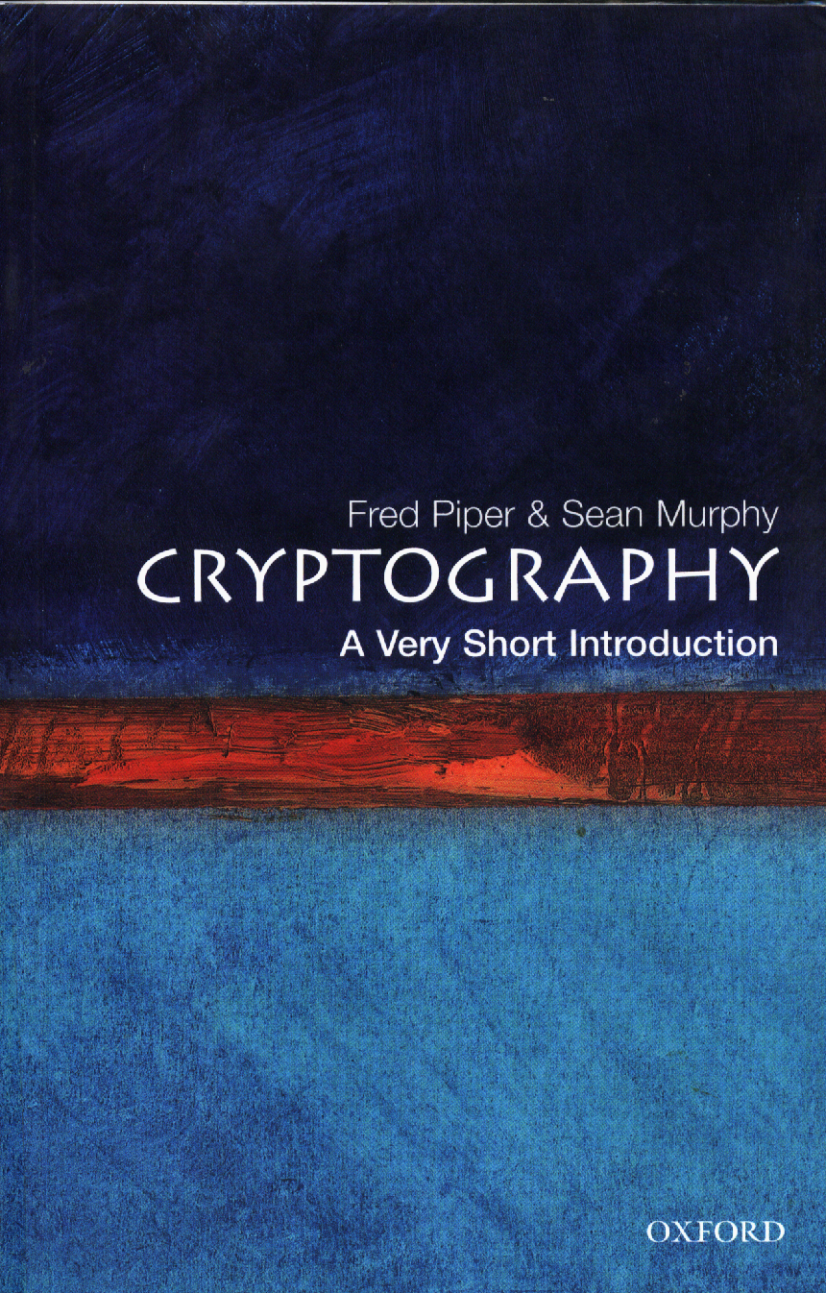
Fred Piper & Sean Murphy
CRYPTOGRAPHY
A Very Short Introduction
OXFORD

IST 2856

Cryptography: A Very Short Introduction

VERY SHORT INTRODUCTIONS are for anyone wanting a stimulating and accessible way in to a new subject. They are written by experts, and have been published in more than 25 languages worldwide.

The series began in 1995, and now represents a wide variety of topics in history, philosophy, religion, science, and the humanities. Over the next few years it will grow to a library of around 200 volumes – a Very Short Introduction to everything from ancient Egypt and Indian philosophy to conceptual art and cosmology.

Very Short Introductions available now:

ANCIENT PHILOSOPHY
Julia Annas
THE ANGLO-SAXON AGE
John Blair
ANIMAL RIGHTS David DeGrazia
ARCHAEOLOGY Paul Bahn
ARCHITECTURE
Andrew Ballantyne
ARISTOTLE Jonathan Barnes
ART HISTORY Dana Arnold
ART THEORY Cynthia Freeland
THE HISTORY OF
ASTRONOMY Michael Hoskin
ATHEISM Julian Baggini
AUGUSTINE Henry Chadwick
BARTHES Jonathan Culler
THE BIBLE John Riches
BRITISH POLITICS
Anthony Wright
BUDDHA Michael Carrithers
BUDDHISM Damien Keown
CAPITALISM James Fulcher
THE CELTS Barry Cunliffe
CHOICE THEORY
Michael Allingham
CHRISTIAN ART Beth Williamson
CLASSICS Mary Beard and
John Henderson
CONTINENTAL PHILOSOPHY
Simon Critchley
COSMOLOGY Peter Coles
CRYPTOGRAPHY
Fred Piper and Sean Murphy
DADA AND SURREALISM
David Hopkins
DARWIN Jonathan Howard
DEMOCRACY Bernard Crick
DESCARTES Tom Sorell
DRUGS Leslie Iversen
THE EARTH Martin Redfern
EGYPTIAN MYTHOLOGY
Geraldine Pinch
EIGHTEENTH-CENTURY
BRITAIN Paul Langford
THE ELEMENTS Philip Ball
EMOTION Dylan Evans
EMPIRE Stephen Howe
ENGELS Terrell Carver
ETHICS Simon Blackburn
THE EUROPEAN UNION
John Pinder
EVOLUTION
Brian and Deborah Charlesworth
FASCISM Kevin Passmore
THE FRENCH REVOLUTION
William Doyle

GLOBALIZATION
Manfred Steger
HEGEL Peter Singer
HEIDEGGER Michael Inwood
HINDUISM Kim Knott
HISTORY John H. Arnold
HOBBES Richard Tuck
HUME A. J. Ayer
IDEOLOGY Michael Freeden
INDIAN PHILOSOPHY
Sue Hamilton
INTELLIGENCE Ian J. Deary
ISLAM Malise Ruthven
JUDAISM Norman Solomon
JUNG Anthony Stevens
KANT Roger Scruton
KIERKEGAARD Patrick Gardiner
THE KORAN Michael Cook
LINGUISTICS Peter Matthews
LITERARY THEORY
Jonathan Culler
LOCKE John Dunn
LOGIC Graham Priest
MACHIAVELLI Quentin Skinner
MARX Peter Singer
MATHEMATICS Timothy Gowers
MEDIEVAL BRITAIN
John Gillingham and
Ralph A. Griffiths
MODERN IRELAND
Senia Pašeta
MOLECULES Philip Ball
MUSIC Nicholas Cook
NIETZSCHE Michael Tanner
NINETEENTH-CENTURY
BRITAIN Christopher Harvie and
H. C. G. Matthew
NORTHERN IRELAND
Marc Mulholland
PAUL E. P. Sanders
PLATO Julia Annas
POLITICS Kenneth Minogue
POLITICAL PHILOSOPHY
David Miller
POSTCOLONIALISM
Robert Young
POSTMODERNISM
Christopher Butler
POSTSTRUCTURALISM
Catherine Belsey
PREHISTORY Chris Gosden
PRESOCRATIC PHILOSOPHY
Catherine Osborne
PSYCHOLOGY Gillian Butler and
Freda McManus
QUANTUM THEORY
John Polkinghorne
ROMAN BRITAIN Peter Salway
ROUSSEAU Robert Wokler
RUSSELL A. C. Grayling
RUSSIAN LITERATURE
Catriona Kelly
THE RUSSIAN REVOLUTION
S. A. Smith
SCHIZOPHRENIA
Chris Frith and Eve Johnstone
SCHOPENHAUER
Christopher Janaway
SHAKESPEARE Germaine Greer
SOCIAL AND CULTURAL
ANTHROPOLOGY
John Monaghan and Peter Just
SOCIOLOGY Steve Bruce
SOCRATES C. C. W. Taylor
SPINOZA Roger Scruton
STUART BRITAIN John Morrill
TERRORISM Charles Townshend
THEOLOGY David F. Ford
THE TUDORS John Guy
TWENTIETH-CENTURY

Available soon:

AFRICAN HISTORY
John Parker and Richard Rathbone
ANCIENT EGYPT Ian Shaw
THE BRAIN Michael O'Shea
BUDDHIST ETHICS
Damien Keown
CHAOS Leonard Smith
CHRISTIANITY Linda Woodhead
CITIZENSHIP Richard Bellamy
CLASSICAL ARCHITECTURE
Robert Tavernor
CLONING Arlene Judith Klotzko
CONTEMPORARY ART
Julian Stallabrass
THE CRUSADES
Christopher Tyerman
DERRIDA Simon Glendinning
DESIGN John Heskett
DINOSAURS David Norman
DREAMING J. Allan Hobson
ECONOMICS Partha Dasgupta
THE END OF THE WORLD
Bill McGuire
EXISTENTIALISM Thomas Flynn
THE FIRST WORLD WAR
Michael Howard
FREE WILL Thomas Pink
FUNDAMENTALISM
Malise Ruthven
HABERMAS Gordon Finlayson
HIEROGLYPHS
Penelope Wilson
HIROSHIMA B. R. Tomlinson
HUMAN EVOLUTION
Bernard Wood
INTERNATIONAL RELATIONS
Paul Wilkinson
JAZZ Brian Morton
MANDELA Tom Lodge
MEDICAL ETHICS
Tony Hope
THE MIND Martin Davies
MYTH Robert Segal
NATIONALISM Steven Grosby
PERCEPTION Richard Gregory
PHILOSOPHY OF RELIGION
Jack Copeland and Diane Proudfoot
PHOTOGRAPHY
Steve Edwards
THE RAJ Denis Judd
THE RENAISSANCE
Jerry Brotton
RENAISSANCE ART
Geraldine Johnson
SARTRE Christina Howells
THE SPANISH CIVIL WAR
Helen Graham
TRAGEDY Adrian Poole
THE TWENTIETH CENTURY
Martin Conway

For more information visit our web site
www.oup.co.uk/vsi

Fred Piper and Sean Murphy

CRYPTOGRAPHY

A Very Short Introduction

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford OX2 6DP

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide in

Oxford New York

Auckland Bangkok Buenos Aires Cape Town Chennai
Dar es Salaam Delhi Hong Kong Istanbul Karachi Kolkata
Kuala Lumpur Madrid Melbourne Mexico City Mumbai Nairobi
São Paulo Shanghai Taipei Tokyo Toronto

Oxford is a registered trade mark of Oxford University Press
in the UK and in certain other countries

Published in the United States
by Oxford University Press Inc., New York

First published as a Very Short Introduction 2002

British Library Cataloguing in Publication Data

Data available

Library of Congress Cataloging in Publication Data

Data available

ISBN 0-19 280315-8

5 7 9 10 8 6 4

Typeset by RefineCatch Ltd, Bungay, Suffolk
Printed in Great Britain by
TJ International Ltd., Padstow, Cornwall

Acknowledgements

This book has evolved over a number of years with many people making valuable comments and suggestions. We thank them all. We are particularly grateful to Gerry Cole, Ross Patel, and Peter Wild for reading the final draft, and to Adrian Culley and Kalatzis Nikolas for saving us from embarrassment by correcting some of our exercises. Most of all we appreciate the contribution of Pauline Stoner who managed to convert apparent random scribble into a presentable format. Her patience was frequently tested and the book would not have been completed without her.

Contents