Requirements

System 7.0, hard drive

Background

The goal of CryptDisk is to provide transparent top grade partition encryption for Macintosh CPUs. A friend and I were talking about the lack of encryption programs on the Mac and the general bungling of existing programs which usually have hideous Mac interfaces or terrible cryptography. There are exceptions, but not many. The most surprising thing is that some of the best examples of this trend are actually commercial programs. I walked around MacWorld Expo SF ‘95 asking every security company if they knew of a way to do something like what CryptDisk does. After a lot of public relations nonsense, I pretty much concluded nothing out there would satisfy what I wanted to do. This was unbelievable to me, so I decided to put aside the project I was working on and write CryptDisk. There are at least 5 programs like this available for the PC, but we’ve got drag and drop!

CryptDisk creates files on your hard disk which act as virtual hard disks. You can drop these files on the CryptDisk application to mount them in the Finder after typing in the appropriate passphrase. The mounting idea is similar to programs like ShrinkWrap and MountImage. These CryptDisk files are encrypted with extremely high security using well-known encryption algorithms. The algorithms used in this program are described in detail later in this document. I would specifically like to thank Colin Plumb for his absolutely invaluable and timely cryptographic advice, and Tom Bryce who helped give me a crash course in modern cryptography. The three of us sent a flurry of about 50 email messages to each other to flesh out the algorithms used in this program.

Reading and writing files on a CryptDisk happens just as it would on a normal hard disk except that everything written to the disk is encrypted, and everything read is decrypted. When you unmount a disk by putting it in the trash or choosing “Put Away” in the Finder, the data becomes completely inaccessible until the disk is mounted again. The entire drive is not decrypted when it is mounted. Many encryption programs only let you decrypt an entire set of files rather than individual files wasting time on files you may not need. Only what is needed at any particular time is actually decrypted.

The security of CryptDisk is actually much greater than many encryption programs by its very nature. The fact that the entire disk rather than just a sequential set of files or (worst case) a single file is encrypted means that no one can retrieve your files names, custom finder icons, file lengths, or any other similar data without first defeating all the encryption. Those attributes are often useful in successful attacks on the encryption, so the security is enhanced by encrypting that just as well as the files themselves.