

User's Guide

WebCrypto for Windows 3.1x and Windows 95

McAfee, Inc.

2710 Walsh Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 A.M. - 6:00 P.M.

FAX: (408) 970-9727
BBS: (408) 988-4004

COPYRIGHT

Copyright © 1996 by McAfee, Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc.

TRADEMARK NOTICES

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of McAfee Associates, Inc. WebScan, SiteExpress, BootShield, ServerStor, WebCrypto, PCCrypto, and NetRemote are trademarks of McAfee Associates, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your feedback to: McAfee, Inc., Documentation, 2710 Walsh Avenue, Santa Clara, CA 95051-0963, or send a fax to McAfee Documentation at (408) 653-3143.

Table of Contents

Chapter 1. Introducing WebCrypto5

What is WebCrypto?	5
Main features	5
How To Contact Us.....	6
Customer service.....	6
Technical support.....	6
McAfee training.....	7
International contact information.....	8

Chapter 2. Installing WebCrypto9

Installation.....	9
System requirements.....	9
Installation procedure.....	9

Chapter 3. Using WebCrypto11

Overview.....	11
Encryption.....	12
Split files.....	15
Decryption.....	16
File/Disk Wipe	19
Logfile	22

Appendix A. Reference25

Understanding Cryptography	25
Cryptography	25
Symmetric algorithms	26
Encryption keys.....	26

Cryptanalysis	27
Choosing a secure password	28
Guidelines for selecting a password	28
Index	29

Introducing WebCrypto

What is WebCrypto?

WebCrypto is a general-purpose encryption tool for Windows that protects both personal and business data and your e-mail correspondence. WebCrypto allows you to securely exchange data over insecure channels, using state-of-the-art encryption algorithms for maximum protection.

Main features

- Uses a Windows interface with tabbed-notebook layout.
- Offers two levels of password (symmetric) encryption for protection of your confidential data.
- Allows for encryption of up to 1,000 files in one archive.
- Offers an option of compressing data before encrypting.
- Performs random stream overwrites to wipe files, slack, and free disk space.
- Creates a secure logfile for password management of your encrypted data.
- Allows for encryption of both text on the Windows clipboard and disk files.
- Offers an option of encrypting data to a self-extracting file. The data can then be decrypted from the Windows Program Manager, File Manager, or DOS command line.

How To Contact Us

Customer service

To order products or obtain product information, we invite you to contact our Customer Care department at (408) 988-3832 or at the following address:

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A.

Technical support

McAfee is famous for its dedication to customer satisfaction. McAfee has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating McAfee software and obtaining the latest news and information. For technical support information and issues, we encourage you to visit our website first.

World Wide Web <http://www.mcafee.com>

If you do not find what you need or do not have access to the Web, try one of McAfee's automated services.

Automated Voice (408) 988-3034
and Fax Response
System

Internet support@mcafee.com

McAfee BBS (408) 988-4004
1200 bps to 28,800 bps
8 bits, no parity, 1 stop bit
24 hours, 365 days a year

CompuServe GO MCAFEE

America Online	keyword MCAFEE
Microsoft Network (MSN)	MCAFEE

If the automated services did not solve your problem, you may contact McAfee Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

Phone	(408) 988-3832
Fax	(408) 970-9727

To speed the process of helping you use our products, please note the following before you call:

- Product name and version
- Computer brand, model, and any additional hardware
- Operating system type and version
- Network type and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem, if applicable

McAfee training

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

International contact information

To contact McAfee outside the United States, use the addresses and numbers below.

McAfee Canada

178 Main Street

Unionville, Ontario

Canada L3R 2G9

Phone: (905) 479-4189

Fax: (905) 479-4540

McAfee Europe B.V.

Orlyplein 81 - Busitel 1

1043 DS Amsterdam

The Netherlands

Phone: (0) 31 20 6815500

Fax: (0) 31 20 6810229

McAfee France S.A.

50 rue de Londres

75008 Paris

France

Phone: 33 1 44 908733

Fax: 33 1 45 227554

McAfee Deutschland GmbH

Industriestrasse 1

D-82110 Germering

Germany

Phone: 49 89 8943560

Fax: 49 89 89435699

McAfee (UK) Ltd.

Hayley House, London
Road

Bracknell, Berkshire

RG12 2TH United Kingdom

Phone: 44 1344 304730

Fax: 44 1344 306902

2

Installing WebCrypto

Installation

System requirements

- IBM-compatible personal computer running Windows 95 or Windows 3.1x
- 1MB hard drive space

Installation procedure

To install WebCrypto, carefully follow the procedure outlined below.

Step	Action
1.	Start your computer.
2.	Do one of the following: <ul style="list-style-type: none">■ If you are installing from diskette, insert it into your floppy disk drive.■ If you are installing from files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive.

3. Select Start>Run.

- If you are installing from diskette, type:

a: \setup.exe

Click OK.

- If you are installing from files downloaded from the McAfee Web Site or a network server, type:

x: \path\setup.exe

where *x:\path* is the location of the files. Click OK.

Response: The Welcome screen is displayed.

Action: Click Next to continue.


4. Select the destination directory for the WebCrypto program files, and click Next.

Response: A progress meter is displayed while WebCrypto is installed.

Action: When setup is complete, click OK.

5. Click Yes to review the README.1ST file.

Response: WebCrypto installation is complete.


 *In the licensed version of WebCrypto, you will be prompted for your name or company name the first time you use the product.*

Overview

WebCrypto's functions are divided into five tabbed pages. Clicking the tab on the top of a page makes that page active. The five pages are:

- **Main**, which is a title page used for program entry and exit
- **Encrypt**, which is used for data encryption
- **Decrypt**, which is used for data decryption
- **Wipe**, which allows you to permanently erase data or file slack
- **Logfile**, which keeps a secure record of your encryption activity

Each page also has its own Help button. Click Help at any time to access online help for WebCrypto's many functions.

 *All of WebCrypto's functions are also available from the keyboard. Press the Tab key to move to the next component on a page. When a page's tab has the focus, you can press the left/right cursor keys to activate a different page.*

Encryption

The Encrypt page is used to secure your data and e-mail correspondence. WebCrypto uses secret password, or *symmetric*, encryption to protect your personal and business data. Once data is encrypted, it can be safely sent across the Internet or saved on your computer system until decrypted.

To encrypt your data, take the following steps:

Step	Action
------	--------

- | | |
|----|-------------------------|
| 1. | Select the Encrypt tab. |
|----|-------------------------|

Response: The Encrypt page is displayed. See Figure 3-1 below.

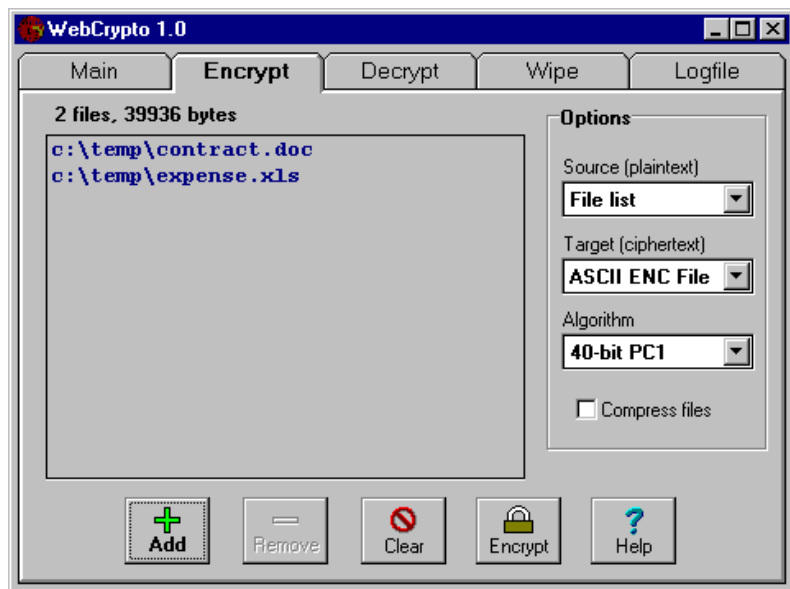



Figure 3-1. WebCrypto Encryption Page

2. Set the Source option. This specifies the location of the *plaintext*, or the data that is to be encrypted. The two source types are File List and Clipboard.

- If you select File List as the source, the disk files you place in the file list will be encrypted.


You can encrypt up to 1,000 files at once. To add files to the list box, select a file and click Add. To Remove selected files from the list, select a file and click Remove. The Clear button removes all the files from the list.

 *To select a range of files, click and drag the mouse. Hold the Ctrl key down while clicking to select multiple files that are not in a continuous range.*

- If you select Clipboard, the contents of the Windows clipboard will be encrypted.

3. Set the Target option. This specifies the location of the *ciphertext*, or the encrypted output. The three target types are ASCII ENC file, Self-extracting EXE file, and Clipboard.


- The ASCII ENC file is the default option. It is an archive file (similar to a ZIP file) with an extension of .ENC that can hold up to 1,000 files. After encryption, these files must be decrypted using WebCrypto.

 *ASCII ENC files are specially coded with 7-bit text characters so that they can be mailed as text files across the Internet and other systems that do not support 8-bit binary transfers. Also, ASCII ENC files can be split into smaller sections if needed to facilitate e-mail transfers.*

- Self-extracting EXE files will prompt the user for a password and decrypt themselves when run from the Windows Program Manager, File Manager, or the DOS command line. WebCrypto is not needed to decrypt the self-extracting files.
- The Clipboard can also be set as the target. If you select the Clipboard as both the source and the target, then the original source plaintext will be overwritten by the ciphertext.

4. Select an Algorithm.


- The 40-bit PC1 algorithm is a very fast stream cipher.
- The 160-bit Blowfish algorithm is a much more secure block cipher.

 *Due to export restrictions, the 160-bit Blowfish option is not available in the international version of WebCrypto.*

- Select Compression if you want WebCrypto to compress the plain-text data before it is encrypted. WebCrypto uses the LZ77 compression algorithm. If a file cannot be compressed, it will automatically be re-encrypted and stored without compression.

5. Click Encrypt to begin the encryption process.

- If the target is set to an ENC or Self-extracting file, you will be prompted for a filename. An extension of .ENC (or .EXE) will automatically be placed on the filename. Click OK.


 *If the file already exists, you will be prompted to overwrite it. You can not add to or update an existing file.*

Response: A password form appears.

6. Select your password options.

- Click Case Sensitive if you want to consider case during encryption and decryption. If this button is selected, the case of the password must match when decrypting. For example, if a password of “abcdefgh” is used to encrypt with case sensitivity on, only “abcdefgh” will decrypt.
- Click the 8-Character Minimum button. This option serves as a reminder that short passwords are insecure and should be avoided.
- Click Echo Asterisks if you want asterisk (*) characters to display as you are typing in a password.


7. Enter a password.

 See *“Choosing a secure password” on page 28*. A poorly chosen password will negate all the security features built into WebCrypto.

8. Enter the password again into the second box for confirmation and click OK.

Response: A progress meter is displayed as your data is encrypted.

9. To save your encryption information in the Logfile, enter a comment when prompted and click OK. Click Skip if you do not want to save an entry to the logfile.

 If Logfile is closed, you will be prompted for the logfile password and the information will be loaded into the logfile editor.

Split files

If the encryption target is an ASCII ENC file, a prompt will appear after encryption displaying the number of data lines in the ENC file. You then have the option of splitting the ENC file into smaller files to facilitate e-mail delivery. A prompt for the maximum data lines to put in each split file will appear. A data line is 64 characters plus a carriage return and line feed for a total of 66 bytes. If you select to create split files, the original ENC file will remain intact while files with extensions of .E01, .E02, .E03, and so forth are created.

Decryption

The Decrypt page is used to decrypt data previously encrypted with WebCrypto.

To decrypt your data, take the following steps:

Step	Action
------	--------

1. Select the Decrypt tab.

Response: The Decrypt page appears. See Figure 3-2 below.

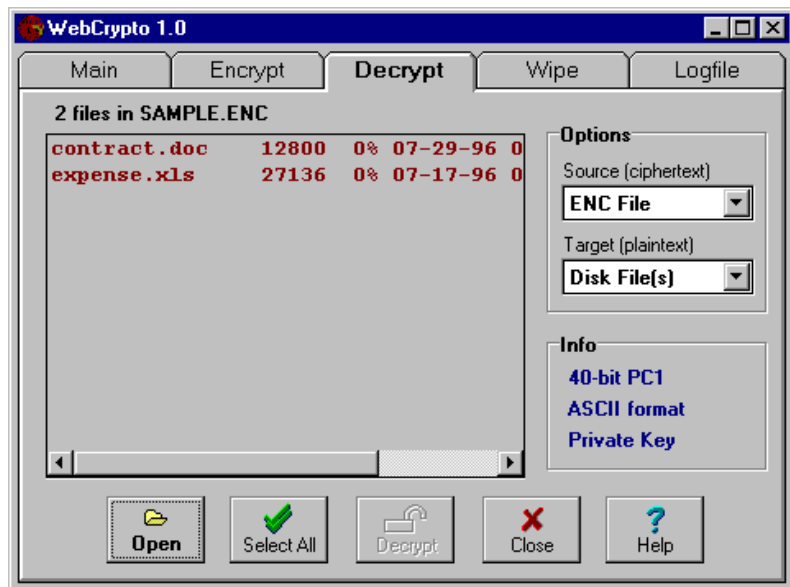



Figure 3-2. WebCrypto Decryption Page

2. Set the Source option. This specifies the location of the *ciphertext*, or the encrypted data. The two source types are ENC file and Clipboard.
 - An ENC file can be a complete ASCII ENC file or the first split file (.E01) in a group of split ASCII ENC files. See [“Split files” on page 15](#) for more details.
 - If you select Clipboard, the contents of the Windows clipboard will be decrypted.
3. Click Open. If the source is an ENC file, you will be prompted to select it from your disk drive. If a valid ENC file is found, WebCrypto will open it and list its contents by displaying the file headers in the list box. Each line will show the filename, original file size, compression percentage, timestamp, and 32-bit CRC value. General format information is displayed in the lower-right information box.
4. Set the Target option. This tells WebCrypto where to place the plain-text files after decrypting. The two target types are Disk file(s) and Clipboard.
 - If the target is set to Disk file(s), the files will be decrypted and saved in the current directory. You will be prompted to overwrite existing files if found.
 - The clipboard can only hold text data, so you should not attempt to decrypt binary files onto the clipboard.
5. Select the files from the list that you want to decrypt. Click Select All to highlight all the files listed.

 *To select a range of files, click and drag the mouse. Hold the Ctrl key down while clicking to select multiple files that are not in a continuous range.*


6. Click Decrypt to start the decryption process. You will be prompted for the password the first time you attempt to decrypt a file. You only have to enter a password once for each ENC file.

Response: If the correct password is entered, the selected files are decrypted. A progress meter is displayed during the decryption process.

Action: Click Close to close the ENC file.

File/Disk Wipe

The Wipe page is used to permanently erase data from your disk drive. Normally, when you delete files from the DOS command line or with Windows File Manager, your files are not really erased. Instead, their directory entries are modified so that they no longer show up in a file listing and their clusters are reallocated by the operating system. Unerase programs can restore these “erased” files if their clusters have not yet been overwritten. WebCrypto's Wipe feature permanently erases data and prevents files from being unerased.

 *You cannot use the wipe function on network drives. Most network operating systems, such as Novell NetWare, make backup copies of files every time a file is edited.*

Files are allocated clusters by the operating system to store their data. The size of a cluster depends on the size of a drive partition. Since files are always allocated a whole number of clusters, there will be some unused space in the last cluster allocated to a file (unless the size of the file happens to be an even multiple of the cluster size). This unused space is called file slack. The file slack can contain data from files previously occupying the cluster or from the drive's sector write buffer. Using WebCrypto, you can erase this file slack.

To use the Wipe function, take the following steps:

Step	Action
------	--------

- | | |
|----|----------------------|
| 1. | Select the Wipe tab. |
|----|----------------------|

Response: The Wipe page appears. See Figure 3-3.

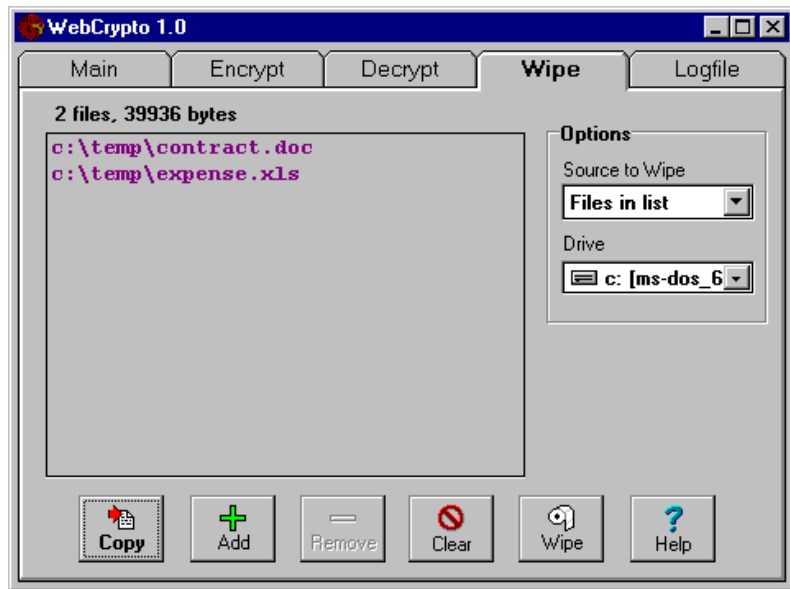


Figure 3-3. WebCrypto Wipe Page

2. Set the Source to Wipe option. The four source types are Files in List, Slack in List, Slack on Drive, and Free Drive Space.
 - **Files in List:** After a file is wiped, it is truncated to zero bytes, renamed to WWIPED\$\$TMP, then erased. All files in the list will be permanently erased, as will the slack in these files. Use this feature with caution. You can never recover these files.
 - **Slack in List:** The slack at the end of all the files in the list will be wiped. The files themselves are not modified.
 - **Slack on Drive:** The slack at the end of every file (except hidden or read-only files) on the selected drive will be wiped. The files themselves are not modified.

- **Free Drive Space:** A temporary file will be created in the root directory of the specified drive and filled with random data until the drive has no space left. The file will then be deleted. This wipes all the unused clusters on the drive, but does not wipe the file slack on the drive or modify any existing files.

3. Do one of the following:


- If the source is set to Files in List or Slack in List, specify which files to wipe by placing them in the file list box. Click Add to add files to the list. Click Copy to copy the files from the Encrypt page to the Wipe page. You can use this option to wipe plaintext files that were just encrypted into a ENC file. The Remove button removes selected files from the list, and Clear removes all the files from the list.
- If the source is set to Free Drive Space or Slack on Drive, set the Drive option to the desired drive.

4. Click Wipe to start the wipe process.

Response: A confirmation message is displayed.

5. Click OK to proceed or Cancel to quit.

Response: WebCrypto overwrites data with a random data stream from the PC1 encryption engine.

 *A separate DOS utility called SFWIPE.EXE is included with WebCrypto to wipe the Windows 3.1x permanent swap file. Because the swap file is active while Windows is running, you must completely exit Windows to run it. SFWIPE overwrites the swap file with one random stream pass. The swap file is not erased, and it will be active again the next time you start Windows.*

Logfile

The Logfile page contains an editor for viewing, editing, and searching the WebCrypto logfile. Each time data is encrypted, WebCrypto gives the user the option to create a logfile entry containing the following information:

- User Comment (up to 60 characters)
- Date and Time
- Source (list of files encrypted or clipboard, up to 255 characters)
- Target (encrypted file name or clipboard)
- Encryption Algorithm (PC1 or Blowfish)
- Compression (Y or N)
- Password (in quotes)

WebCrypto will prompt you for the User Comment after the encryption is complete. The remaining fields are generated automatically. New logfile entries are added to the end of the logfile.

The logfile will be created automatically the first time an entry is made and will be encrypted to disk when closed. You will be prompted for the password and will use the same password the next time the logfile is opened. You can change the logfile password at any time.

To view and edit information in the Logfile, take the following steps:

Step	Action
1.	Select the Logfile tab.

Response: The Logfile page appears. See Figure 3-4.

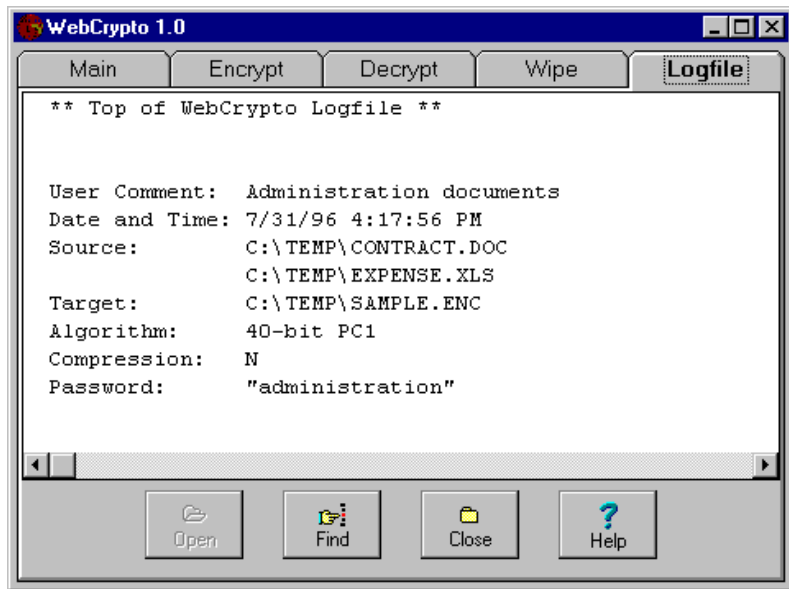


Figure 3-4. WebCrypto Logfile Page

2. Click Open to manually open and load the logfile. Enter your password when prompted. If the logfile does not exist, a new one will be created with a single line reading "*** Top of WebCrypto Logfile ***" at the top.

The logfile is a simple text file that can be edited by the user.

- To delete a section of text, select it and press the Delete key.
- Use Ctrl-X to cut or Ctrl-C to copy selected text onto the Windows clipboard.
- Use Ctrl-V to paste text from the clipboard.

The logfile editor can hold as much text as you have available RAM (16MB maximum). If the logfile becomes too large, you may want to delete older entries or rename or move the logfile so that a new one will be created.

3. Click Find to search for a text string in the logfile. The search string can be up to 20 characters and is not case sensitive. The search begins at the current cursor position.
4. Click Close to close the logfile.

- If changes have been made to the logfile since it was opened, you will be prompted for a password and the logfile will be encrypted and saved to disk. The logfile name is WCRYPTO.ENC and is saved in WebCrypto's program directory.



You will need to remember the last password used so that the logfile can be opened later.

- If no changes have been made to the logfile since it was last opened, the logfile editor is simply cleared and no encryption is performed.



If you exit WebCrypto when the logfile is opened and modified, you will be asked if you want to close the logfile and save the changes.

Understanding Cryptography

Cryptography is based on sound mathematical principles. This appendix includes basic tips and terminology you should know to help you make full use of WebCrypto's features.

Cryptography

Cryptography is the science of encrypting data, while cryptanalysis is the science of breaking encrypted data. Cryptology is the combined science of cryptography and cryptanalysis. A message or data file is called plaintext before it is encrypted and ciphertext after it is encrypted. The process of scrambling the plaintext into ciphertext is called encryption. The process of unscrambling the ciphertext back to its original plaintext state is called decryption.

Some of the best cryptanalysts in the world work for the National Security Agency (NSA), a secretive agency created by U.S. President Harry Truman in 1952. Its purpose is to decrypt foreign communications that are of interest to the national security of the United States. Cryptography is classified as munitions in the U.S. Munitions List (USML) and is covered in the International Traffic in Arms Regulations (ITAR). The NSA, through the State Department, controls the encryption technology that is exported from the United States. The international version of WebCrypto contains the strongest encryption technology allowed for export from the United States. The U.S./Canada registered version of WebCrypto is not subject to these controls and therefore contains much stronger encryption technology.

Symmetric algorithms

Symmetric algorithms are conventional password-based systems: You supply a password, and the file is encrypted. To decrypt the file, you supply the same password again, and the process is reversed. WebCrypto supports two symmetric algorithms: PC1 and Blowfish.

PC1 is a 40-bit cipher that produces an identical key stream as RC4. RC4 (a trademark of RSA Data Securities, Inc.) is a fast variable-key size stream cipher developed in 1987 by Ron Rivest. It is an unpatented algorithm that has special export status. It is the only algorithm (along with RC2) allowed for export from the United States with a key size of 40 bits using the State Department's Commodity Jurisdiction (CJ) request.

WebCrypto's other symmetric algorithm is Blowfish with a 160-bit key. Blowfish is an unpatented algorithm invented by Bruce Schneier and was first published in the April 1994 edition of Dr. Dobbs's Journal. It also appears in the second edition of *Applied Cryptography*. Blowfish is a fast variable-key size block cipher based on a 16-round Feistel network. Because of export restrictions, this algorithm is only available to users who reside in the U.S. or Canada.

Encryption keys

Assuming you are using secure encryption algorithms, the difficulty of breaking an encoded message or file is directly proportional to its key size. WebCrypto generates keys by running your password through a one-way hash function. A one-way hash function takes a variable size stream of data and produces a fixed-length number that represents the data. One-way hash functions are cryptographically secure: They cannot be reversed, and it is mathematically infeasible to find two messages that produce the same hash value. WebCrypto uses the Secure Hash Algorithm (SHA-1), which was developed by the National Institute of Standards and Technology (NIST) along with the NSA.

Keys are measured in bits. A single-bit key has two possible combinations: 0 and 1. Each additional bit doubles the combinations. An 8-bit key has 256 combinations, a 40-bit key has over 1 trillion combinations, and a 160-bit key has 10^{48} combinations.

Trying each key until the right one is found is called a brute-force attack. A personal computer that could try 50,000 keys per second could test all combinations of a 40-bit key in about 255 days. On average, you would only have to try half the keys before the right one is found. The 40-bit key, therefore, would be classified as casual security. The 160-bit key used in the Blowfish algorithm would be classified as military-strength security. A trillion supercomputers that could each test a trillion keys per second, would take about 463 trillion centuries to go through all the key combinations in a 160-bit key.

Cryptanalysis

An encryption system can be attacked (cryptanalysed) in several ways. If the algorithm has weaknesses, then ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext attacks are possible. In WebCrypto's algorithms, there are no known significant weaknesses. A brute-force attack on the key space is another possibility. These attacks are infeasible when 160-bit keys are used. Another attack is a breach of physical security, such as someone physically breaking into your computer and stealing unencrypted documents or planting a virus program that records your keystrokes to obtain your passwords. A final attack is a dictionary attack, where thousands of words and common phrases are tried one at a time. A specially written computer program could perform a dictionary attack quickly. For this reason, McAfee recommends that you follow the guidelines provided in this appendix for selecting secure passwords.

Choosing a secure password

Passwords in WebCrypto can be up to 50 characters in length. You can use several words, incorporating all the characters available to you on your keyboard.

Guidelines for selecting a password

- Never use personal information that could be guessed by someone who knows you. Do not use your name, your spouse's name, your kids' names, or your dog's name. Do not use your social security number, your phone number, your address, or your birthday. Do not use your school name, company name, or favorite football team's name.
- Don't use any word that would appear in the dictionary by itself. Don't use common phrases, famous quotations, titles of nursery rhymes, or song titles.
- The best password is a combination of several words, totalling approximately 15 characters. Use symbols like ~!@#\$\$%^&*() and numbers. Mix upper and lower case, use odd spelling, or make up words.
- Most importantly, choose something that you can remember. If you forget a password, you are out of luck. There are no backdoors, trapdoors, or escape hatches in WebCrypto.

A

Algorithms 26
America Online 7

B

BBS 6
Bulletin Board System 6

C

Choosing a password 28
CompuServe 6
Cryptanalysis 27
Cryptography 25
Cryptology 25
Customer Care department 6
Customer service 6

D

Decryption 16
Disk wipe 19

E

Encryption 12
Encryption keys 26

F

Features 5
File/disk wipe 19

I

Installing Web-Crypto 9
Internet support 6

L

Logfile 22

M

McAfee
 BBS 6
 support 6
 website 6
Microsoft Network (MSN) 7

P

Passwords 28

R

Requirements system 9

S

Support
 international 8
Symmetric algorithms 26

T

Technical support 6
 contacting 6
 international 8
Terminology 25
Training
 scheduling 7

U

Understanding cryptography 25
Using WebCrypto 11

W

WebCrypto
 installing 9
 introducing 5
 using 11
What is Web-Crypto? 5
Wipe 19

