

Academic Computing's (Real) Summer Plans



While relaxing in front of a movie at the new Galileo and McAlister cinemas sounds like a good way to spend the summer (if you missed this exciting new development, see our April Fool's issue of *Occasional Downtime*), summertime is actually one of Academic Computing's busiest times. The absence of most of the students and some of the faculty makes it the best time for us to do major software upgrades, install new software and perform other upgrades and changes to the computer resources at HMC.

This summer Academic Computing has a number of projects we hope to work on. The most major will be an upgrade to the campus network. Our goals will be to increase the capacity and maintain or improve the reliability of the network. The current campus backbone is an FDDI (Fiber Distributed Data Interface) ring. This provides 100 Mbits/second of capacity shared across the campus, from Linde to Olin. This has been a very reliable backbone for us, but we need to increase the capacity. To maintain or improve the network's reliability, we would like to provide some redundancy as we make the upgrade.

Attached to the FDDI backbone are a number of resources (e.g., *osiris*, *Kato*, and *thuban*) as well as two routers. A router is a device that directs traffic from one part of the network to another, for example from our FDDI backbone to an Ethernet port in South dorm. The first HMC router (located in Jacobs) provides a dedicated 10 Mbit Ethernet port for each academic department, plus ports for connecting to the other Claremont Colleges and to the administrative computing network. The second HMC router (located in Linde) provides a dedicated Ethernet port to each dorm. Some of the academic departments are beginning to saturate their Ethernet segment so we need to expand the capacity to those departments.

We are currently meeting with the major network vendors. Although we have not settled on a specific design, the general plan includes two parts. First, we will parallel the FDDI backbone with a new backbone, probably based on 155 Mbit ATM (Asynchronous Transfer Mode) technology. Like the FDDI backbone, this would span from Linde to Olin. This will greatly increase the capacity of the backbone, and the redundancy should improve reliability. The second step will be to install switches (mostly Ethernet switches) in each of the main academic buildings, including Parsons, Jacobs, and Olin. This will allow us to provide additional capacity to the individual academic departments. In addition to "technology" criteria, two of the main criteria for choosing a final design will be that the changes in technology will not require any changes by users and that the changes can be performed incrementally during the summer with minimal downtime.

One of Joe Youn's major projects will be the completion of the long-awaited user database system called QI. This database will contain (continued on page 6)



Software Use in the Humanities and Social Sciences Department

IN THIS ISSUE

AC Summer Plans ----- cover

Software Use in the Humanities and Social Sciences Department ----- 2

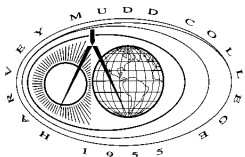
Editor's Notes ----- 3

Data Encryption: Part II ----- 4

Tricks & Tips ----- 7

Q&A ----- 8

Occasional Downtime is composed on a Apple Power Macintosh 6100/66 using Aldus PageMaker 5.0 and Microsoft Excel 4.0. The primary typefaces used are Times and Optima. We wish to thank Sally Rich Arroyo of the HMC Office of College Relations for all her help.



The Humanities and Social Sciences department uses computers throughout its teaching, research, and office management activities. Much of our day-to-day activity utilizes very common software packages, of course; but many of us are also using software beyond the common office products like WordPerfect, Microsoft Word, Excel, and Eudora.

Several department members (Bill Alves, Tad Beckman, Gary Evans, Jeff Groves, and Margo Malakoff) have been serving course materials through the World Wide Web since the fall. During the spring semester, Beckman and Malakoff have also been using NetForms on the new Macintosh Web server, *www4.hmc.edu*, and have been developing interactive course-work on their course-related Web pages. Jeff Groves is developing similar Web materials for the upcoming fall semester.

In his Philosophy 118 seminar, Beckman has three modes of interactive work set up through the Web; students access these modes through Netscape, entering information directly onto the course Web pages through NetForms. Presentation outlines are submitted in advance of class sessions so that students can review what issues will be raised in class. A discussion archive is maintained so that submitted discussion texts can continue and amplify whatever has developed in the classroom. And final papers, based on presentations, are submitted on the Web, one week after the class session; from this location, they are available for the whole class to read.

For basic office management and student advising, the department has made extensive use of FileMaker Pro 2.0. One of the most important features of FileMaker Pro is the fact that it runs on a network and is cross-platform. All members of the department, whether they use a PC or Macintosh, can access FileMaker Pro database files and edit them simultaneously. Another important feature of FileMaker Pro is the versatility of layouts that can be created; a single record can be viewed in a wide variety of ways, including all or excluding some of the fields.

Our most important FileMaker Pro 2.0 file is our advising database which resides on *Kato*. The file maintains records for all HMC students, contains basic information about each student, and tracks courses taken for humanities and social sciences credit. One of the nice features of our advising database file is a graduation application layout (which has been approved by the Registrar) so, when a student's record is complete, we can simply print and sign a copy of this form.

Another very useful database file on FileMaker Pro is designed to organize teaching schedules. The schedule database file also resides in common space on *Kato* where individual faculty can access it and enter their teaching preferences for the coming semester (or year). The file tracks information by individual course and includes course information (field, number, and title), times, places, and special comments or restrictions. As work on the file is completed, the department chair can review the teaching schedule through different layouts, make corrections and

adjustments, and print the final schedule sheets for submission to the Registrar.

FileMaker Pro is also a very effective way of maintaining a bibliography. For instance, Beckman has a bibliography of more than 600 books and articles on Native Americans which includes topical categories, comments, and library locations, aside from normal bibliographical statistics. FileMaker Pro files can be served through the World Wide Web (either from www2.hmc.edu, the Web server on *thuban*, or from www4.hmc.edu) and you can access the Native American bibliography as one of the Web resources under Beckman's Hum 2D course materials at <http://www4.hmc.edu/Humanities/hum2d/>. Both Groves and Sullivan maintain extensive FileMaker Pro databases for their research materials.

Another very useful software package is Harvard Graphics. Gary Evans uses this package to prepare presentation slides for a number of classes. Harvard Graphics is used in two ways: (1) it allows him to make good hard-copy to be handed out in class, reflecting some of the material he shows on the overhead projector, and (2) he projects the slides directly during lectures using either (a) his TI TravelMate 4000 laptop attached to an LCD panel or (b) color transparencies printed from Harvard Graphics on his color inkjet. So far he has used this in Financial Economics, Government Policy, and Introductory Macroeconomics.

Bill Alves combines his teaching in music with computers in several ways. In World Music, he has used a program which he wrote himself about Gamelan Music of Indonesia. It uses sound, images, and video with hyperlinks. It resides in the Humsoc folder in the Macintosh Applications volume on *Kato*. Bill has also written a program for Hum 2 about Debussy (but with an interactive audio CD and no video) and has used a commercial interactive CD program about Stravinsky. (continued on page 7)

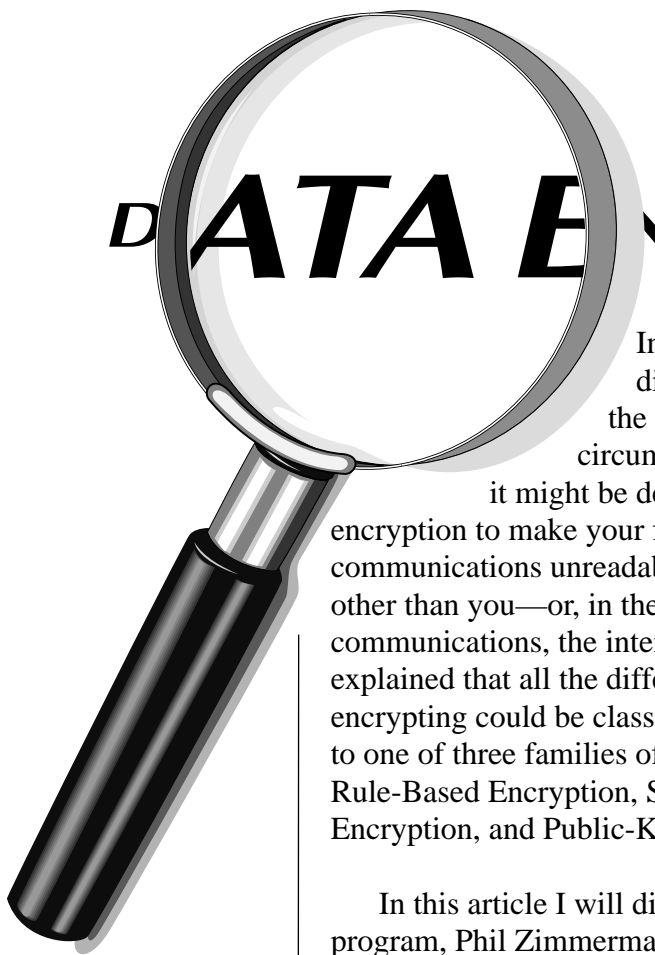
Editor's Notes

Welcome to the anniversary issue of *Occasional Downtime*. This month's issue marks the one-year anniversary of the new *Occasional Downtime* and my taking over as editor. We hope you have enjoyed reading *Occasional Downtime* over the past year and have learned a few things about Academic Computing and the computing resources at HMC.

This month's article in our series on software use in the various departments focuses on the Humanities and Social Sciences department. It should be of particular value to other departments, since the HumSoc department uses some commonly used software packages in very interesting ways. We also have an article on Academic Computing's summer plans (No April Fool's this time!), as well as a short article by Josh Hodas on Pretty Good Privacy, a free data encryption program. This is the second part of his article on data encryption.

—Elizabeth Hodas

Occasional Downtime is published bimonthly by the Academic Computing Department at Harvey Mudd College. It is also available in a variety of formats on the HMC Web Server. Comments and questions can be directed to downtime@hmc.edu.



DATA ENCRYPTION: PART II

In the last article I discussed some of the different circumstances in which it might be desirable to use encryption to make your files or communications unreadable by anyone other than you—or, in the case of communications, the intended recipient. I explained that all the different methods for encrypting could be classified as belonging to one of three families of techniques: Rule-Based Encryption, Secret-Key Encryption, and Public-Key Encryption.

In this article I will discuss just a single program, Phil Zimmerman's *Pretty Good Privacy*, and how it can be used to encrypt both files and communications.

PRETTY GOOD PRIVACY

Pretty Good Privacy (PGP) is a free implementation of the RSA public-key encryption algorithm, which was discussed in the last article, though it also supports “old-fashioned” secret-key encryption of files for those times when it is more appropriate or useful. Zimmerman developed and released PGP in 1991, in response to the US government's first move—in Senate Bill 266, an omnibus anti-crime bill—to restrict access to strong cryptography. Zimmerman believes that strong cryptography should be available to everyone in order to protect the right of privacy. He feels, as he states in the PGP manual, that restricting the use of cryptography for electronic communications is like requiring that all postal mail be in the form of postcards. Even the most idle eavesdropper can access anything he wants.

PGP is free for non-commercial use, though it is not in the public domain. Zimmerman distributed the source code for PGP in order to make it easy to confirm that the system does not have any secret “trap doors” that might allow him or some other person to break PGP-encrypted documents. PGP is distributed by MIT, and implementations are now available for Unix, VMS, MS-DOS, and Macintosh OS. While it does not run directly under Microsoft Windows, a variety of Windows shell programs have been written that put a “pretty” face on the underlying MS-DOS program. Similar shells have also been written for use on X-Windows workstations. PGP is not yet installed for general use on *osiris* or *Kato*, though many individuals have installed it for their own use. It is installed on the VMS cluster. Documentation is available via CLUE. We expect it to be installed on *osiris* and *Kato* sometime soon.

In order to make PGP useful to the widest possible audience, it is designed to encrypt and decrypt files. To encrypt a mail message, the message would first be written in a file. The file would then be encrypted and attached to a mail message. This way PGP does not have to know the details of any particular mail program. Unfortunately, it is a bit cumbersome, and a small freeware and shareware industry has grown up to build shells and scripts which automate this process.

USING PGP DIRECTLY

Recall that in public-key encryption, someone who wishes to receive encrypted communication publishes their public key so that others can use it to encrypt messages intended for them. When you set

up PGP the first thing you will probably do is to have it generate a public key for you to distribute. It will simultaneously generate a private key to be used to decode messages encrypted with that public key. For added security, PGP also allows you to associate a *pass phrase* with the private key. Decoding will require both the private key (which must be stored on the computer, since it is not the sort of thing one could remember) and the pass phrase. PGP allows you to collect public keys from any number of people. They are gathered together in a structure appropriately called the *key ring*.

In the command-line versions of the program encrypting a file is as simple as typing:

```
pgp -e filename recipient
```

where *recipient* is the name of the person to whom the file will be sent. By specifying the intended recipient of the file, you are telling PGP whose key to take from the key ring to encrypt the file. A document can also be *signed*—digital signatures and sender authentication were discussed in the last article—or signed and encrypted by changing the arguments to the command. If no arguments other than the filename are given, then PGP assumes the file contains encrypted text sent to you and will use your private key to decode the file after prompting you for the pass phrase. In MacPGP, and in the various Microsoft Windows and X-Windows shells, these commands would be issued from the menu bar.

USING PGP INDIRECTLY

As mentioned earlier, a variety of tools have been developed to make using PGP easier. The most complete and successful is the MacPGP Accessories Kit, developed by the Macintosh Cryptography Interface Project (MCIP). This is a set of Applescript scripts and user interface tools, for System 7 and above, that add a PGP icon to the Macintosh menubar, right next to the

Balloon Help/Apple Guide icon. From this icon you can access a menu of options that allow you to encrypt and decrypt files, manage keys, and most useful, encrypt, decrypt, sign, and authenticate messages directly inside Eudora, without managing them as files. For Windows, the most popular current option appears to be a package called Private Idaho, which puts an easy-to-use face on PGP. Unfortunately, it does not interface directly with Eudora for Windows. Messages must be transferred to and from the Windows Clipboard. These and many other PGP tools for a variety of systems can be accessed via links on the PGP Tools and Add-ons web page at <http://www.ifi.uio.no/pgp/utills.shtml>.

A company called ViaCrypt (<http://www.viacrypt.com>) holds the exclusive right to sell commercial software based on PGP. They offer a reasonably priced version of PGP with graphical interface for Windows and Macintosh. The next version of their Windows product is expected to offer tighter integration with Eudora for Windows.

It should also be mentioned that Zimmerman has recently released a package called PGPfone (currently available only for Macintosh) that uses PGP to allow secure voice communications by using real-time encryption to encode conversations transmitted over TCP/IP.

GETTING PGP

PGP itself (as well as PGPfone) is distributed at <http://web.mit.edu/network/pgp.html>. Extensive documentation (including very good introductory material on encryption) is also available at that site, and in a variety of FAQs to be found all over the web. 🐉

by Josh Hodas

information similar to a phone book for everyone at HMC. However, it will also include entries for e-mail addresses, e-mail forwarding and Web home pages. The QI system will replace the UserInfo and MailCentral system we have been using. The new system will have all the functionality of the old systems, but will update information as soon as it is entered instead of daily. Users will be able to use the Web to access QI to update their information, as well as to search for information about other users.

We are also considering a replacement for *osiris*. If we do move to a new general-use UNIX machine, Joe will be configuring that system and transferring accounts from the old system to the new system. In any case, we should be updating the system on all AC-operated Suns to Solaris 2.5.

Chris Marble will be working on a project to allow users to have a single password and home directory on the Math, Engineering and Physics HP systems. The first step in this project will be to resynchronize the internal user id's between the three systems. The next step is to set up a unified password file for all three systems. When this project is complete users will have a single password and home directory across all the systems.

In addition to various software installations and upgrades on the AC file server, *Kato*, Patience Brooks will also be working on configuring NDS (Network Directory Service) on our Netware network. NDS is a feature of Netware 4.1, the new version of Netware which we installed on *Kato* last summer. NDS allows us to define a hierarchical tree of our users. Last summer we simply defined one large structure, called "STAFF" and put all of our users in it as a temporary measure. (Yes, that's what that cryptic message means when you first enter your login

name when logging in to *Kato* on a PC). This summer we will be implementing a more complete NDS tree of our users. NDS allows us to organize our users into logical units with specific privileges for each unit.

Cynthia Souza will be working on developing a new FileMaker Pro 3.0 database for purchase orders, requests for checks and for maintaining general ledger records. Cynthia had already implemented a prototype of the purchase order and request for checks database in the previous version of FileMaker Pro (version 2.0) which several other departments have also used. The new version of the database will take advantage of FileMaker Pro's new relational database features. If you are interested in using the database or if you have special features that you would like to see implemented, please contact Cynthia.

In addition to developing new workshops for the summer and the fall semester, Elizabeth Hodas will be developing and testing a new Help Desk database with a Web interface. The database will be implemented using a Macintosh package called Butler SQL. The Web interface will be designed using Academic Computing's Webstar Web server, www4.hmc.edu and a tool called Tango. The Web Help Desk should be ready for use by the HMC community by the beginning of the fall semester. Users will be able to report computer problems and check on the status of their Help Desk problems over the Web. AC staff will be able to check and update the problems they are responsible for over the Web as well.

Academic Computing would also like to request that if you have any summer plans that we should know about, to please contact us as soon as possible. This would include the purchase and installation of any new computers or the installation of any new software on the file server for the fall semester. 🐶

For Music 3, Alves just finished writing a HyperCard stack to drill the students on pitches, intervals, and audio interval recognition. Like the above two programs, it keeps track of the students' use so that he has some record of who used it how much. But Alves' main use of computer software is in Computer Music. The main software used here is CSound, a public domain computer music programming language developed at MIT. Other software packages used in the computer music course include Digital Performer, a professional-level MIDI sequencer, and Deck II, a digital audio recording/editing/multitracking application. These work only on the Media Studio computer. A MIDI sequencer is a program that enables the computer to record key strokes on a keyboard (or other MIDI source), layers that information with previously recorded tracks, allows the user to edit that information, and then plays it back on a variety of sound-producing modules available in the Media Studio.

Margo Malakoff uses special statistical packages in her research and teaching. SPSS is a powerful software package designed to handle large data sets and run many different types of statistical analyses on them. The interface for entering data is quite similar in appearance to various spreadsheet packages (i.e. Excel). Some of the statistics SPSS can handle are ANOVAs, t-tests, descriptives, frequencies, among many others. SPSS additionally allows for the manipulation of data sets for ease in comparing data. For example, SPSS can select cases based upon characteristics of another variable of interest. SPSS allows the creation of new variables based on mathematical manipulations of existing variables and also allows many different types of data (time, string, numeric, alphabetic, date, etc.). 🐾

by Tad Beckman

Tricks & Tips

& Tricks

CREATING A SLIDE SHOW IN POWERPOINT

Powerpoint can be used to create black-and-white and color overhead transparencies, 35-mm slides, and on-screen presentations. The best way to display an on-screen presentation is to use Powerpoint's slide show feature. You can run a slide show in a couple of different ways—the slides can be advanced manually or you can set up a timed slide show.

To run a slide show from within Powerpoint select **Slide Show** from the **View** menu. A dialog box will appear where you can indicate whether you want to manually advance the slides or if you want to create a timed slide show. Once you've made your selection click the **Show** button.

Once you've setup your slide show preferences you can also start the slide show by clicking the **Slide Show** button at the lower left corner of the Powerpoint window. The slide show will begin immediately, without bringing up the **Slide Show** dialog box. It will also begin with the currently selected slide, so be sure to go to the beginning of your presentation before clicking this button if you want to start at the first slide.

Another way to run a slide show is to use the Powerpoint Viewer instead of the full Powerpoint application. This is particularly useful if you want to use a computer that is not your own and that might not have Powerpoint installed on it. To use it just double-click on the Powerpoint Viewer application and select your presentation file in the file dialog box. Then click the **Show** button.

Powerpoint files are cross-platform compatible meaning that you can view a Macintosh Powerpoint file on a PC and vice-versa. 🐾

QUESTIONS *and* ANSWERS

Q: How can I read my e-mail on *osiris* from home this summer?

A: The easiest way is to get an account with an Independent Service Provider (ISP). Most cities now have local ISP's which can provide a connection to the Internet. Once you login to their service you can telnet to *osiris* to read your e-mail. Most ISP's now even offer PPP or SLIP connections which will allow you to use Netscape or another Web browser from home.

If you're working at an organization or company that provides you with a computer account you can setup forwarding on *osiris* so that you receive your e-mail at your work account. See the February issue of *Occasional Downtime* for instructions on how to set up mail forwarding. Just don't forget to remove mail forwarding when you return!

Q: Can I access my *Kato* account from home over the summer?

A: No. Unfortunately there is no way to access your *Kato* account from off-campus.

Q: I'm graduating this May. What happens to my computer accounts when I graduate?

A: Your computer accounts (ie. *osiris*, *Kato*, and *thuban* accounts) will expire on July 1st of your year of graduation. Our policy for alumni accounts can be found on the Web at <http://www.hmc.edu/comp/policy/accounts.html>.

If you are staying at HMC as a student or as a staff member you can request an extension to your account by sending e-mail to help-desk@hmc.edu.

Q: Will I need to request a new IP address for my dorm computer when I get back to school next fall?

A: No, you should be able to use the same IP address as long as you are at Harvey Mudd College.

Q: Have a computer question that has you stumped?

A: Send it to *Occasional Downtime* at downtime@hmc.edu and we'll try and answer it for you! 🐶

