ANCHOR BOOKS

eBooks

The Code Book

The Science of Secrecy from Ancient Egypt to Quantum Cryptography

Simon Singh

PRAISE FOR SIMON SINGH AND *The Code Book*

"Singh spins tales of cryptic intrigue in every chapter."

—The Wall Street Journal

"Brings together … the geniuses who have secured communications, saved lives, and influenced the fate of nations. A pleasure to read."

—Chicago Tribune

"Singh pursues the fascinating story [of codes] through the centuries, always providing plenty of detailed examples of ciphers for those who appreciate the intricacies of the medium."

—Los Angeles Times

"Especially effective at putting the reader in the codebreaker's shoes, facing each new, apparently unbreakable code.… Singh does a fine job."

—The New York Times Book Review

"Entertaining.… Singh has a flair for narrative."

—San Francisco Chronicle

"Singh is an interesting mix of scientist and storyteller, and this subject is the perfect mix of true fact and tall tales."

—The San Diego Union-Tribune

"Where would we Information Age ignoramuses be without smart guys like Stephen Jay Gould, the late Carl Sagan, or Simon Singh? They are the troubadours of our time, making complicated subjects understandable and entertaining."

—The Plain Dealer

"In this entertaining survey, the evolution of cryptography is driven by the ongoing struggle between code-makers and codebreakers."

—The New Yorker

“[Singh] is well-equipped to describe all the arcane mathematics in layman’s language.”

—*Forbes*

“Wonderful stories.… Close reading is rewarded with the flash of logical insight that the codebreakers must enjoy.”

—*Hartford Advocate*

“An illuminating and entertaining account.… From the first page, Singh shows his knack both for explaining complex areas of science and telling rip-roaring stories.”

—*New York Law Journal*

“My only regret is that this great book has come far too late. If only someone had given it to me when I was 10, my secret plans for world playground domination might never have been foiled.”

—James Flint, *The Observer* (London)

“Full of fascinating case histories covering the development and practical use of cryptography.”

—*Mail on Sunday* (London)

“Singh has created an authoritative and engrossing read which both explains and humanizes the subject.… This intelligent, exciting book takes its drive from a simple premise-that nothing is as exciting as a secret.”

—*Scotland on Sunday*

SIMON SINGH

The Code Book

Simon Singh received his Ph.D. in physics from Cambridge University. A former BBC producer, he directed an award-winning documentary film on Fermat's Last Theorem that aired on PBS's *Nova* series and wrote the bestselling book, *Fermat's Enigma*. He lives in London, England.

Also by Simon Singh

Fermat's Enigma

The Code Book

The Science of Secrecy
from Ancient Egypt
to Quantum Cryptography

Simon Singh

Anchor Books
A Division of Random House, Inc.
New York

FIRST ANCHOR BOOKS EDITION, SEPTEMBER 2000

 Published in the United States by Anchor Books, a division of Random House, Inc., New York, and simultaneously in Canada by Random House of Canada Limited, Toronto. Originally published in hardcover in the United States by Doubleday, a division of Random House, Inc., New York, and in the United Kingdom by the Fourth Estate, London, in 1999.

Anchor Books and colophon are registered trademarks of Random House, Inc.

The Library of Congress has cataloged the Doubleday edition as follows:
Singh, Simon.
The code book : the evolution of secrecy from Mary Queen of Scots to quantum cryptography / Simon Singh. –1st ed.
p. cm.
1. Cryptography–History. 2. Data encryption (Computer science)–History. I. Title.
Z103.S56 1999
652′.8′09–dc21 99-35261

eISBN: 978-0-307-78784-2

www.anchorbooks.com

v3.1_r2

For my mother and father,

Sawaran Kaur and Mehnga Singh

The urge to discover secrets is deeply ingrained in human nature; even the least curious mind is roused by the promise of sharing knowledge withheld from others. Some are fortunate enough to find a job which consists in the solution of mysteries, but most of us are driven to sublimate this urge by the solving of artificial puzzles devised for our entertainment. Detective stories or crossword puzzles cater for the majority; the solution of secret codes may be the pursuit of a few.

John Chadwick

The Decipherment of Linear B

Contents