Dr. R. Beezer Math 133
Practicum #5 Fall 2003
PGP Key Generation

In this practicum, we will create our keys for public-key encryption, via the program Pretty Good Privacy. The necessary software is installed in Thompson 120. You may install the PGP software on your own computer (it is freeware, see notes below and links on course page). However, failure to make your own installation function properly is not an excuse for not finishing this practicum.

Procedure

1. Login to your UPS account on a computer in Th 120 (or use your own computer after installing PGP.)

2. Follow Start > Programs > P G P > PGPkeys to start the key management software.

3. A wizard will walk you through building your own public/private key. Observe the following notes.

   (a) Use your full name, last name first, middle initial, correct capitalization, etc. (e.g Beezer, Robert A.). Use your full email address (e.g. beezer@ups.edu). Remember, you are creating an on-line identity here.

   (b) Pick your passphrase *very* carefully, reading the links on the course page *first*. **All** of the subsequent security relies on this key step. Make it reasonably complicated, don't write it down, yet do not forget it!

4. Highlight your key, then follow Keys > Properties. In the "Fingerprint" area click the checkbox that says "Hexadecimal." You will then see a new string of digits and letters (A through F, possibly) in base 16 (i.e. hexadecimal). This is a hash of your key (not the key itself), and will be a convenient way to determine if two versions of the same key are really identical. When you uncheck the "hexadecimal" box, you get a list of strange words. Reading these aloud is another way to compare two versions of the same key.

   Write down the hexadecimal version of your fingerprint and bring it to class with you when we have our keysigning party. This way we can verify face-to-face that the key I get from you is *really* your key.

5. Post your key on the keyserver by choosing Server > Send To from within PGPkeys. Select the keyserver at `keyserver.pgp.com`.

6. Export a copy of your key to a text file as follows. Choose Keys > Export. Name the file something like beezer.asc (use *your* last name, but keep .asc on the end). Don't include your private key, and do include version 6.0 extensions. This will create a text file. You might be curious to peek at this file (using a program like Notepad), but be certain not to make any changes to it in the process.

7. Email me the text file version of your public key that you just created, as an attachment to an email message.

8. I will *sign* your key (more about this in class) and email it back to you as a text file *after* our keysigning party. I will also be emailing you a copy of my public key.

9. Import the signed copy of your key, or my public key, as follows. Choose Keys > Import. Navigate to the file that came to you from me as an attachment. Open the file, click on the key, and add it to your keyring.

10. Update your public key on the keyserver, as above, by simply sending it to the same server as before.

Grading

1. Full credit once I verify your fingerprint in class (so you have to send me your public key in advance). You must accomplish a few steps beyond this (adding your signed key to your keyring, updating the server, adding my key to your keyring) in order to participate in further practicums and other class activities, so make sure you finish everything beyond this stage now.

Notes

1. Some of this will seem very confusing at first. Please try to follow the directions carefully. I'll explain some of the finer points in class. Notice that we will not be doing any official communication in this practicum, just getting organized for doing that in the next two practicums.

2. Even though we won't appear to be accomplishing much, this is the most critical (and difficult) stage of using PGP. Specify your identity carefully and protect it with strong passphrase that nobody could ever guess. I'll say that again: protect your private key with a strong passphrase that nobody could ever guess. Memorize your pass phrase, do not write it down. Make a backup of your public/private key pair onto a floppy, zip disk, rewritable CD, USB portable drive, etc.

3. If you choose to make your own installation, be sure to get PGP 7.0.3, since that is what I am using, and what is installed in Th 120. Go to the International PGP site (download area link is on the course page), choose PGP itself, then your operating system, then the version numbered closest to 7.0.3.

4. Extra: Highlight your key in the PGPkeys application. Then choose Keys > Add > Photo. Include a 120 × 144 photo of yourself in your key, if you wish (not required).

5. Extra: If you decide that your passphrase is not secure enough, you can change it by going through Keys > Properties > Change Passphrase.

6. Extra: Your keys are stored in three files: `pubring.pkr`, `secring.skr`. The file `randseed.rnd` contains information related to how PGP generates random numbers and is unique to your use of PGP. You can locate these file as follows in PGPkeys: Edit

> Options... > Files. Once located, you can back up these files, move them to a new location, or install them on a new machine. If you do move them, remember to tell PGPkeys where they went (through this same dialog box, using the Browse buttons).

7. Extra: You may sign your classmates keys as follows. Obtain a copy of your classmates key by email, floppy disk, USB storage device, or off the keyserver. Look at its properties and view the fingerprint. Have your classmate tell you the fingerprint of their key, based on the original copy that they possess (either the hexadecimal version or the funny word version). Make sure that his comparison is done over a "secure channel," i.e. face-to-face, over the phone (if you are confident that you can recognize your classmate's voice). Do not verify a key's fingerprint by email!

   Once you've signed a key, put it back on the server by sending it there. Now its a new and improved version since it has been signed by you. Your classmate can get the improved version by highlighting their key and choosing "Update" off the Server menu.

8. Extra: While we are not doing any communication in this practicum, you can fiddle with PGPtools, which is the subject of the next two practicums. We will use it to actually encrypt messages and to build digital signatures.

9. Extra: Your private key must remain in your control, since it is what you use to decrypt messages meant only for you, and it is what you use to establish your on-line identity. Normally, the fact that it is encrypted itself with your passphrase is sufficient to protect it. However, if the secret police were to get a copy, with enough time, they might have sufficient resources to break that encryption.

   So you might want to keep your secret key under your physical control at all times. However, this risks losing it altogether, which is almost as catastrophic, since all of your correspondents will have to verify a replacement key over secure channels. So make a backup copy on permanent media (a CD-R might be a good choice) and lock it up (in a vault or safe-deposit box) off-site.