Dr. R. Beezer
Practicum #6
PGP Encyption

Math 133
Fall 2003

In this practicum, we will use our PGP keys to encrypt messages to each other.

Procedure

1. I will send you a message, encrypted with your public key.
2. Use PGPtools and your private key to decrypt my message (see below). Notice that whenever you want to access your private key, you must verify your identity by typing the passphrase associated with your private key.
3. Determine the author of the passage I sent you (Google would be a good tool to use for this).
4. Send me a message, encrypted with my public key, containing the name of the author. Notice that anybody can get my public key off a keyserver, or my WWW page, but they will not immediately be guaranteed that it is really *my* key. However, you have verified my fingerprint in class during our keysigning party, so you know the key I sent you is genuine.

Grading

1. Full credit once I receive the author's name, properly encrypted to me.

Notes

1. Here's how to use PGPtools for encryption. Got to Start > Programs > P G P > PGPtools. Then fire up whatever you use for email, probably Webmail. Compose a new message, then highlight it and copy it to the clipboard with Ctrl-C. Click on the "encrypt" button in PGPtools (second from left, closed lock on an envelope). The dialog box has a button in the lower right-hand corner that says "Clipboard." Click on this and PGP will encrypt whatever is on the clipboard (your message in this case). Be careful about being sure to place the correct key in the right area for the recipients when asked which keys to use for encrypting the message.

   Once the contents of the clipboard have been encrypted (you won't see any noticeable changes anywhere) go back to your message in your mail program. Highlight the text, and do a paste with Ctrl-V. This will erase your original message and replace it with the encrypted version. Now send the message as usual.

2. To decrypt, reverse the process above. When you receive an encrypted message, copy the whole thing, especially the parts that indicates the beginning and end of the message. Once on the clipboard, use the Decrypt/Verify button in PGPtools (third from the right, open lock on an envelope), again using the "Clipboard" button in the dialog box. You'll be asked for your passphrase — accessing your private key this way insures that only you can decrypt the message (presuming you have been careful with your passphrase and custody of your secret key).

3. Notice that your decrypted message is displayed in a special viewer. You wouldn't want to write sensitive information to a file, now would you? (See the web page link about "deleted" files.) Some versions of PGP write decrypted files on the screen in very ugly fonts that frustrate tempest attacks for interpreting the electronic emissions from your monitor!