Dr. R. Beezer
Practicum #7
PGP Signatures

Math 133
Fall 2003

In this practicum we will practice with digital signatures using our PGP keys.

Procedure

1. I will send you several numbered messages. All will be digitally signed, but only one will be signed by me.

2. Send me a reply identifying the number of the message that was *really* from me. Sign your reply using your private key. Notice that to sign your message, you use a piece of secret information, your private key, that only you know. The recipient uses your public key (which everybody knows) to verify that it was indeed your private key that was used.

Grading

1. Full credit once I receive the correct number of the genuine message, in a message that is properly signed by you.

Notes

1. Digital signatures are as important (or maybe more so) for the proper functioning of the Internet for secure communications. While we often want to hide information (encryption), we also want to verify the identity of people we communicate with (authentication). People are authorized to do different things, depending on who they are, so it is important that we authenticate identities.

2. Now that we can do digital signatures, from now on I will not recognize any email from you (including discussion group postings and replies) unless it is properly signed. For convenience you might want to install PGP on your own computer, if you haven't already.

3. Losing your key or forgetting your passphrase will not be excuses for doing discussion groups or practicums late. Act accordingly — backup your keyrings to secure media now and choose your passphrase carefully!