# Keep It Secret! A File-Encryption Starter Kit

PASSWORD-PROTECT YOUR PERSONAL FILES SO THAT ONLY YOU CAN SEE THEM. **BY MATTHEW LAKE AND JEFF PROSISE**

EVERYONE HAS SECRETS. Whether it's your CompuServe ID and password, a confidential report, or a Christmas list, there's always something on your hard drive or floppy disks that's for your eyes only. Here are several ways to keep secrets on your PC by scrambling sensitive files so that only you can use them.

The password-protection routines here are all based on a small file-encryption program called ENCRYPT.COM that you create with DEBUG. Four batch files—SCRAMBLE.BAT, SEE.BAT, GET.BAT, and SECRET.BAT—enhance the program. SCRAMBLE encrypts files with a password you provide, SEE shows text hidden in encrypted files (when you provide the right password), GET extracts files from encryption, and SECRET enables you to write confidential information in a text file and encrypt it in one step.

### /// ENCRYPT.SCR ///

```
N ENCRYPT.COM
E 0100 EB 34 53 79 6E 74 61 78
E 0108 3A 20 45 4E 43 52 59 50
E 0110 54 20 22 70 61 73 73 77
E 0118 6F 72 64 22 20 3C 69 6E
E 0120 66 69 6C 65 20 3E 6F 75
E 0128 74 66 69 6C 65 0D 0A 24
E 0130 00 00 00 00 00 00 FC BE
E 0138 81 00 AC 3C 20 74 FB 3C
E 0140 0D 74 61 3C 22 75 5D 8B
E 0148 EE 33 C9 AC 3C 22 74 07
E 0150 3C 0D 74 50 41 EB F4 0B
E 0158 C9 74 49 89 0E 34 01 B8
E 0160 00 80 33 D2 F7 36 34 01
E 0168 F7 26 34 01 A3 30 01 B4
E 0170 3F BB 00 00 8B 0E 30 01
E 0178 BA C4 01 CD 21 72 20 0B
E 0180 C0 74 1C A3 32 01 E8 24
E 0188 00 B4 40 BB 01 00 8B 0E
E 0190 32 01 BA C4 01 CD 21 72
E 0198 06 3B 06 30 01 73 D0 B8
E 01A0 00 4C CD 21 B4 09 BA 02
E 01A8 01 CD 21 EB F2 8B F5 BF
E 01B0 C4 01 8B 0E 32 01 AC 3C
E 01B8 22 75 03 8B F5 AC 30 05
E 01C0 47 E2 F3 C3
RCX
C4
W
Q
```

To get these files onto your hard disk, copy each of the listings in this article into a text editor, and save them as text files with the names indicated. Or, download NCRYPT.ZIP, a compressed file of all four batch files, from PC/Contact's data library 1 (Hot Tips/Secrets). Save them in a directory mentioned in AUTOEXEC.BAT's PATH statement, such as your batch or utilities directory, so that you can run them from any prompt.

## Tales from Encrypt

Once you have the text file ENCRYPT.SCR on your hard disk, switch to the directory it's in and type the following command to create the program ENCRYPT.COM. (*Note:* Ensure that there is a carriage return following the final *Q* in ENCRYPT.SCR, or your computer will hang when you enter this command.)

```
DEBUG < ENCRYPT.SCR
```

Type DIR *.COM to verify that ENCRYPT.COM has been generated. Enter ENCRYPT at the DOS prompt to see ENCRYPT's command-line syntax. Use redirection characters—the greater-than (>) and less-than (<) symbols—to specify your password, the file to be encrypted, and a filename for the new, encrypted file. Then test the utility by encrypting a text file in the current directory—ENCRYPT.SCR is a good choice—with the following command:

```
ENCRYPT "PASSWORD" < ENCRYPT.SCR
  > TEST.ENC
```

Use DOS's TYPE command to view the contents of both ENCRYPT.SCR and TEST.ENC and be assured that no word processor or any other program can make sense of the encrypted file.

ENCRYPT works by using a logical operation called an exclusive OR (XOR) that sets a destination bit to 1 or 0 depending on the values of two source bits. Each byte in the password is combined in an XOR relationship with each byte in the file, and the resulting byte is put into the encrypted file. After a file undergoes the XOR encryption process, its contents are no longer recognizable.

The remarkable thing about the XOR algorithm is that running a file through ENCRYPT a second time with the same password decrypts the file, so you don't need a separate utility. To restore the file, enter a line with a syntax similar to the original:

```
ENCRYPT "PASSWORD" < TEST.ENC
  > RESULT.SCR
```

To check that the file is restored, type COMP ENCRYPT.SCR RESULT.SCR, and DOS should respond with "Files compare OK."

If you need additional security, encrypt the file twice. After encrypting a file the first time, use ENCRYPT on the encrypted file, with a new password (since using the same password would just decrypt the file). The resulting doubly encrypted file will resist the most determined efforts to decode it. To decrypt a doubly encrypted file, simply reverse the process. Run it through ENCRYPT with one of the passwords, then run the resulting file through ENCRYPT with the other password. Because of the way the XOR encryption works, it doesn't matter which password you use first, as long as the passwords are the same two you used to encrypt the file.

## Want Those Files Scrambled?

Although ENCRYPT.COM works fine by itself, its complicated command-line syntax and rudimentary help instructions leave a little to be desired. To make things easier (and to guard against typing mistakes), use SCRAMBLE.BAT, SEE.BAT, and GET.BAT.

Enter SCRAMBLE at a DOS prompt for instructions from SCRAMBLE.BAT. To encrypt an existing file of any sort—text, formatted text or number, or binary (graphics or programs)—use the following syntax:

```
SCRAMBLE source.doc
         password target.doc
```

If you miss any of the three required parameters, the batch file's IF (%3)==()

GOTO INFO line jumps to a help paragraph. You can customize any line in this paragraph (just remember to precede any line you want to see onscreen with an ECHO command).

The batch file offers to delete the original file as a security measure. If you want to delete the original, press Enter. For a little protection against DOS's UNDELETE command, the batch file overwrites the original file with a single word so that once you've deleted the file, it's extremely difficult to restore the information. This poses a risk to your data (if you forget the password, you'll never get your file back), but it also provides a fair amount of security.

If you don't want to delete the original, simply press Ctrl-C or Ctrl-Break when the batch file prompts you, and answer Y to DOS's question "Terminate Batch operation?" If you don't like this option, just delete the lines between ECHO. and :INFO or precede each of them with REM to make them remarks instead of instructions.

If you want to scan an encrypted text file without first decrypting it, use SEE.BAT. This batch file requires only two parameters: the encrypted file's name and the password. The batch file redirects the decrypted information to the DOS command MORE, which displays it onscreen one page at a time. When you're finished reading the file, SEE clears the screen so that nobody else can see your files. If you don't want to clear the screen, press Ctrl-C or Ctrl-Break to stop the batch file.

To extract a file from its encrypted form and leave it on disk, use GET. This batch file requires three parameters: the encrypted source file, its password, and the target file. The DIR %3 command at the end of the batch file verifies that the file has been decrypted—if you get a FILE NOT FOUND statement, it's because there was a problem creating it. Make sure that you entered the encrypted file's name correctly and that it's in the current directory or one in your PATH. Then try running GET again.

**SCRAMBLE.BAT**

```
@ECHO OFF
IF (%3)==() GOTO INFO
ENCRYPT "%2" < %1 > %3
ECHO.
ECHO SCRAMBLE will remove every trace of the file you just hid,
ECHO except for password-protected information in an encrypted file,
ECHO unless you enter Ctrl-C or Ctrl-Break now.
ECHO Press any other key to delete the original file.
ECHO.
PAUSE > NUL
ECHO SECRET > %1
DEL %1
GOTO END
:INFO
ECHO.
ECHO SCRAMBLE uses ENCRYPT.COM to encrypt a file you want to keep secret.
ECHO Use this syntax:
ECHO SCRAMBLE file password encrypted_filename
ECHO.
:END
```

**SEE.BAT**

```
@ECHO OFF
IF (%2)==() GOTO INFO
ENCRYPT "%2" < %1 | MORE
GOTO OUT
:INFO
ECHO.
ECHO SEE uses ENCRYPT to display information hidden in encrypted files.
ECHO Use this syntax:
ECHO SEE file password
ECHO.
GOTO END
:OUT
ECHO.
ECHO Press any key to clear the screen, or press
ECHO Ctrl-C to quit the batch file and keep the info displayed.
PAUSE > NUL
CLS
:END
```

### Keep a Secret

A short text file containing such private information as your credit card numbers, online service ID numbers and passwords, and appointments can be crucial for the mobile computing expert. To make a quick and confidential list, use SECRET.BAT, which sends the text you enter to ENCRYPT.

SECRET.BAT requires two parameters: output filename and password. First, the batch file uses COPY CON to create a text file from characters you type. Enter data line by line, and DOS stuffs it into a temporary file, TEMP.TMP. When you've finished, press Ctrl-Z (or F6) followed by Enter. The batch file then calls ENCRYPT.COM and passes it the name of the temporary file and the two parameters you entered at the DOS prompt. Finally, SECRET.BAT overwrites the temporary file with a single word (to make it difficult to recover) and deletes it.

Because SECRET.BAT uses temporary files, it can promote disk fragmentation by writing and deleting files. To prevent this and to speed up performance a notch or two, edit the batch file to send the decrypted temporary file to a RAM disk, if you have one. To do this, simply insert the RAM disk's drive letter before each instance of TEMP.TMP in the batch file. If your RAM drive letter is G:, for example, the encryption line would read

```
ENCRYPT "%2" < G:\TEMP.TMP > %1
```

Putting the temporary file on a RAM disk also will eliminate the remote possi-

# PC/Contact

**THIS MONTH'S FREE SOFTWARE** All the public-domain and shareware programs, batch files, and utilities featured in *PC/Computing* each month are available on our online service, PC/Contact, or on disk from Public Brand Software for a fee. Here's a sampling of the programs you'll find this month.

**Protect Your Secrets** ........................................................ Help, page 272

Everyone has secrets they want to protect. It might be a CompuServe password, a confidential report, or even Junior's Christmas list. We've compiled four programs that together help you encrypt files, and then decrypt or simply view them. These password-protection routines are based on a small file-encryption program called ENCRYPT.COM that you create with DEBUG. Look for NCRYPT.ZIP in data library 1 (Hot Tips/Secrets).

**Enhance Your PATH string** ........................................................ Help, page 230

Feel constrained by DOS's arbitrary limit on the number of characters in your PATH statement? The classic way to circumvent that limit is to use the SUBST command, as demonstrated in this month's DOS column. But we've made an alternative available to you on PC/Contact. ADDTOIT.COM, a short utility, can append additional directory names to the end of a PATH or break a long PATH into several commands. Download ADDIT.ZIP from data library 1 (Hot Tips/Secrets).

**New File Format for PC/Contact!**

Starting with this issue, we'll be providing files in the popular ZIP file format. Files stored this way offer several advantages. First, many files are stored in together in an *archive* file so you don't have to download multiple files. Second, the files within an archive are compressed so that you can download the archive file faster, saving telephone and connect charges. You need a program that supports ZIP files, however, and we offer several. PKZ110.EXE is a shareware collection of command-driven utilities for managing files in the PKZIP format. If you favor a menu-driven format, check out the shareware PKZMEN.EXE. If you just want a free unZIPper, try PDZIP.EXE. All ZIP utilities are in data library 0 (General/Forum Info).

## HOW TO JOIN PC/CONTACT

For current CompuServe subscribers, just type GO PCCONTACT to access the forum. Cost is based on CIS's fee of $12.80 per hour for 1,200/2,400 bps and $22.80 per hour for 9,600 bps. There is an additional $2.50 ZiffNet membership charge per month for all users, which includes a number of free services. For complete information, type GO ZNT:RATES when online.

For new subscribers, follow these steps:

1. Set the following parameters within your communications program: 7 data bits, even parity, 1 stop bit, and full duplex.
2. Call CompuServe's toll-free Customer Assistance Line at (800) 848-8990 (United States) or (800) 635-6225 (Canada). From other countries, dial CompuServe direct at (614) 457-8650. A voice-response system will ask you if you want a local-access number. Then you'll be asked to enter your phone number and the speed at which you want to access the system. CompuServe reads back the local number you'll use to access the service.

   Or, call CompuServe with your modem. Set up your modem and telecommunications package using 7 data bits, even parity, 1 stop bit, and full duplex, and call (800) 346-3247. When the modem connects, press Enter. When you see the HOST NAME prompt, type in PHONES and then hit Enter. Then just follow the onscreen menus and note the access phone number for your area.
3. Dial the local-access number with a modem. When you connect to the network, press Ctrl-C to get its attention.
4. At the HOST NAME prompt, type CIS (which is the acronym of the CompuServe Information Service).
5. At the USER ID prompt, enter 177000,5300.
6. At the PASSWORD prompt, enter PC/CONTACT.
7. At the ENTER AGREEMENT NUMBER prompt, type Z10DPCC1.
8. If you have trouble, call the Customer Assistance Line at (800) 848-8990. After you follow the above procedures, the CIS system will provide you with your own user ID—called a PPN—and a temporary password. You can then log on and begin to explore PC/Contact. In about two weeks, you'll receive a letter from CIS confirming your PPN and providing you with a new password. You should then change your password by typing GO PASSWORD at any CIS prompt.

## TOP PICKS ON DISK

You can easily get all the public-domain utilities or shareware covered in this month's issue by calling the disk vendor Public Brand Software at (800) 426-3475. Ask for this month's Editors' Picks from *PC/Computing*. They're available for $5 or less per disk (most disks have several utilities and programs on them), plus $5 for shipping and handling. Visa and MasterCharge are accepted.

### GET.BAT

```
@ECHO OFF
IF (%3)==() GOTO INFO
ENCRYPT "%2" < %1 > %3
DIR %3
GOTO END
:INFO
ECHO.
ECHO GET retrieves files you've
ECHO encrypted with SCRAMBLE or
ECHO ENCRYPT.
ECHO Use this syntax:
ECHO GET file password
ECHO decrypted_filename
ECHO.
:END
```

### SECRET.BAT

```
@ECHO OFF
IF (%2)==() GOTO INFO
ECHO Enter your secret below.
ECHO Press Enter at the end of
ECHO each line.
ECHO Use as many lines as
ECHO necessary.
ECHO When you're done, press
ECHO Ctrl-Z, Enter.
COPY CON TEMP.TMP > NUL
ENCRYPT "%2" < TEMP.TMP > %1
ECHO SECRET > TEMP.TMP
DEL TEMP.TMP > NUL
GOTO END
:INFO
ECHO.
ECHO SECRET.BAT lets you enter
ECHO text, and uses
ECHO ENCRYPT.COM to hide it in a
ECHO file of your choice.
ECHO Use this syntax for the
ECHO command:
ECHO SECRET filename password
ECHO.
:END
```

bility that a snoop with a disk editor will find the remnants of the decrypted temporary file on your disk. Because the decrypted text in the RAM disk is never written to your hard disk, it disappears forever as soon as you turn off your computer.

One final word of warning to those tempted to be inventive with their passwords: Don't get carried away. There's no key that will let you decrypt a file whose password you have forgotten. For safety's sake, use the same password for every file—you'll be less likely to suffer a memory lapse. ◪