P.O. Box 3506
Chico CA 95927
wwww.documentsdelivered.com

Document #
10253-1
1 of 1

Name	Order ID	Order Date	Client Reference | Billing Number	Service
Jeff Bosh	10253	05.08.2014 1:42 pm	41484-80050/Broughan	Regular Order

Document Details

Source : PC Magazine

Volume : 5

Issue : 1

Date : 1986 Jan

Pages : Cover, Table of contents, 164-182

Author : Taylor J

Title : The Copy-Protection Wars

Order Options

☑ Title Page if Available	☐ Datestamp	☐ English Only
☑ Table of Contents if Available	☐ Color if Available	☐ Extra Clean
☑ Copyright Page if Available	☐ Hardcopy Only	☐ Include Suppl. Material if Available
☐ Digital Only	Notes	

Quality Notes

Best copy available
We obtained this from microfilm.

THE INDEPENDENT GUIDE TO IBM PERSONAL COMPUTERS

PC

Volume 5 Number 1
$2.95

January 14, 1986

FIRST LOOK AT JAVELIN

THE BEST OF 1985

Beyond 640K: PC Labs Tests Expanded/Extended Memory Boards

Paradox: A Database Manager with a Spreadsheet Format

The Copy Protection Wars: A Report from The Front

PC Magazine Picks the Most Memorable Hardware and Software Of the Year

0 71486 02391 02

PC
The Independent Guide to IBM Personal Computers

PUBLISHER	William Lohse
EDITOR	Bill Machrone
EXECUTIVE EDITORS	Barry Owen, Paul Stetherson
SPECIAL PROJECTS EDITOR	John Dickinson
SENIOR EDITOR	Bill Howard
TECHNICAL EDITOR	Craig L. Stark
ASSISTANT MANAGING EDITORS	Lipsa Simone, Gus Venditto
MANAGER, COPY EDIT	Linda Louk
ASSOCIATE EDITORS	Charles Bermant, Jennifer de Jong, Lisa Kleinman, Barbara Krasnoff, Stephanie Stallings
SENIOR COPY EDITOR	Janet Lewis
PRODUCT TESTING EDITOR	Michael O'Cone
PRODUCTION EDITOR	Paul B. Ross
ASSISTANT EDITORS	Gerald Carney, Victoria Danoff, Virginia Dudek, Cheryl Goldberg, Jane Mintzer, David Obregón, Ann Ovodow
COORDINATING EDITOR	Greg Pastrick
EDITORIAL ASSISTANTS	David Baker, Christina Dyar, Christopher Johnston, Christina Okang, Paul M. Stafford, Al Weisel
BUSINESS MANAGER	Iris Knittel
PROOFREADERS	Michael Cohn, M. Stephanie Ricks
TECHNICIAN	Charles Rodriguez
RECEPTIONIST	Frieda T. Smallwood
CONTRIBUTING EDITORS	Richard Aarons, Frank J. Derfler, Jr., Glenn Hart, Steve Holzner, James Langdell, Stephen Manes, Peter Norton, Charles Petzold, Martin Porter, Winn L. Rosch, Craig Stinson, Jared Taylor, Robin Webster
ASSISTANT to the PUBLISHER	Suzanne N. Silver
DESIGN DIRECTOR	Peter J. Blank
ART DIRECTORS	Mary Zisk, Gerard Kunkel
ART EDITOR	Mariano Nicieza
ASSISTANT ART DIRECTORS	Monique Cubicciotti, Ilissa Goodheart
LAYOUT ARTISTS	Natalie Chu, Susan McGuire
ADMINISTRATIVE ASSISTANT	Jill Alexander
PUBLIC RELATIONS MANAGER	Jessica Kelsey
PUBLIC RELATIONS ASSISTANT	Kimberly Humphries
SINGLE COPY SALES DIRECTOR	Bob Woltersdorf
ASSISTANT CIRCULATION MANAGER	Mickey Krueger
CIRCULATION COORDINATOR	Robert Smahl
ADVERTISING OFFICE	Ziff-Davis Publishing Company, One Park Avenue, New York, NY 10016, (212) 503-5100
SENIOR AD. PRODUCTION MANAGER	Roberta Thomas
AD. PRODUCTION MANAGER	Patricia White
AD. PRODUCTION ASSISTANT	Christine LeBlois
SENIOR EDIT PRODUCTION COORDINATOR	Rosemary Taylor
EDIT PRODUCTION COORDINATOR	Randi C. Fox

COMPUTER PUBLICATIONS DIVISION

PRESIDENT	Kenneth H. Koppel
VICE PRESIDENT, EDITORIAL	Jonathan Lazarus
VICE PRESIDENT, PRODUCTION	Baird Davis
VICE PRESIDENT, CREATIVE SERVICES	Herbert Stern
VICE PRESIDENT, CIRCULATION	Alicia Marie Ivans
VICE PRESIDENT, CIRCULATION SERVICES	James Ramaley
VICE PRESIDENT, MARKETING SERVICES	Ann Pollak Adelman
VICE PRESIDENT	Hugh Tietjen
MARKETING MANAGER	Ronnie Sonnenberg
BUSINESS MANAGER	Gary A. Gustafson
EDITORIAL DIRECTOR	Ernest F. Baxter

ZIFF-DAVIS PUBLISHING

President Richard P. Friese **Senior Vice Presidents** Philip Sine, Kenneth H. Koppel **Vice Presidents** Rory Parisi, William Phillips, J. Malcolm Morris **Treasurer** Selwyn Taubman **Secretary** Bertram Abrams

PC: The Independent Guide to IBM Personal Computers ISSN 0745-2500 is published bi-weekly except in July and August for $34.97 for one year (22 issues), $61.97 for two years, and $81.97 for three years. Additional postage $15.00 for Canada and all other foreign countries. PC Communications Corp., a subsidiary of Ziff-Davis Publishing Co., One Park Ave., New York, NY 10016. Second-Class postage paid at New York, NY 10016 and at additional mailing offices. POSTMASTER: Address changes to *PC, The Independent Guide to IBM Personal Computers*, P.O. Box 2445, Boulder, CO 80322. **Editorial and Business Office:** One Park Ave., New York, NY 10016. Editorial (212) 503-5655. Advertising (212) 503-5100. **For subscription inquiries and service,** write to *PC Magazine*, P.O. Box 2445, Boulder, CO 80322, (303) 447-9330. *PC Magazine* is an independent journal, not affiliated in any way with International Business Machines Corporation. IBM is a registered trademark of International Business Machines Corp.

BPA

The Independent Guide to IBM Personal Computers

VOLUME 5 NUMBER 1 • JANUARY 14, 1986

FEATURES

COVER STORY

The Best of 1985 (and Some of the Worst) **107**

Honoring the tradition of ringing out the old before ringing in the new, *PC Magazine* takes a fond look backward. We asked our editors and writers to nominate the PC-related products they consider The Best of 1985. And since we couldn't resist poking fun at the year's more outrageous turkeys, we've included some tongue-in-cheek "Worst Product" nominations.

HARDWARE

Enlarging the Dimensions of Memory **120**

Charles Petzold, Phil Wiswell, and Winn L. Rosch/Good news—your software's style need no longer be cramped by the 640K-byte limitation. Two methods now break that memory barrier: extended memory and expanded memory. Although both schemes add multiple megabytes of storage, the techniques they use are very different. Extended memory, available only on PC ATs and compatibles, builds a potential 15 megabytes of RAM on top of the existing 640K bytes. Expanded memory, available for PCs and XTs, uses a simple bank-switching scheme to pack more memory into the same space. *PC Magazine* explains the differences, offers a quick-decision guide, and benchmarks 12 boards.

COLUMNS/DEPARTMENTS

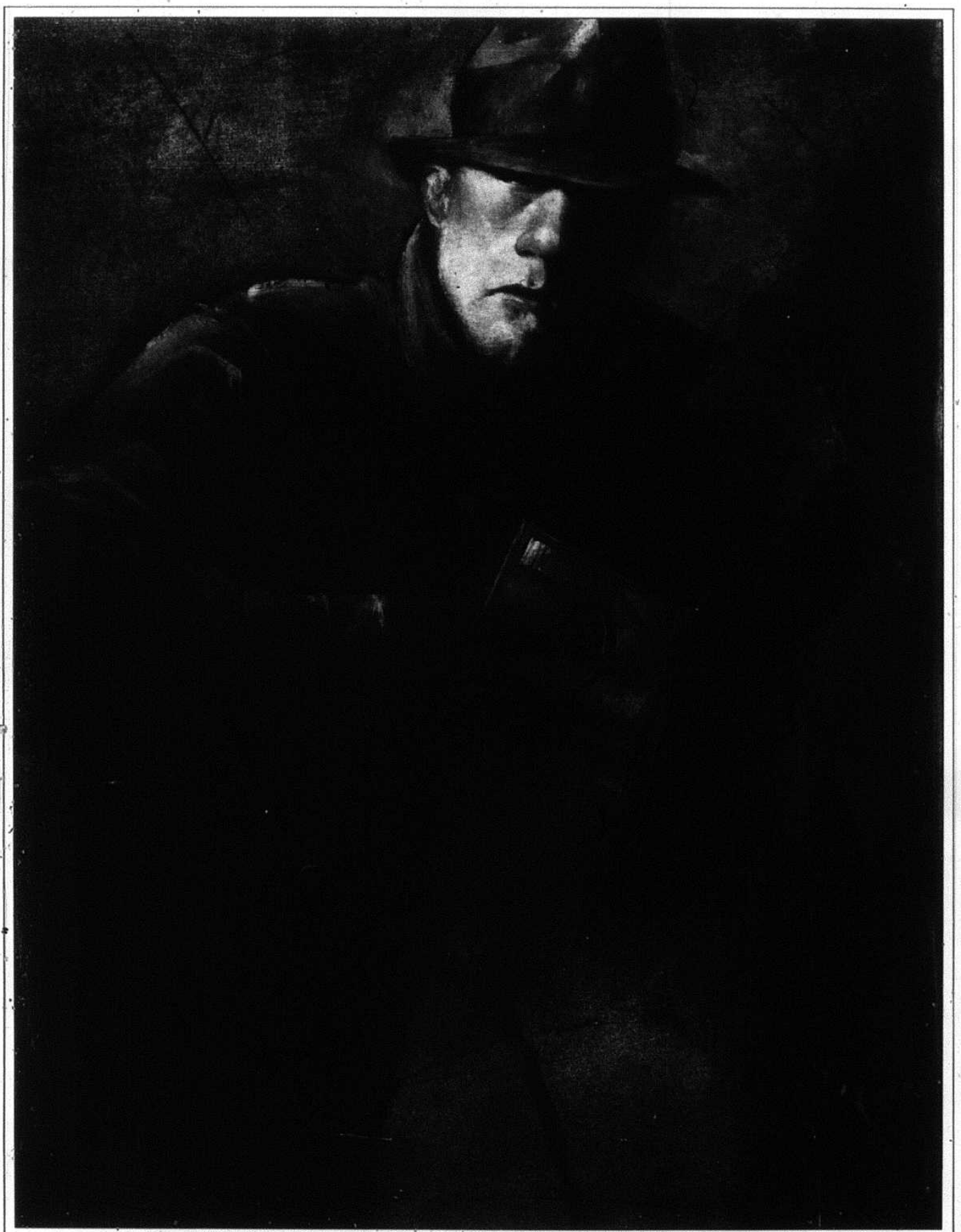


Illustration: Kent Williams

THE COPY-PROTECTION WARS

Software vendors and end users battle over the right to make money versus the right to make backups. Both sides possess powerful arsenals.

Quietly but constantly, the war rages between those who protect software and those who copy it. It's a fascinating struggle of brains and imagination, with each side in business to outwit the other. Like a miniature arms race, each new weapon quickly gives rise to another, and countermeasures are foiled with counter-countermeasures. Lately there's been escalation as both sides roll out hardware in a fight that until now has mostly been fought with a software arsenal.

The struggle for data security rages on the same battlefield. As personal computer use spreads, more and more users need to protect sensitive data. Here, the first round has clearly gone to the protectors. Even inexpensive data-protection programs use exotic encryption methods that may be foolproof. In just a few seconds, you can scramble a file so thoroughly that not even the C.I.A. can read it. However, the real threat to your data can come from unexpected sources.

The problem of unauthorized copying is especially serious for the microcomputer industry for two reasons. First, software and data can be extremely valuable. Second, anyone with a computer can make perfect copies of originals. Record companies would have the same problem if records cost hundreds of dollars and anyone with a record player could make a perfect copy for next to nothing.

Software copying is such a temptation that, if we're to believe the software industry, nearly everyone is doing it. According to a survey done in January by Future Computing, one pirated copy of business software is in use for every legitimate copy. If you make the conservative assumption that one in four pirate users would have bought the program if unable to copy it, then last year the software industry lost $600 million to piracy. No wonder vendors protect their programs.

Two Kinds of Protection

There are two ways to protect a computer program—with hardware or software. Classic software-based protection itself has two parts. The first element is a magnetic pattern or "fingerprint" in one spot on each original copy of a program disk. The second part is a small check pro-

gram that looks for this fingerprint. When you try to start the protected program, the check routine runs first. If it finds the fingerprint, it figures the disk is an original and loads the application program.

What happens when you use DOS to copy a protected disk? Everything will copy perfectly except for the fingerprint. When you try to run the program, the check routine won't find the fingerprint and therefore won't run the application program. The copy protection is thus based on the fact that the NEC disk controller used in the IBM PC can recognize the odd magnetic pattern of a fingerprint on the original disk but can't reproduce it on a copy.

How is it that a system that normally makes perfect copies can read things it can't write? Rick Landuyt, president of a copy-protection company called Glenco Engineering, explains: "Electronically speaking, reading and writing are entirely different. They're separate circuits, just as your eyes and ears are separate circuits. You can see the color red, but you can't hear it. In the same way, the PC reads things it can't write." In effect, the fingerprint on a protected disk is a disk error. It's useful for DOS to be able to detect errors, but there's no reason for it to replicate them.

Companies that make protection schemes have invented many different kinds of fingerprints. The IBM PC formats a blank disk so that it writes data in separate tracks. Each track is divided into eight or nine sectors (depending on the version of DOS) with 512 bytes per sector. A typi-

PC FACT FILE

Personal Copier
Disk-Tech
P.O. Box 162
Waseo, IL 56183
(312) 365-2803
List Price: $39.95
Requires: 128K RAM.

CIRCLE 672 ON READER SERVICE CARD

SuperKey
Borland International Inc.
4585 Scotts Valley Dr.
Scotts Valley, CA 95066
(408) 438-8400
List Price: $69.95 without copy protection
Requires: 128K RAM, one disk drive, DOS 2.0 or later.

CIRCLE 664 ON READER SERVICE CARD

Copy II Option Board
Central Point Software
9700 SW Capitol Hwy., #100
Portland, OR 97219
(503) 244-5782
List Price: $95 plus $3 shipping charge
Requires: 128K RAM, one 360K drive.

CIRCLE 669 ON READER SERVICE CARD

FILELOK
Vault Corp.
2649 Townsgate Rd., #500
Westlake Village, CA 91361
(800) 445-0193 (800) 821-8638 (in Calif.)
List Price: 2-pak (two diskettes) $16.65
Requires: 128K RAM.

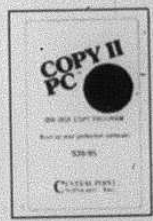
CIRCLE 668 ON READER SERVICE CARD

PROLOK
Vault Corp.
2649 Townsgate Rd., #500
Westlake Village, CA 91361
(805) 496-6602 (800) 445-0193
List Price: 2-pak (two diskettes) $17.40
Requires: 128K RAM.

CIRCLE 667 ON READER SERVICE CARD

Copy Write
Quaid Software Ltd.
45 Charles St. E., 3d Fl.
Toronto, Ontario
CD M4Y 1S2
(416) 961-8243
List Price: $50
Requires: 256K RAM.

CIRCLE 671 ON READER SERVICE CARD

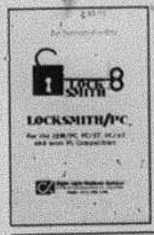


Copy II PC
Central Point Software
9700 SW Capitol Hwy., #100
Portland, OR 97219
(503) 244-5782
List Price: $39.95 plus $3 shipping charge
Requires: 64K RAM.

CIRCLE 670 ON READER SERVICE CARD

Privacy Plus
United Software Security Inc.
8133 Leesburg Pike
Vienna, VA 22180
(703) 556-0007
List Price: perpetual corporate license (unlimited number of machines and sites) $146.25. Perpetual site license (one site) $48.75
Requires: 64K RAM.

CIRCLE 663 ON READER SERVICE CARD



Locksmith PC
Alpha Logic Business Systems
4119 N. Union
Woodstock, IL 60098
(815) 568-5166
List Price: $79.95
Requires: 192K RAM; IBM PC, XT, or compatibles.

CIRCLE 659 ON READER SERVICE CARD

ENC-300, ENC-304, ENC-305, ENC-306
Jones Futurex Inc.
3079 Kilgore Rd.
Rancho Cordova, CA 95670
(916) 635-3972
List Price: ENC-300, $245; ENC-304, $595; ENC-305, $995; ENC-306, $895
Requires: 128K RAM, MS-DOS 3.1 or earlier.

CIRCLE 662 ON READER SERVICE CARD

MagLock
Flinder Software Laboratories
169 Burnside
Tanwanda, NY 14150
(716) 693-0584
List Price: $89 plus $5 shipping and handling
Requires: 128K RAM, PC-DOS 2.0 or later.

CIRCLE 661 ON READER SERVICE CARD

Disk Mechanic
MLI Microsystems
P.O. Box 825
Framingham, MA 01701
(617) 926-2055
List Price: $70
Requires: 192K RAM on PC or XT, 256K RAM on AT, and 320K RAM on COMPAQ.

CIRCLE 660 ON READER SERVICE CARD

Knight Data Security Manager
AST Research Inc.
2121 Alton Ave.
Irvine, CA 92714
(714) 863-1333
List Price: $295
Requires: 128K RAM, hard disk drive, DOS 2.0 or later.

CIRCLE 665 ON READER SERVICE CARD

The Access Key
Gordian Systems Inc.
3512 W. Bayshore Rd.
Palo Alto, CA 94303
(415) 494-8414
List Price: $30

CIRCLE 666 ON READER SERVICE CARD

cal fingerprint might be a track made up of a peculiar number of sectors or a series of sectors that are an odd size. One of the most common schemes is to physically overlay a series of sectors. Another is to give a sector a strange ID.

Another fingerprinting technique uses *weak* bits. These bits are of unstable data that have a different value every time they're read. In a copy-protection scheme, the program reads the weak bits several times in a row. If the program gets different values for the data, it knows the data is weak and that the disk is an original. A DOS DISKCOPY command doesn't produce weak bits; it writes permanent values in the sector that was supposed to be weak. Thus, if the check routine finds *strong* bits that return the same value every time they are read, it knows the disk is a copy and will refuse to load.

Some fingerprints are harder to produce than others. A standard PC can actually be made to write simple fingerprints if you use special software to drive the disk controller. Both Glenco Engineering and another well-known copy-protection company, Softguard Systems Inc., sell kits that turn a PC into a copy-protection machine. Strictly through software, they make the disk controller write oddball tracks that DOS normally doesn't allow. Disks with these fingerprints can't be copied using standard DOS utilities.

However, anything that the PC can be made to write with special software, it can be made to copy with special software. Such low-level protection schemes are easily defeated by the many good copying programs that are now available. Disk-Tech, Quaid Software, and Central Point Software all make copy programs that act like the kits sold by the copy protectors (see sidebar, "The Master Copiers"). They analyze the original disk's fingerprint and tell the disk controller to copy it. What software can do, other software can undo.

The copy-protection companies have fought back by using special machines that lay down tracks that the PC's disk controller can read but can't possibly be made to copy. This is, of course, more of a bother for the software producer because it can't duplicate this protection system itself. It must either buy specially formatted disks from the protection company or get the protection company to do the duplicating.

Even so, protection may not be perfect, since the copy-busting program may not have to make a perfect copy of the fingerprint. Kevin Larsen, sales manager of Disk-Tech, which produces *Personal Copier*, gives the example of a copy-protection scheme that might write 101 sectors to the fingerprint track instead of the usual 8 or 9. Even with special software, the NEC controller can't write a track with 101 sectors. However, as Larsen explains, when the protection routine checks the fin-

The Right to Bill

If users have the right to make free, painless backups and software companies have the right to be paid for the fruits of their labor, whose right comes first?

Copy protection is a thorny issue. It's at the heart of a clear conflict between the right of software vendors to guard against piracy and the right of legitimate users to make backup copies. On the basic issues the law is clear: You can't make copies of commercial software to sell or give away, but you can make archival copies. Enough people want to make copies—for whatever reason—to make a good market for companies that sell copy-busting programs.

The rest of the software industry thinks these companies sail under the skull and crossbones. And no doubt some people buy copying software so they won't have to buy anything else. However, the vendors of copying software take a strong public stand against piracy. Central Point, for example, includes ADAPSO's "Thou Shalt Not Dupe" brochure along with its *Copy II PC*.

Mike Brown, Central Point's president, thinks the solution is education. "The computer is too new," he says. "People just don't know it's wrong to steal software." He also argues that if software vendors gave good value for money and were good to their customers, there'd be no need for copy protection.

Brown cites his own products. Most distributors won't carry them for fear of offending other software vendors. That makes *Copy II PC* hard to find. It's also unprotected. This combination is a great incentive to piracy, but Brown says it's not a problem. He keeps his prices low, supports his customers, and issues frequent updates. "We give the customer a reason to like us and to continue to do business with us," he says. "When you do that, you don't need copy protection."

Although Brown's business depends on copy protection, he would like to see it go away. His company is a member of ADAPSO and of the Software Publishers Association, where he preaches his brand of customer service.

W. Krag Brotby, chairman of copy-protection maker Vault, is less sanguine about customer honesty. "As the density of micros becomes greater, the opportunity for software theft increases," he says. Brotby agrees that protection is a nuisance, but he thinks it's necessary. "We've all gotten used to the car lock," he says, "although it's an impediment to using a car."

He also points out that software lets people do in hours what might have taken days or weeks without it. Hunting for a key disk or waiting a few seconds for a protection check is a small price to pay. "Maybe we're looking for too much instant gratification," he says.

Joe Diodati of Softguard makes a living selling copy protection, but he's no evangelist for it. He sees it as an unfortunate necessity with no inherent value. "What utility have we [copy protectors and copy busters] added to the world?" he asks. "All we've done is add to entropy—nobody really gets anything out of it." Ultimately, he too would probably like to see copy protection go away. "Education," says Diodati, "is more important than technology."

—Jared Taylor

gerprint, all it can actually look for is the address of the 101st sector rather than count all 101 to be sure they're there.

To defeat such a scheme, all you have to do is write an address for sector 101 rather than format 101 physical sectors. This the NEC controller card can do. The fingerprint check will then find what it's looking for and be fooled into loading the program.

Getting Tough

It didn't take the protection companies long to get wise to this trick. Now they make programs that run a thorough check for a fingerprint that the PC itself can't possibly write. But still, the copiers can beat them. *Copy Write*, by Quaid Software, has a utility that doesn't even try to copy an ornery fingerprint. Instead, it puts a *description* of the fingerprint on the new disk rather than the real thing. Before you run the copy, you first load a small, memory-resident Quaid utility. At run time, the utility interrupts the protection-checking routine, reads the description of the uncopyable fingerprint from the new disk, and tells the check routine, "Here's what you're looking for." The protection program thinks it's found the real thing and loads the program.

Yet another software-based protection scheme starts with a scrambled, unusable version of the program on disk. As usual, the protection routine first looks for a fingerprint. Part of the fingerprint is a key that unscrambles the program after it's already in memory. Only then will it run.

Bob McQuaid, president of Quaid Software, explains that even if it isn't possible to copy the fingerprint and key perfectly, there's a way to defeat this scheme. A clever utility can capture the protected program after it's been unscrambled and write it out to disk. The unscrambled program can then be copied with no trouble. "We have not found anything that we cannot copy," says McQuaid.

However, as software protection schemes proliferate, it gets harder to design a single program to beat them all. The copy busters have neatly solved the problem with hardware. Central Point and Disk-Tech have both introduced add-on boards for the PC that make perfect magnetic copies of any disk. Central Point's board costs $95 and is cabled to both the disk controller and the drive. When Central Point software is running, the board takes over from the controller. Since it has none of the write limitations of the NEC disk controller, it can copy anything. As Central Point president Michael Brown explains, "It just picks up the data from one disk, puts it down on another and says, 'Next sector, please.' "

Joe Diodati, Softguard's vice president for marketing and sales, takes a dim view of the new boards. "We've been pretty good at being a moving target," he says, "but this is an escalation in the war." Diodati says his company is not planning a hardware counterattack but is trying to find a software technique to outwit the copying boards. Even so, he is generous to the competition. "You've got to give Central Point a hell of a lot of credit," he says. "What they have done is produce a cheap duplication system—it's a nice piece of equipment."

PROLOK burns tiny holes in the protected disk with a laser. This branding makes a physical fingerprint that even the new copy boards can't reproduce.

On the Hard Disk Front

As the floppy disk battle rages, another front has opened up on hard disks. More and more software is designed to run on a hard disk, but that poses a different kind of protection problem. So far, many vendors have taken the key-disk approach. You can copy the protected program onto as many hard disks as you like, but in order to run it, you have to put the original floppy in the A: drive. When the program runs from the hard disk, it checks for the fingerprint just as if it were running from the floppy.

Since some of the most popular programs (*1-2-3*, *Framework*, *Symphony*, *dBASE III*) use this technique, there is incentive to defeat it. The most common method is to use a small, memory-resident utility that sits and waits for the protection routine to hunt for the disk in drive A: The utility ambushes the query, tells it that all is well in drive A: and sends it home. The check thinks it's done its job and runs the program.

Quaid and Nostradamus Inc. both sell memory-resident programs that defeat the key-disk check for some popular programs. Central Point's *Copy II PC* includes a similar utility at no extra charge.

Lately, the hard disk battle has taken a new turn, since legitimate users are tired of key disks. The protection companies have responded with a way to install protected programs so that they run without a key disk while remaining protected. Such programs come with an installation utility that counts how many times you put the program on a hard disk. Two or three shots is all you get. However, since you might decide to move the program to a different hard disk, there's usually an "uninstall" routine to remove the program. Each time you uninstall, you get another chance to reinstall onto a different hard disk.

This technique could work well for site licenses. A large company that wants 500 copies of a program could strike a deal with a software company for a custom-made floppy disk that allowed 500 hard disk installations instead of the usual 2. The deal could include a fat discount on the cost per copy.

Hard disk installation uses the old fingerprint technique. However, since the fingerprint has to be on each user's hard disk, each PC has got to write it. As I discussed earlier, any fingerprint a PC can be made to write on a floppy it can be made to copy—with special software. This sounds like a copy-buster's dream. It's not. Each hard disk fingerprint includes information about the unique physical characteristics of the disk.

As it happens, hard disks are rarely, if ever, identical. Each has a different number of bad tracks in different locations. Thus, if the fingerprint contains this information, even using DISKCOPY to duplicate the contents of one hard disk on another will not make a good copy. The fingerprint on the second disk won't match its physical characteristics and the program won't run.

One way around this, of course, is to

make faithful magnetic copies of the program disk before you use it to install to a hard disk. Then you could use up all the installations on the original disk and still have live copies that will also install. The battle of wits goes on.

The Hardware Wars

Physical copy-protection schemes are a different matter. Of these, the best known is certainly *PROLOK* by Vault Corp. *PROLOK* works by burning one or two tiny holes in the protected disk with a laser. This branding makes a physical fingerprint that even the new copy boards can't reproduce. If the check routine doesn't find the little holes, the program won't run.

This hole scheme sounds like bullet-proof protection, but it's not. Quaid Software took advantage of the fact that *PROLOK* was making a series of checks for the laser burn rather than a single pass. During one of those checks, a Quaid program fooled *PROLOK* into thinking it had found the burn. Vault has taken Quaid Software to court for breaking its protection scheme.

Vault chairman W. Krag Brotby says he knows of no copy program that can defeat the latest version of *PROLOK*. He says the company puts out a new version "roughly every quarter" to take advantage of new releases of DOS and to keep ahead of the copy busters.

Vault also sells a product called *FILELOK* that protects data as well as programs. It comes on fingerprinted disks that are blank except for the check routine. Any data you put on that disk can't be copied. This is a good solution for defense contractors, for example, that routinely deal with sensitive information. For added security, *FILELOK* comes with an option that encrypts the data to make it unreadable as well as uncopyable.

Vault was in the news about a year ago on account of a punitive protection scheme that became known as "Killer PROLOK." Brotby says that Vault developed the infamous scheme at the request of its customers. Many of them had gotten tired of seeing their software pirated in huge quantities, especially overseas. In Mexico, for example, as many as 200 illegally made copies may exist for every legitimate piece of business software. In Singapore and Hong Kong, there are stores that openly sell cheap, pirated programs.

Killer Prolok, which Vault never planned to sell in the U.S., was going to teach pirates a lesson. If it couldn't find the laser holes on a bogus copy, it would wipe out data. If the disk were write-protected, Killer Prolok would wait and bash the next disk. Vault never released the product overseas either, but the very idea scared a lot of people.

The ADAPSO Key

Another physical software-protection technique is the ADAPSO key. ADAPSO, which is headquartered in Virginia and calls itself "the computer software and services industry association," has invented an eleventh commandment: Thou shalt not dupe. However, injunction alone hasn't kept people from duplicating software, so ADAPSO has proposed a true hardware-based protection scheme.

The ADAPSO system would require a lock box and a key. The key would be a small ROM chip that contained a small fraction of a protected program. The rest of the program would be on disk, but without the ROM key the program wouldn't work. The key would go into the lock box, a receptacle about the size of a pack of cigarettes, that, in turn, would plug into a computer's serial port. The lock box would include a pass-through to let you use the port for other things, but its main feature would be a set of slots, or keyholes.

Protected software would come with a disk and a key that you'd have to plug into the lock box. The floppy portion of the program wouldn't be protected, so you could back it up all you wanted. ROM chips seldom go bad, so you wouldn't have to back them up. ROM chips are also damn hard to copy, so the vendor wouldn't

(continues on page 178)

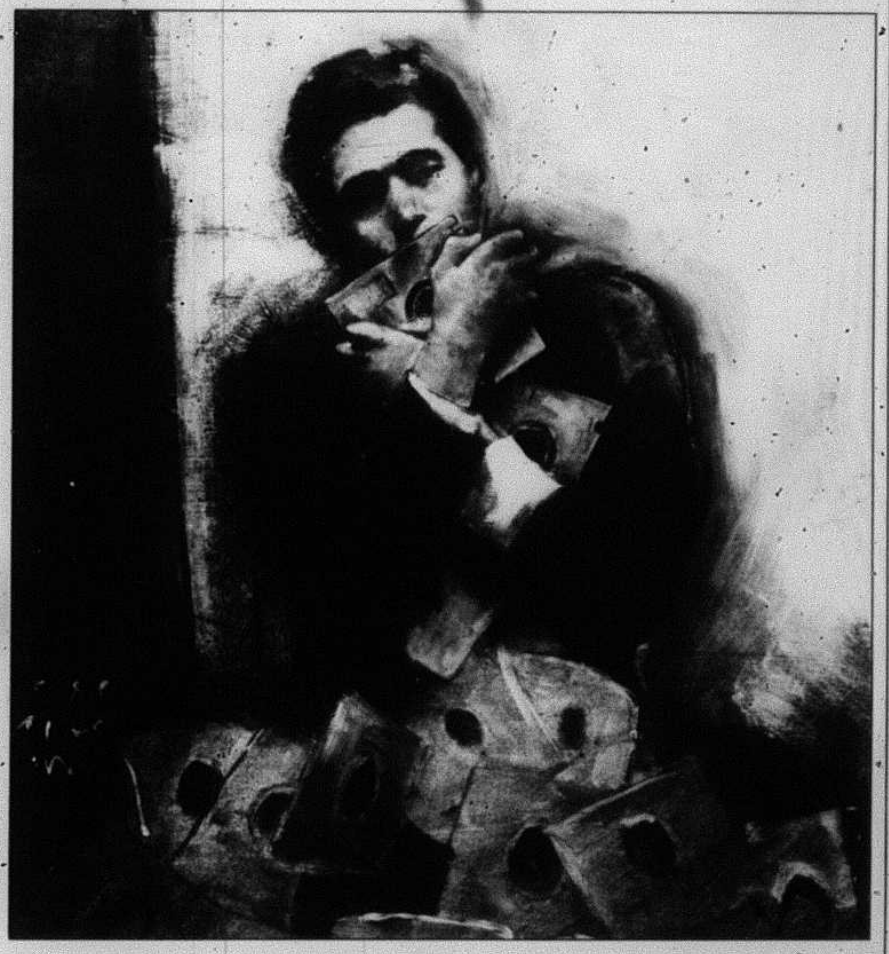


Illustration: Kent Williams

have to worry about piracy.

So long as you left the key in the box, you could run the program any time. If you wanted to run it on another machine, you'd have to crawl behind your computer, pull out the key, and take it with you. You'd also have to have a serial port and a lock box on each machine. Finally, software vendors would have to set standards for the physical characteristics of the key and lock box and for the communications protocols between key and computer. Without standards, you'd have to have a different lock box for each program.

ROM chips are cheap, so the key would probably cost no more than $3 or $4. Lock boxes, even if they were made out of plastic in Taiwan, would cost more. The user, of course, would pay for this stuff.

In spite of ADAPSO's enthusiasm, its key and lockbox proposal has run into a very serious obstacle. Since ADAPSO is made up of competing software houses, the association has to get Justice Department permission before it can set standards. Otherwise the key might be seen as anticompetitive. Last December, ADAPSO asked for a formal "business review letter" from the Justice Department so it could proceed with the proposal. Nearly a year later, the department is still sitting on its hands. Says Dave Sturtevant, senior director of public communications for ADAPSO, "We're now on hold and about as frustrated as you can get." He doesn't know why the Justice Department won't move.

A different hardware-based protection scheme that won't need a green light from the bureaucrats has been developed by Gordian Systems Inc. of Palo Alto, California. The Access Key system works by encrypting or scrambling a program. You can copy it all you want, but it's still scrambled. When you try to run the program, you get a logo screen, a series of flashing lights, and an invitation to type in a password.

The password is coded in the flashing lights, and once again you need a hardware "key" to figure it out. The key is a device about the size of a big eraser with a window at one end and a small, watch-sized liquid crystal panel on one side. When you hold the window up to the flashing lights, a battery-powered chip inside the key de-

The Master Copiers

Each of these five programs has its strengths and weaknesses, but all share a common goal: copying protected software.

Software vendors protect their products for only one reason: They don't trust you. They're afraid that any program that can be copied will be pirated—and they're right. Many computer users don't understand that taking home a copy of a friend's program is like stealing it from a store.

But the software vendors' right to protect their products runs smack into the users' right to protect their investments. Magnetic storage isn't perfect; nothing can spoil your day like a program that won't run. A back-up copy can prevent disaster.

A few small software companies have sided with the user against the vendor: They sell programs that break copy-protection schemes. For copy protectors, these programs are the tools of the pirate's trade, and anyone who sells them is the enemy.

The mainstream software industry has managed to keep these black sheep out of normal retail channels. Many computer stores won't carry them for fear of pressure from the vendors of protected programs, and computer magazines have traditionally tried to ignore them for fear that other advertisers will take business elsewhere.

As a result, copy busters are sold almost exclusively by mail and rely on word-of-mouth advertising. But even this shadowy market has found room for at least five different copying programs for the IBM PC and compatibles. Whether they're used to make legitimate back-ups or illegal copies, clearly there's a demand for them.

All the copying programs I tested come with clear warnings against piracy and none are copy-protected. At the simplest level, they all work by analyzing the format and contents of an original disk and trying to reproduce them on a target disk. It's very much like running the DOS DISKCOPY command, except that this process takes much longer.

In terms of performance, though, these products diverge sharply (see table). Because copy programs are rarely reviewed by the press, second-rate software can sell for the same price as the best.

Generally, if a program can copy one disk that uses a particular protection scheme, it can copy any software that uses it. Since Lotus Development Corp. and Ashton-Tate have switched to Softguard Systems Inc.'s *SUPERLoK* copy-protection scheme for their latest releases, there's a clear line between products that defeat *SUPERLoK* and those that don't. The standard copy-protection-breaking procedure doesn't work on *SUPERLoK*, so programs that break it must use a special technique: They capture the protected .COM file and turn it into an unprotected .EXE file.

Vault Corp.'s *PROLOK* is another protection technique that can't be defeated by the normal copying procedure. Although it's not currently used on any really popular software, it can be broken by only two of the five copying programs reviewed here.

Bear in mind that the protection wars never end. Both the protectors and the copiers come out with new versions as often as once a month. By the time you read this article, the results of PC Magazine Labs' tests will be out of date. By then, the latest releases of the better copying programs should be able to copy Version 2.0 of *1-2-3* and Version 1.1 of *Symphony*. The best way to find out if a program will copy your software is to contact the manufacturer of the copying program.

The Lineup

Personal Copier from Disk-Tech is the lightweight of the lot. It defeats only

the simplest protection schemes and doesn't come with any supplementary programs for dealing with anything complex. After you load *Personal Copier*, you stick the original in one drive and a disk in the other and hit the designated Go key. After 9½ minutes, you either have a working copy or you don't. The instructions all fit on one page, and that's all you need.

Central Point Software's *Copy II PC* is a much better product for the same price. Not only does it copy just about everything except *PROLOK*-protected disks, it also comes with a utility that lets you run protected software from a hard disk without putting the key disk in the A:drive. NOKEY.COM is a small, memory-resident program that intercepts the query to the A:drive and makes the program think it's found the fingerprint on the key disk. It works with *1-2-3*, *Symphony*, *SideKick*, and the older versions of *dBASE* and *Framework* that required a key disk. Other programs on the market do the same thing. *Hardrunner*, at $39.95 for a protected version and $69.95 for an unprotected version, is probably the best known. But why would you buy it if *Copy II PC* does the job at no extra cost?

Copy II PC comes with a long list of the software that it can copy and gives special copying instructions when necessary. It claims to have a routine for breaking *SUPERLoK* protection, even though it failed to work on the *SUPERLoK*-protected copy of *Spotlight* I tried.

The program also has a utility to check the speed of your drives. This statistic can be important if your drives run at slightly different speeds because you'll get better copies if you copy from the faster drive to the slower drive.

> Generally, if a program can copy one disk that uses a particular protection scheme, it can copy any software that uses it.

The instruction booklet is only 5 pages long, but it's clear and adequate.

Locksmith PC from Alpha Logic Business Systems is primarily a disk housekeeping utility program, but it also backs up some protected disks. You can use *Locksmith* to salvage deleted files, examine and change sector data, and analyze disks by track or sector. You can also hide and "unhide" files or encrypt and decrypt them.

The disk utilities are good, but the copy program isn't. Alpha Logic promises updates that can beat *PROLOK* and *SUPERLoK*, but in the meantime, *Locksmith*'s disk-analysis tools are supposed to let you figure out copy-protection schemes and duplicate them yourself.

The 60-page manual does have a lot to say about copy protection and about how disks are formatted, but it doesn't say it well. Clusters, boot records, sector gaps, and cyclical redundancy are complex stuff, and this isn't a clear introduction to them. *Locksmith* originally made a name for itself on the Apple and its PC version still has a recently ported look to it.

Disk Mechanic from MLI Microsystems, like *Locksmith*, is a file-utility program that also backs up disks—but the difference is that *Disk Mechanic* is an excellent back-up program. It can defeat both *SUPERLoK* and *PROLOK* and comes with a list of what it can copy along with special instructions for breaking unusual protection schemes.

The file utilities handle such functions as retrieving erased files, hiding and unhiding, and disk mapping. You can use *Disk Mechanic* to examine or modify any byte in any sector and to check the speeds of your drives.

Disk Mechanic comes with a 60-page manual that, alas, is no clearer than *Locksmith*'s. As the manual suggests, you could probably use *Disk Mechanic*'s utilities to beat copy-protection schemes that haven't been invented yet, but it would take more work and patience than you're likely to have.

A Licensed Scheme

Quaid Software Ltd.'s *Copy Write* is a copy program and nothing more, but it's probably the best. Its copyrighted techniques for defeating *SUPERLoK* and *PROLOK* are so good that MLI Microsystems licenses them for use in *Disk Mechanic*. The program is easy to use and does exactly what you expect.

As a tribute of sorts, Vault Corp. (maker of *PROLOK*) has sued Quaid Software for breaking its protection scheme. Near the end of its 20-page manual, Quaid appeals to *Copy Write* customers to help with its fight against Vault. To do so, you can either send money or evidence that you use *Copy Write* to make legitimate backups rather than for piracy.

Quaid puts out a new edition of *Copy Write* every month. You can "subscribe" for $180 per year.—**Jared Taylor**

Copying Copy-Protected Software

	Type of copy-protection scheme					
	A Lotus proprietary scheme		*SUPERLoK*			*PROLOK*
Copy program	Time for copying *1-2-3* 1A (minutes)	*Symphony* 1.0	*dBASE III* 1.1	*FrameWork* 1.1	*Spotlight* 1.0	*Power-base* 1.0
Personal Copier	9.5	yes	no	no	no	no
Locksmith PC	12	yes	no	no	no	no
Copy II PC	4	yes	yes	yes	no	no
Disk Mechanic	7.5	yes	yes	yes	yes	yes
Copy Write	3	yes	yes	yes	yes	yes

Each of the five copy programs was tested on six pieces of copy-protected software. All the programs were able to copy *1-2-3*; the time they took to do so is given in minutes. The other columns simply indicate whether the copy-protected software could be copied or not.

The Data Encryption Standard

Developed by IBM and adopted and approved by the National Bureau of Standards, the Data Encryption Standard is based on a complicated, effective coding algorithm.

The Data Encryption Standard (DES) is the National Bureau of Standards' (NBS) approved method for protecting sensitive but unclassified computer data. It was adopted in 1977 after the NBS formally solicited encryption algorithms from the public. The one that NBS chose was called the Data Encryption Algorithm (DEA) and was developed by IBM, under the code name Lucifer. DEA is now in the public domain, and it can be used free by any American company. All IBM gets is glory.

NBS got into the algorithm business in order to protect the consumer and to set a uniform standard. Data-protection schemes have been around for a long time, but most users had no idea if they were any good. Now that the NBS has anointed one, most data managers use it with complete confidence. Also, since it's a standard, they don't have to learn a lot of different codes.

Technically, DES is a hardware implementation of the DEA. Encryption programs like *SuperKey* use DEA, but they are not, strictly speaking, DES. Software can be fiddled with, so the NBS puts its official stamp only on hardware.

DEA is a very complex, bit-level algorithm that is described in an NBS publication called *FIPS 46*. A DEA key must be made up of 64 bits, of which 8 are parity bits. In very simple terms, the 56 remaining bits are turned into 16 different subkeys. All 16 subkeys are used on every bit of data, which is processed in blocks of 64 bits. Encryption involves shifting bits around, combining and recombining them until they are thoroughly scrambled. Decryption works backwards through the same steps with the same key.

DEA operates in several modes. In one mode, called chaining, the results of encrypting each block are used as an additional key in encrypting the next block. This is a very secure mode of encryption, but it is seldom used when data must be transmitted. If there is a single transmission error, it will be passed along through the chain during decryption and the data will be unreadable.

Since the algorithm itself is public knowledge, there's no mystery about what's been done to encrypted data. The problem is figuring out the key. Since there are 56 relevant bits to a key, and each bit can be either one or zero, there are 2^{56} or 72,057,594,037,927,946 possible DES keys. That's a little over 72 quadrillion.

Most folks are satisfied with that. In 1980, the American National Standards Institute (ANSI) officially adopted DES. Many U.S. and international banks have converted to DES for coding their payment instructions. Last August, the U.S. Treasury Department announced that all instructions for moving funds in or out of it would have to be coded with DES.

Still, there are skeptics. The U.S. government doesn't use DES for classified information, which suggests that it thinks DES isn't good enough for data it cares about. This makes one wonder whether the government has been pushing DES because the National Security Agency knows how to crack it. Big Brother could read everyone else's mail but keep its own private.

Some code experts, like Dr. Harold Highland, editor in chief of *Computers & Security* magazine, don't believe in the absolute security of large numbers. "The German Enigma code [used during World War II] had over 50 million keys," he says, "and we broke that by hand." In the age of computers, 72 quadrillion may not be such a huge number after all.

Highland also argues against standards: "It takes a lot of patience to break a code," he says, "so it's got to be worth your time to do it. If every bank in the country is using the same code, it's definitely worth your time." There may be convenience in standards, but there's safety in diversity.—**Jared Taylor**

codes the six-character password and flashes it on the liquid-crystal panel. You type it in at the keyboard, and the program will unscramble and run.

The Gordian Method

This scheme sounds like the same protection technique that is defeated by snatching the unscrambled version of the program out of RAM. There is, in fact, no defense against a utility that stops execution of a program and reads the contents of memory to disk. However, Gordian claims that the unscrambled version thus captured will not run. This defensive strategy works by taking a survey of the characteristics of the machine in which the program has been loaded at the time it is unscrambled. Thereafter, it checks every so often and if it finds it has been moved to another machine, it will refuse to run.

One slick feature of The Access Key system is that every time you run the program, it uses a random-number generator to produce a different six-character password. Thus, you never have to remember a password, but you can't run the program without a key. All keys have serial numbers so you can get a replacement if you're in a jam.

Just to make things harder for anyone to break the password code, The Access Key *changes* the coding scheme every 36 hours. When the protection software runs, it first checks the system date and modifies the encryption pattern accordingly. Only then does it throw up the logo screen and ask for the password. How does the key know what decoding method to use? It contains a quartz watch that tells it the date, and it, too, changes its decoding system every 36 hours.

The Gordian key is primarily an encryption/decryption device that is cunningly used to protect software. It can easily be used for data security. In this mode, you use a special software routine to make the key act as an encryptor. What started out as a readable file is now garbage. You use the same software routine and key to decrypt the file. This time, instead of keeping the unscrambled file in memory, the system writes it back to disk in readable form. Thus, the Gordian key is also a weapon in the battle for file security.

Protecting Your Data

There are many ways to keep data out of the wrong hands. One obvious way is to keep it all on floppies and to keep the floppies locked up. If you need more storage, you can use removable hard disks and keep them in a safe.

If you have a fixed disk, one clever way to fool snoopers is to make it look as though the data isn't there. *MagLock*, by Flinder Software Laboratories, is a program that fiddles with the directory table so that DOS doesn't know your files are on the disk. *MagLock* can hide single files, subdirectories, or the contents of a whole disk, and it takes .85 seconds per file no matter how large or small. The data itself is untouched and will show up as bad sectors if you run a CHKDSK. Your files are still accessible to a snoop with a disk utility that reads individual sectors.

AST Research has developed a similar scheme called *Knight Data Security Manager*. It takes between 300K to 400K bytes on your hard disk and will ask for your name and password every time it boots. It is for multiuser systems, and it can be set up to keep certain people out of certain subdirectories. It also has an auditing option that records how much time people spend in which directories and how many times they try to get into off-limits directories. *Knight* is also set up so that if you boot from a floppy, DOS doesn't know the hard disk is there. If you ask for a directory, DOS gives you an "invalid drive spec" message. *Knight* also gives you the option of encrypting files.

Codes and Ciphers

A good way to keep data safe is to make it unreadable to anybody else. Soldiers and diplomats started doing this thousands of years ago when they invented codes, or ciphers.

Some codes are childishly simple. Take pig Latin. You code a word by moving the first consonant(s) to the end of the word and adding "ay." Implesay odescay ancay ooklay ickytray. To decode, you do the reverse. This procedure for scrambling and unscrambling data is called an algorithm.

A simple computer-data encryption algorithm might increase the ASCII number of every character by a set number. If you choose to increase it by 20, the letter *K* (ASCII 75) would become a hyphen (ASCII 95), and the number 4 would become the letter *H*. To decode the file, you would reduce all the ASCII numbers by 20. The ASCII shift is the algorithm and the number 20 is the key, or password. An algorithm that consistently replaces one piece of data with another is called a substitution algorithm.

MagLock fiddles with the directory table so that DOS doesn't know your files are on the disk. It can hide single files or subdirectories in .85 seconds per file.

Permutation algorithms are another kind. If you were coding data in blocks of 64 characters, you might move every third character one place to the right. Even such a simple permutation algorithm, in combination with a substitution algorithm, would take a little while for an amateur to figure out. Real computer encryption algorithms, such as the U.S. government's Data Encryption Standard (DES) are, of course, much more complex (see "The Data Encryption Standard").

Although many encryption programs are on the market, one of the most widely available is included in *SuperKey* by Borland International. *SuperKey* actually contains two encryption methods, one a full-blown DES and the other a proprietary Borland algorithm that is not as complex but runs faster.

In both cases, the key or password can be up to 32 characters long. The encrypted file is written right over the original file, so no trace of the original is left on disk. If you type an encrypted file, all you get is smiling faces, Greek letters, and musical notes.

Borland also offers a text mode for encryption if you want to send code through a modem with a communications program that doesn't handle binary files. This mode produces a file that contains only the capital letters *A* through *Z* and is a good deal longer than the original file. If the person at the other end of the phone lines knows the password and also has a copy of *SuperKey*, he can decode the file.

Another company, United Software Security, produces an encrytion program called *Privacy Plus*. It, too, offers DES encryption as well as a simpler algorithm that is twice as fast. It also produces text mode for confidential data transmission. Like the Gordian system, it offers a hand-held device that decodes randomly generated passwords from flashing lights on the screen.

One interesting option on *Privacy Plus* is "master-keyed" encryptors, which permit multileveled, or "hierarchical" security. These programs are set up so that no matter what key you use to encrypt a file, there is always another one—a sort of skeleton key—that will also decrypt it. This makes sense in a company where a lot of people work with sensitive data. The security officer issues master-keyed versions of *Privacy Plus* to the employees. They can protect their data from each other and from outsiders, but if someone is out sick or forgets the password, the security officer can use the master key to decode anybody's files.

Hardware Encryption

Master keys may be handy for some purposes, but they point up an important weakness in encryption that's done with software: A clever hacker might fiddle with your program and insert a homemade master key, using it to decode everything you coded, and you might never know.

Encryption on a chip is the solution. Jones Futurex sells encryption boards for the IBM PC that incorporate tamperproof DES-standard chips made by Advanced Micro Devices and Western Digital.

COPY PROTECTION

Hardware encryption is also much faster than software encryption; Futurex boards clip along at 12,000 bytes per second. If you were running *1-2-3* or *WordStar*, the board would automatically encrypt everything you wrote to disk and decrypt everything you read. Your application wouldn't run noticeably slower, your data would never be on-disk in readable form, and you wouldn't have to encrypt your files at the end of the day.

The more expensive Futurex boards go one step further, with an EPROM chip you can program with 64 encryption keys. Once again, a company's security officer would choose the on-board keys and also assign passwords to the system's users. The users' keys would work only with boards that were programmed to accept them. That way, disgruntled employees couldn't buy an identical Futurex board, take it home, and use it to decode company data. Even if they had valid user keys, the new board wouldn't be programmed with the matching on-board key.

As an extra barrier to sub-rosa decryption, 32 of the programmable keys are designed to disappear if you take the board out of the machine. That way you can't even sneak the company board home for a little decoding.

As a final precaution, Jones Futurex puts a steel case around the EPROM chip and fills the case with epoxy. There's a trip wire running through the epoxy, so if you try to cut through it, you'll destroy all the programmable encryption keys. This is real, hard-boiled security and probably more than most people need.

Know Your Enemy

However, the Futurex system underlines one of the differences between copy protection and data security. On the first battle front, it's a clear fight between copy protectors and copy busters. On the second, the combatants aren't always clear. Today's encryption algorithms are so arcane that anything that gets coded stays coded—unless there's an inside job.

But whichever side of the struggle you're on, the battle is far from over, and new weapons go into action every day. ■

Jared Taylor is a contributing editor of PC Magazine.