They first created plasmids that could be used in their own version of the reverse two-hybrid system. Basically, the plasmids were designed to create yeast that could synthesize fusion proteins containing the transcriptional activator B42 and the DNA-binding protein LexA in the same cell. When the two proteins dimerize via the fusion protein portion, they turn on transcription of a gene that is toxic and kills the cell. This lethal interaction was made inducible by using the Gal promoter, which can be rapidly switched on with a simple change of media.

Next, they set out to scale the system such that it would work in nanoliter cultures. To rapidly deliver small quantities of a test small molecule, they took advantage of the fact that combinatorial synthesis can be performed on small beads. By incorporating an ultraviolet (UV)-sensitive linkage into the process, they were able to make a molecule of the form drug-linker-bead. In their test case, the drug was FK506. With the photolytic effect of a short UV pulse, FK506 could be rapidly released.

To make cultures in which the small amount of released drug (about 100 pmol/bead) would have a reasonable concentration, they used a new technique that can deliver droplets of defined numbers of yeast, media, and a drug bead in 100- to 200-nl increments (*2*). In these nanodroplets, growth can be easily scored visually in large arrayed formats. They tested the whole system with a mock experiment by showing that FK506, a known inhibitor of the interaction between the proteins FKBP12 and TGF-β receptor, could actually block the lethal action of this toxic two-hybrid construct.

The new nanodroplet yeast technique is significant in that it serves as a method that can bridge two fairly evolved fields, combinatorial chemistry and yeast molecular genetics, with the young field of genomics. The ever increasing number of proteins found to interact in the two-hybrid screen can now be tested in bulk for small inhibitors. Tests can even be performed on mixed populations of two-hybrid–positive proteins to sort out those interactions that can be blocked by a selected inhibitor.

–Robert Sikorski and Richard Peters

References

1. J. Huang and S. L. Schreiber, *Proc. Natl. Acad. Sci. U.S.A.* **94**, 13396 (1997).
2. A. B. Borchardt *et al.*, *Chem. Biol.* 4, 961 (1997); A. You *et al.*, *ibid.*, p. 969.

Digital mailbox:
www.sciencemag.org/dmail.cgi?53492b

Jamming Spam

NET TIPS

No, we're not talking about some odd new cuisine here, but rather a plague: the problem of junk e-mail. Known in the Internet culture as "spam," junk e-mail can be mass mailings to bulletin boards, newsgroups, or lists of people. While mailings from listserves that you subscribe to can be helpful, spam mailings can be annoying. Spam mail can also use up considerable resources on the Net. At some Internet service providers, as much as 10% of their resources is devoted to handling junk e-mail.

How do the spammers—the companies that distribute e-mail ads—get your e-mail address in the first place? One way is simply from online directories. These databases, such as Bigfoot (http://www.bigfoot.com/) and Four11 (http://www.four11.com/) house extensive collections of addresses. Another way is by using software robots that traverse the Net and look for addresses, focusing specifically on the @ sign in World Wide Web pages or newsgroups. This means that if you have put your e-mail address on your lab, university, or company Web page, it is fair game for the "spambots." Newsgroup fishing for e-mail addresses in particular is very easy and efficient. For example, if you post to a newsgroup discussing computer software, the spammer already has a clue to target you with junk e-mail advertising software.

How to avoid the spam? There are three different strategies: protect your e-mail address, use several e-mail addresses, or filter your e-mail.

Strategy 1: To protect your e-mail address, you can send your outgoing messages through an intermediate program called a remailer. This software (usually free) strips the header fields from the message so that the recipient never gets your original address. If you want the recipient to have the ability to send you a reply, you can use a remailer service that tags on its own special address, such as msg1233@remailer.com. During the return trip, the remailer then acts as a switchboard to direct the message back to you. In fact, a remailer can strip the addresses on the reverse path as well so that the entire communication is anonymous. To find out more about how to use remailers, check out http://www.well.com/user/abacard/remail.html.

Strategy 2: Use multiple e-mail addresses. If you intend to post to newsgroups or participate in mailing lists, this is an appealing option. The idea is to have a set of public e-mail addresses that are used exclusively for public purposes. That way, when the inevitable spamming comes, the damage is localized to just these e-mail boxes. To make it even easier to switch e-mail accounts, you can take advantage of the fact that you can now get free addresses that can be accessed through a Web browser. One popular free service is Hotmail (http://www.hotmail.com/). The e-mail service acts like a post office box for regular mail.

Strategy 3: Block incoming spam with software filters. This can be done in two ways: by using the filtering capabilities of your e-mail program or by acquiring a separate anti-spam filter. In the Pro version of the e-mail program Eudora, for example, you can set any number of filters that examine the headers or body of incoming mail. If you get spam from one particular address or it has phrases such as "make money quick" in the subject, it is easy to configure a blocking filter. However, the spammers usually change their address, so you have to change the filter as well. That is where anti-spamming software is useful. This software looks at your e-mail before your mail program does. The better software is designed such that it can learn about new spamming operations and adapt. For the Mac, there is really only one anti-spammer program, called Spam Blaster (http://www.cnet.com/Resources/Swcentral/Mac/Result/Download/0,162,39634,00.html). For the PC, there are several. You might try SpammerSlammer (http://www.cnet.com/Resources/Swcentral/PC/Result/TitleDetail/0,160,0-29003-g,0 0.html).

Use one or all of the above tips, and you should be one step ahead of the spammers. Unfortunately, technology solutions work both ways, and spam operations evolve rapidly. Also, the fact that e-mail advertisement costs about one-thousandth that of printed ads ensures that spamming will continue. To find out more about spamming and anti-spam tactics, we've put together a list of useful Web sites at www.medsitenavigator.com/tips.

–Robert Sikorski and Richard Peters

Digital mailbox:
www.sciencemag.org/dmail.cgi?53494

Tech.Sight is published in the third issue of each month, and appears in Science Online *at www.sciencemag.org. Contributing editors: Robert Sikorski and Richard Peters, Medsite Communications Corp., Boston, MA. The editors welcome your comments by e-mail to techsight@aaas.org. Specific comments and feedback should be routed via the Web with the Digital Mailbox URLs at the end of each item.*

(continued on page 414)