning device
MI6	Military Intelligence department 6 – responsible for external intelligence (comparable to the modern CIA)
MND	Marine Nachrichtendienst, the information service of the German Navy

Glossary of Terms Used • xiii

OKW	Oberkommando der Wehrmacht (Wehrmacht high command)
one-time pad	A code based on sheets of substitutions to be used once only. Highly secure
Purple	American code name for the high-grade Japanese diplomatic cipher machine used just before and during the war
re-encodements	Signals encrypted in more than one Enigma net (repeats)
rotors	The turning wired wheels inside electromechanical cipher machines, such as Enigma, which created a set of electrical paths and the machine’s enciphering component
RSHA	Reichssicherheit Haupt Amt (Primary Reich Security Bureau), the Nazi government security and intelligence agency that eventually absorbed the Wehrmacht’s Abwehr
Shark	Allied code name for the Enigma M used for U-boat communications
Sigaba	American high-grade electromechanical cipher machine, more advanced than Enigma
sigint	Signals intelligence or any intelligence from signals, including D/F, Traffic Analysis, and decrypts
SLUs	Special Liaison Units, the teams responsible for protecting and transmitting Ultra Intelligence to battle-field commanders
TA	Traffic Analysis, the tracking of signals, usually undecrypted, by origin, length, and number, and comparing this information with past experience to project bombing raids, offensives, and retreats
TICOM	Target Intelligence Committee, Anglo-American teams sent into German territory around the end of the war to gather documents and personnel with information on intelligence, cryptology, and technological developments
Triton	German code name for the Enigma M used for U-boat communications
Typex	British electromechanical cipher machine, more advanced than Enigma

xiv • Glossary of Terms Used

Ultra	Allied code name for intelligence derived from Enigma decrypts
WAVES, WRENS, WAAFS	The women’s auxiliary forces who assisted in cracking Enigma, often running the Bombes
Walze	Rotors in the German Enigma machines
Watch	The group of people at BP staffing an eight-hour shift of translating, typing, and analyzing Ultra
Wehrmacht	German Armed Forces (i.e., Marine, Heer, Luftwaffe, etc.; for most ex-officers, this term excludes the Nazi military and paramilitary groups such as the SS and Waffen SS)
X-B-Dienst	Division of B-Dienst responsible for decryption of enemy codes and ciphers

Cambridge University Press

0521855225 - Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers

R. A. Ratcliff

Frontmatter

[More information](#)

ACKNOWLEDGMENTS

True knowledge comes from the exchange of ideas. No author researches and writes a book without help from many sources – I am no exception. My work rests not just on the foundations of the literature cited, but on the help, ideas, and enthusiasm of numerous people. As the research for this book took me across two continents, numerous archives, and many years, I had help and encouragement from strangers, colleagues, and friends. I cannot attempt to thank all of them, but here, briefly and incompletely, is an attempt to thank some of those helping hands.

I am greatly indebted to the Center for Cryptologic History at the National Security Agency (NSA), its NSA Scholar-in-Residence program, and its staff. David Hatch brought me into the program, opened all kinds of vital doors, and introduced me to some of America's cryptologic geniuses. I had regular help on matters both small and significant from all the staff of the CCH and the National Cryptologic Museum, including Larry Sharp, Rowena Clough, and the late Dave Mowry, who also commented on drafts of this work.

My year at NSA also provided the wisdom and insights of two excellent sigint specialists and historians. Dr. Thomas Johnson has a likely unparalleled knowledge of American intelligence history and practice that I hope will inform our leaders as well as it has me. Robert J. Hanyok has shared his enthusiasm for history and sigint and spent many hours confirming details and procuring photos. Both of these experts have shaped my thinking and writing about cryptology and sigint. Thank you.

I owe much to Wladyslaw Kozaczuk and the late Sir Harry Hinsley for their works and correspondence. Arthur Levinson, Sir Edward Thomas, Alan Stripp, Peter Calvocoressi, and Ralph Bennett all spoke

Cambridge University Press

0521855225 - Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers

R. A. Ratcliff

Frontmatter

[More information](#)

xvi • Acknowledgments

eloquently of Bletchley. The late Cecil and Nancy Phillips provided useful details on the American side. Robert Harris saved me hours in the Public Record Office and kindly kindled interest with his novel *Enigma*. David J. Alvarez connected me with the journal *Intelligence and National Security (INS)* and NSA. Whitfield Diffie, Judith Field, and the British Society for the History of Mathematics prodded me to explore Enigma's mathematics. Brian McCue offered radar and U-boat help and a most marvelous small-world moment. My thanks to Stephen J. Kelley and *Cryptologia*'s Louis Kruh for their interest and information.

Jürgen Rohwer gave me access to his archives and the Bibliothek für Zeitgeschichte and answered numerous questions about German historians, life in the Marine, and the German perspective on Enigma and Ultra. Ralph Erskine and Steve Budiansky pointed out important documents and gave me access to their own writings on World War II sig-int. Wesley K. Wark read a very early version of this work and gave me excellent guidance. Mary Sutphen also offered comments on several chapters.

David Kahn has always been most generous with his time, knowledge, and materials. Although I have tried consciously not to lean too heavily on his excellent foundations, I owe a great debt to his works on cryptology, Enigma, and German intelligence.

Several grants made the research for this work possible, including the NSA residence program, a grant from the Department of Education for initial research and advanced German, and University of California, Berkeley, grants for research, travel, and writing. Sections of Chapter 6 appeared in the journal *Intelligence and National Security*, and I acknowledge their permission to include that material here.

Thanks also to my UCB connections, particularly Deborah Cohen, Takiyoshi Nishiuchi, Patricia Reilly, and Maxine Fredericksen. I still owe much to my doctoral committee: David Cohen, Margaret Anderson, Anthony Adamthwaite, Reginald Zelnick, and the late Art Quinn, who is greatly missed.

Throughout my research, I received crucial assistance from the personnel of several libraries and archives: the Mitarbeitern of the Bibliothek für Zeitgeschichte; the staffs of the Bundes-Militärarchiv and the Auswärtiges Amt's archive; the reference librarians at the PRO; and the staff and volunteers at NSA's National Cryptologic History Museum.

Cambridge University Press

0521855225 - Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers

R. A. Ratcliff

Frontmatter

[More information](#)

Acknowledgments • xvii

My greatest debt of all is to Timothy P. Mulligan of National Archives and Records Administration. The use of technology in archives has improved the researcher's lot tremendously; but no technology, however advanced, can provide a researcher with the depth of information, years of lessons in German naval matters, and numerous gentle nudges toward crucial documents that Tim has provided for more than a decade. Archivists such as he are a national resource, and they are retiring unreplaced. In the midst of its rush to acquire all things electronic, NARA's administration should not neglect this most valuable resource of all.

For the actual writing, I was aided by Sonja Aschenbrenner and Tanja Fassel managing Schnabel and Snüffel, by quiet spots in Stevens Hall, NARA, and Cañada College, by my antique printer's forbearance, and by Chris Gellrich's support and technical assistance. Dr. (med.) Birgit Jödicke not only introduced me to German and provided decades of friendship, including ein Patenkind (Lisa Joanna), she also cast her professional translator's eye over my work (any remaining errors are, of course, mine).

The support and encouragement from family and friends has made this work both possible and a joy. Thanks and appreciation to my parents, who still keep an eye out for all things Enigma-related; to the best siblings ever, Rosemary and Jamie; and to S. G. Hamlen, whose support, encouragement, and keen editorial eye made all the difference and who recommended the Groupthink book ages ago. Jonathan Klein, Anne Wright, and Chris Gellrich kindly agreed to read everything with fresh eyes. I remain forever grateful to James E. Ratcliff, Jr., for mentioning that story about the Poles cracking some code during the war and for subsequently reading everything I passed him on the subject – including the numerous iterations of this work. Thanks Dad.

Finally, thanks to Lewis Bateman for initially adopting the book, and to Eric Crahan and, especially, Frank Smith of Cambridge University Press, who waited patiently through my mergers and acquisitions for the final product.

R. A. Ratcliff
May 2005