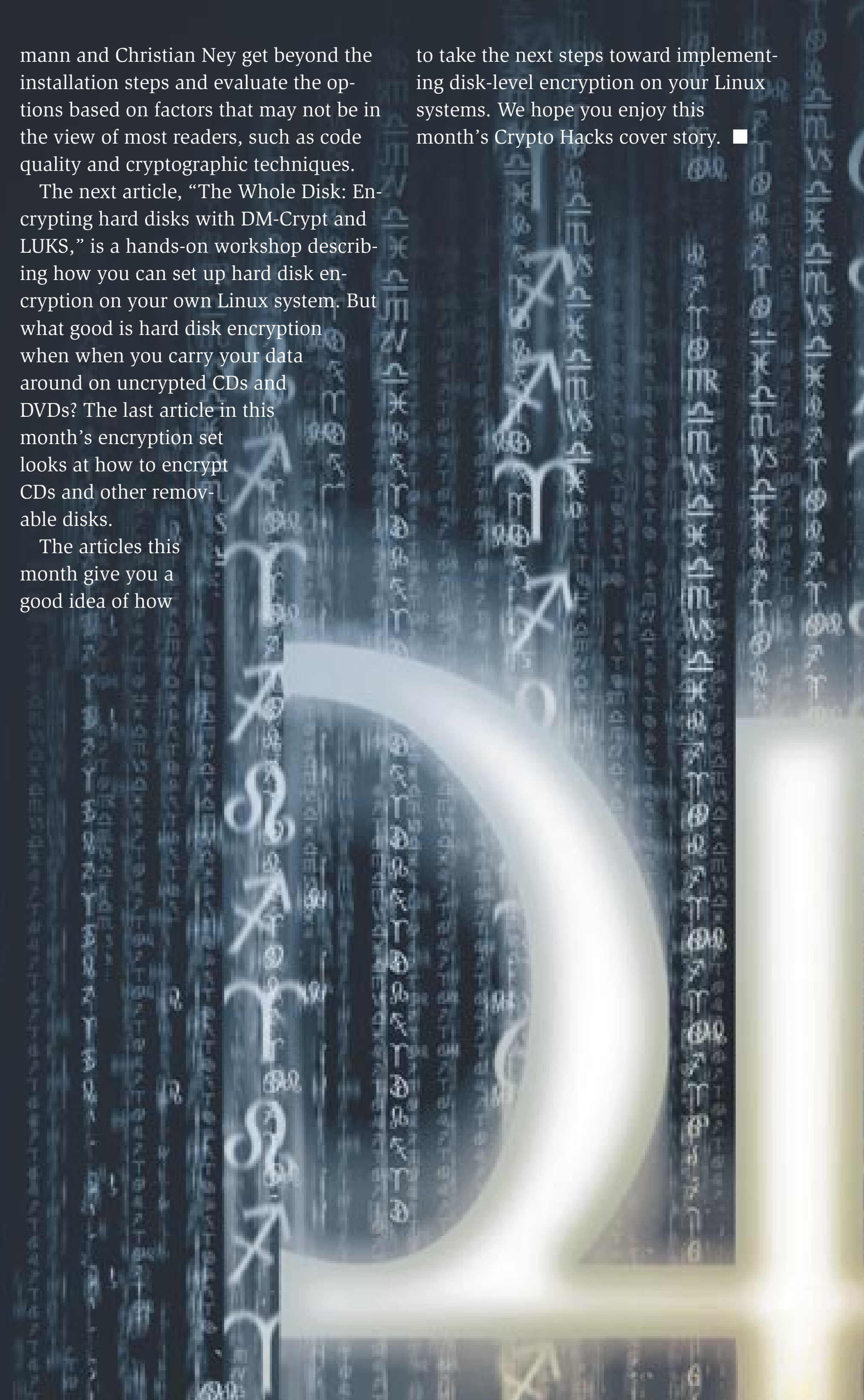
Disk-level cryptography in Linux

SECRETS AND DISKS

Today's computers are fast enough for some very sophisticated cryptography techniques. We'll show you how to keep your data safe from the prying eyes of snoops and spies. **BY JOE CASAD**



Spies, soldiers, and mathematicians have been toying with cryptography for centuries, and every year, computer users gain new powers for concealing their documents and messages. Of course, users *need* new and better techniques for hiding their data because computers are getting so accessible and portable. What if you leave your laptop at Starbucks? Or what if an intruder slips into an empty chair at one of the 100 desktop PCs on your office network?

Encrypted filesystems offer powerful protection for today's casual computer culture. With an encrypted filesystem, your data is safe even if the computer is turned off and the disk is removed. If you've ever worried about spies, soldiers, mathematicians, and everyday nosy people getting their hands on your valuable information, you'll love this month's Crypto Hacks cover story.

We'll start out with a review of some of the most popular encrypted filesystem options for Linux, including Loop-AES, DM-Crypt, Truescript, Crypto-FS, and Enc-FS. Cryptography experts Peter Gutmann and Christian Ney get beyond the installation steps and evaluate the options based on factors that may not be in the view of most readers, such as code quality and cryptographic techniques.

The next article, "The Whole Disk: Encrypting hard disks with DM-Crypt and LUKS," is a hands-on workshop describing how you can set up hard disk encryption on your own Linux system. But what good is hard disk encryption when when you carry your data around on uncrypted CDs and DVDs? The last article in this month's encryption set looks at how to encrypt CDs and other removable disks.

The articles this month give you a good idea of how to take the next steps toward implementing disk-level encryption on your Linux systems. We hope you enjoy this month's Crypto Hacks cover story. ■

COVER STORY