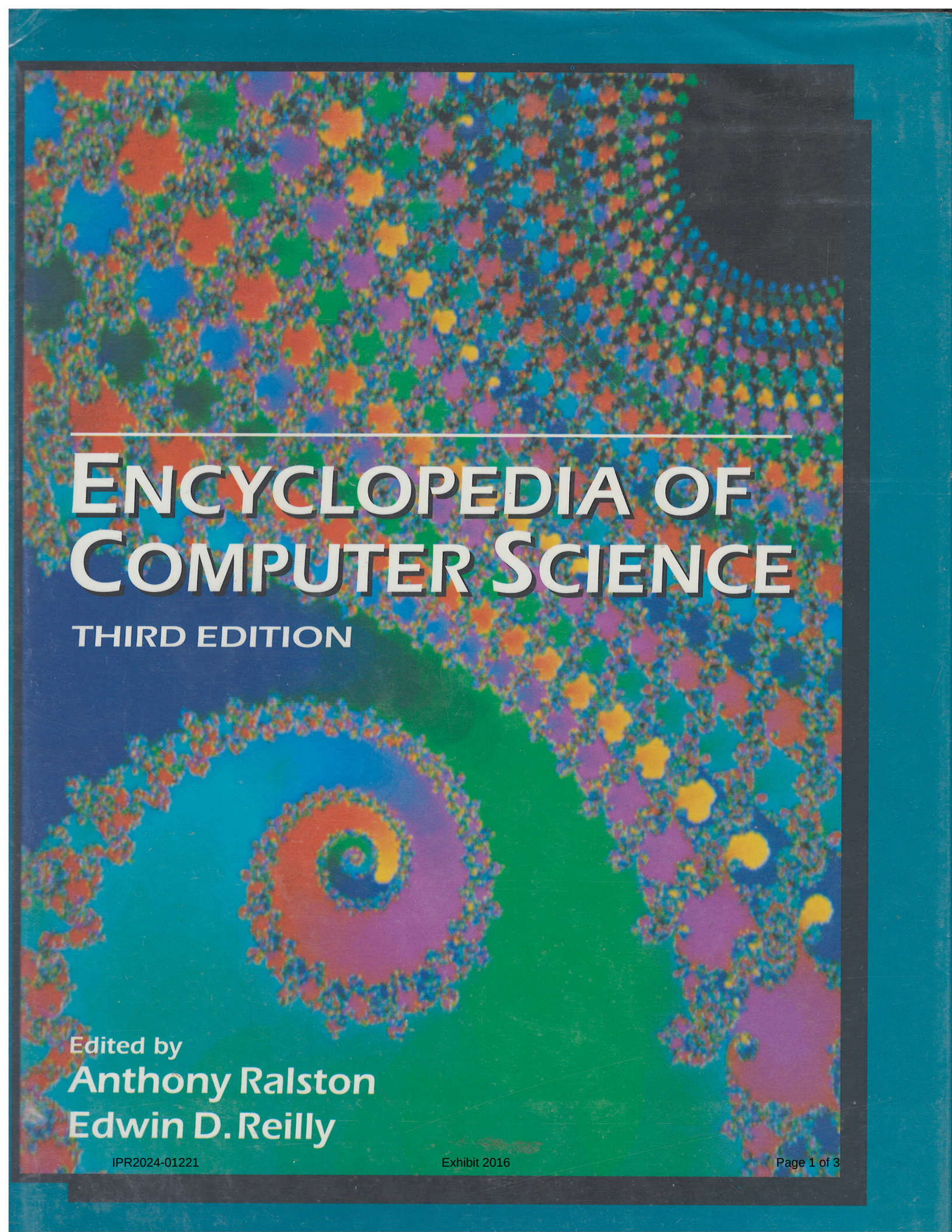




ENCYCLOPEDIA OF COMPUTER SCIENCE

THIRD EDITION

Edited by
Anthony Ralston
Edwin D. Reilly

Copyright © 1993 by Van Nostrand Reinhold

Library of Congress Catalog Card Number 92-14553
ISBN 0-442-27679-6

All rights reserved. Certain portions of this work ©1983, 1976 by Van Nostrand Reinhold. No part of this work covered the copyright hereon may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without written permission of the publisher.

Printed in the United States of America

Van Nostrand Reinhold
115 Fifth Avenue
New York, New York 10003

Chapman and Hall
2-6 Boundary Row
London SE1 8HN, England

Thomas Nelson Australia
102 Dodds Street
South Melbourne 3205
Victoria, Australia

Nelson Canada
1120 Birchmount Road
Scarborough, Ontario M1K 5G4, Canada

16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

Encyclopedia of computer science / Anthony Ralston, Edwin D. Reilly, editors ; Caryl Ann Dahlin, managing editor.

p. cm.

Includes bibliographical references and index.
ISBN 0-442-27679-6

1. Computer science—Encyclopedias. 2. Information science—Encyclopedias. I. Ralston, Anthony. II. Reilly, Edwin D.
QA76.15.E48 1992
004'.03—dc20

IPR2024-01221

Exhibit 2016

92-14553
CIP

Page 2 of 3

CROSS-ASSEMBLERS AND COMPILERS

For articles on related subjects see ASSEMBLER; COMPATIBILITY; COMPILER CONSTRUCTION; LANGUAGE PROCESSORS; and PORTABILITY.

Cross-processors, a term that includes both *cross-compilers* and *cross-assemblers*, are programs written to run on machine A (called variably the development machine, the controller, the host, or the front end), to produce programs to be run on machine B (called the target machine or the main processor). Thus, A is running a program (the cross-processor) written in a language acceptable to A. The input to this program are statements in assembly language for machine B (for a cross-assembler) or in any language for machine B for which there exists a cross-compiler.

The output of a cross-processor is machine language for machine B, which is then down-loaded from machine A to machine B. Downloading is the process by which the host computer transfers binary core images (or sometimes coded information) into the target computer so that the target computer can then proceed with program execution. The data for the program is either read directly by machine B or is part of the downloaded binary or coded image.

The two major uses of cross-processors are indicative of their versatility. Cross-processors are used for production of software for machines whose hardware is not yet available or is just being designed and evaluated. In this case, machine B may be initially a simulation rather than actual hardware, to be later replaced by actual hardware. Cross-processors are also used for production of programs for target machines whose specialized instruction set is not suitable for software production (e.g. signal processors or array processors) or whose cost may make them too expensive and thus not cost effective for compilation (e.g. vector machines, supercomputers (*q.v.*), massively parallel machines).

GIDEON FRIEDER

CRT. See TERMINALS.

CRYPTOGRAPHY, COMPUTERS IN

For articles on related subjects see COMPUTER CRIME; DATA COMMUNICATIONS; and DATA SECURITY.

Cryptography is the science of transforming messages for the purpose of making the message unintelligible to all but the intended receiver of the message. The term *data encryption* refers to the use of cryptographic methods in computer communications for the same reason, but also implies the additional goals of providing assurance to the receiver that the message is not a forgery, and/or allowing the receiver to prove to a third party that the message is not a forgery. These various aims are called, respectively,

the goals of *communication security*, *authentication*, and *digital signatures*.

The transformation used to encipher a message typically involves both a general method, or algorithm, and a *key*. While the general method used by a pair of correspondents may be public knowledge, some or all of the key information must be kept secret. The process of transforming (enciphering) a message is to apply the enciphering algorithm to the message, where the key is used as an auxiliary input to control the enciphering. The reverse operation (deciphering) is performed similarly.

Classical encryption techniques involve such operations as substituting for each message letter a substitute letter; in this case, the key is the correspondence between message (plaintext) letters and the enciphered message (ciphertext) letters. Such *substitution ciphers* can also be based on substituting for two or more letters at a time. Another common technique is to use a transposition cipher which permutes the order of the message letters using an algorithm whose steps are determined by a *key*. Many complicated hand or mechanical ciphers have been developed in the last few centuries; see Kahn (1967) for details. These techniques are insecure in general; the breaking of the German Enigma cipher during World War II attests to the vulnerability of even complicated rotor-machine ciphers (see Colossus).

The *one-time pad* is a technique that provides the ultimate in security: It is provably unbreakable. To encipher a 1,000-bit message, however, requires the use of a 1,000-bit key that will not be used for any other message. Each ciphertext bit is the exclusive-or of the corresponding message and key bits. The one-time pad is used only in very important applications (like the Moscow-Washington hot-line) because of the expense in creating and distributing the large amount of key information required.

Cryptosystems, which, unlike the one-time pad, depend upon an amount of key information that is independent of message length, are breakable in theory. What makes them usable in practice is that the person trying to break the cipher (the *cryptanalyst*) must use an impractical or infeasible amount of computational resources in order to break the cipher. These ciphers are constructed so that the "work-factor" in breaking them is high enough to prevent a successful attack.

The major application of cryptography today is for data transmitted between computers in computer communication networks and for computer data encrypted for storage.

The most widely used cipher in the U.S. for the encryption of stored or transmitted computer data is undoubtedly the Data Encryption Standard (DES), which was designed at IBM and approved as a standard by the National Bureau of Standards in 1976. The DES enciphers a 64-bit message block under control of a 56-bit key to produce a 64-bit ciphertext. The enciphering operation consists of roughly 16 iterations of the following two steps.

1. Exchange the left half of the 64-bit message with the right half.
2. Replace the right half of the message with the