Overview: You are going to do the following things

1. Install the Gnu Privacy Guard, also called GnuPG or GPG, on your computer
2. Determine a passphrase to guard your private key
3. Generate a public/private key pair for yourself
4. Export your public key to an ASCII document file, sometimes called "ASCII armored." (There is no real armor or other security advantage and besides, this is your public key; it doesn't need security.) Name the key file <yourname>_key.asc
5. Send a friend your public key. Your friend can use it to encrypt a document that only you can decrypt.
6. Get a friend's public key, use it to encrypt a document, and send it to your friend.

Optional steps: You may want to do the following:

- Generate a revocation certificate (You will probably have to use the command line interface to do this.)
- Upload your public key to a public key server. (Key servers talk to each other, so one is usually enough.)
- Set up both digital signature and encryption for your preferred email program, if supported.
- Export your private key and revocation certificate to a backup medium.
- Have your public key digitally signed by two or three other people, beginning a "web of trust" for y our key. Note: you should only sign the public key of someone you can absolutely identify; similarly, only people who know you or can identify you should sign your key. For a counter-example, see this. (Contains vulgar language, so be warned.)

The handout doesn't contain instructions for doing these things, but you will have learned enough to figure most of them out by the time you've completed the assignment. GnuPG does work as a command line program in all operating systems. In general, you must be "in" the directory containing the gpg binary. For actions not supported by the GUI interface, check http://www.gnupg.org/gph/en/manual/book1.html (This was written in 1999; remarks about the encryption algorithms are out of date, but the procedures are correct.)

Beware:If you start to use GnuPG, and one hopes you will, you will need to guard both your private key file and your passphrase. If you lose either, you will lose access to everything encrypted with your public key. If your revocation certificate is compromised, Evil Eve can revoke your public key. Be sure to take appropriate precautions.

Some terminology: You will likely do some research on the web. The terminology used in some web articles is a bit confusing. Here are definitions to help you.

OpenPGP

OpenPGP is a standard describing a mechanism for both encrypting and digitally signing files. Those files may be email messages or, as in this exercise, a "plain" data file. There is no "OpenPGP" program; two programs that implement the OpenPGP standard are described below.

PGP

PGP is a company and also the name of that company's products. The PGP products implement the OpenPGP standard. They're commercial products; they cost money. People pay PGP Corp. money to get technical support, regular product upgrades, etc. There was a free version of PGP, but it i sPeobuobupstomGP(P)-4.5-20 (pr)-d (t)-40.1 (o)-.6 0.007 To5.7 (

You can make guessing a lot harder by "lying" when you create a pass phrase. My actual