

INTERNET SECURITY DICTIONARY

VIR V. PHOHA



Springer

Vir V. Phoha
phoha@acm.org

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA

Phoha, Vir V.
Internet security dictionary / Vir V. Phoha.
p. cm.

Includes bibliographical references and index.

ISBN 0-387-95261-6 (sc : alk. paper)

1. Computer networks—Security measures—Dictionaries.
2. Internet—Security measures—Dictionaries. I. Titles.

TK5105.59 .P56 2002

005.8'03—dc21

2001053056

Printed on acid-free paper.

© 2002 SPRINGER-VERLAG NEW YORK, INC.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Text design by Steven Pisano.

Manufacturing supervised by Jerome Basma.

Typeset by Impressions Book and Journal Services, Inc., Madison, WI.

Printed and bound by Edwards Brothers, Inc., Ann Arbor, MI.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-95261-6

SPIN 10796881

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science + Business Media GmbH

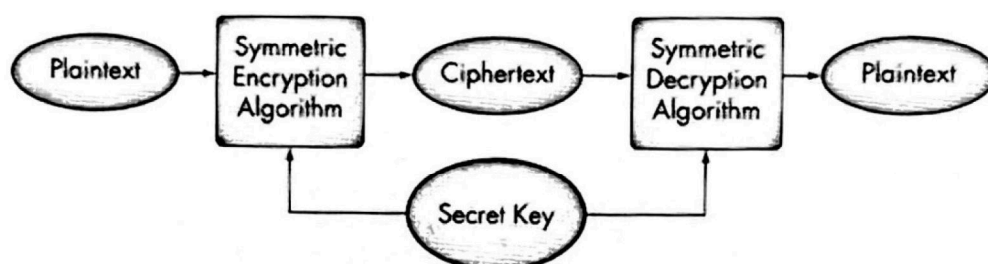


FIGURE S1 . Secret key cryptography.

script kiddies A slang term used for hackers who use tools written by others to attack systems because they themselves lack the technical knowledge and skills to write their own tools.

SDMI  SECURE DIGITAL MUSIC INITIATIVE.

secrecy Protects information from people with unauthorized access. *See also* CONFIDENTIALITY.

secret (1) (noun) A quantity known only to principals that can be used for AUTHENTICATION and encryption of information flow between them. (2) (adjective) A label applied to CLASSIFIED INFORMATION whose unauthorized disclosure may cause serious damage to individual, organizational, or national security.

secret key The information that is used for both the ENCRYPTION of data and its subsequent DECRYPTION. Typically, a method needs to be used for sharing this secret key between the parties who encrypt and decrypt the data.

secret key cryptography Also known as SYMMETRIC CRYPTOGRAPHY. A scheme in which the same key is used for ENCRYPTION and DECRYPTION. *See* Figure S1.

secure communications Telecommunications secured by TYPE 1 (U.S.) products and/or PROTECTED DISTRIBUTION SYSTEMS.

Secure Digital Music Initiative A consortium of companies and organizations with an aim to develop an open framework for storing, playing, and distributing digital music and to prevent the distribution of illegal copies of music. At present there are more than 200 members in this consortium representing consumer electronics, Internet service providers, information technology, telecommunications, security technology, and the music industry. It also provides specifications for portable devices. For more details see the information at <http://www.sdmi.org>.

secure hash algorithm A specification for a secure hash algorithm in which a condensed message representation, called a MESSAGE DIGEST, can be generated.

Secure Hypertext Transfer Protocol Developed within the Internet standards process, this protocol defines the security additions to the HTTP protocol. This protocol is an application-level protocol (TCP/IP four-layer model and OSI seven-layer model) and adds encryption and AUTHENTICATION to World Wide Web communications. *See* RFC 2660.

NOTE: S-HTTP is now virtually obsolete.

HTTPS (HTTP using SSL) is currently the most dominant protocol for protecting Web traffic, and the TLS (TRANSPORT LAYER SECURITY) protocol is being developed (RFC 2817, RFC 2818).

Secure Socket Layer Protocol First introduced in 1994 by Netscape (U.S.), us-